Table of Contents

20. juni 2021 15:48

'All Commands' include many of the commands taught in Advanced Switching Course.
You will also find commands that were helpful to some students, but that you didn't see in the course.

This is NOT a 'monkey see monkey do' manual but it is up to you to choose which commands to use and when.

2. **VLAN, VTP, Trunk, MAC**
3. **EtherChannel, InterVLAN**
4. **STP**
5. **STP vs RSTP**
6. **DAI, IP Source Guard**
7. **DHCP Snooping**
8. **HSRP (FHRP)**
9. **VACL, RACL, PACL, MAC ACL, dot1x, SPAN**
10. **Voice**
11. **IP SLA**
12. **SNMP**
13. **NTP, DHCP, AAA**
14. **SDM Templates , TCL scripting**
15. **PVLAN**
16. **IPv6**

SWITCH cmd - VLAN, VTP, Trunk, MAC

20. juni 2021 15:48

```
!------------------------------
! show commands
!------------------------------
sh interface status
sh interface <vlan-id>
sh interface <>
sh vlan [brief]
sh vlan [< >]

!-----------------------------------
! speed settings on ports
!
! Link Speed: determined by electrical signaling
! Duplex mode: negotiated through an exchange of
!  information
! If autonegotiation fails (10/100Mb)
!  - falback default is 'half-duplex'
! If autonegotiation fails (1000Mb)
!  - falback default is 'full-duplex'
! Functions only if BOTH ENDS are set to
! AUTONEGOTIATION!!!
!-----------------------------------
int fa 0/x
 speed 100
 duplex full

!-----------------------------------
! Management module in Layer 2 switch
! SVI (Switched Virtual Interface)
!-----------------------------------
interface vlan <vlan-id>
 ip address …
!
ip default-gateway <IP of GW>

!-----------------------------------
! Create VLANs
!-----------------------------------
vlan <vlan-id>
 name <name>

!-----------------------------------
! Shutdown VLAN (locally)
!-----------------------------------
! on vtp server or transparent
vlan <>
 shutdown
! on vtp client
shutdown vlan <>

!-----------------------------------
! Suspend VLAN (done on vtp server)
!-----------------------------------
vlan <>
 state suspend
or
state suspend vlan <>

!-----------------------------------
! Activate VLAN (done on vtp server)
!-----------------------------------
vlan <>
 state active
or
state active vlan <#>
```

```
!-----------------------------------
! VLAN on port
!-----------------------------------
int range fa 0/x - y
or
int range fa 0/x, fa0/y, fa0/z
 description ...
 switchport mode access
 switchport access vlan <vlan-id>
Or
Switchport host

!-----------------------------------
! Create trunks (802.1Q)
!-----------------------------------
int range fa 0/x - y
 switchport trunk encapsulation {dot1q|isl}
 switchport mode {trunk|dynamic auto|dynamic desirable}
 switchport nonegotiate
 switchport trunk native vlan <vlan-id>
 switchport trunk allowed vlan x,y,a - b
 no shutdown

sh int trunk
sh int <> switchport
sh run int <>
```

VLAN 1 carry control protocols: DTP, VTP, STP BPDUs, PAgP, LACP, CDP… from IOS 12.1(11b) VLAN1 can be removed from trunk and control protocols continue to flow on VLAN1

```
!-----------------------------------
! VTP
!-----------------------------------
vtp mode server | client | transparent
vtp version <1,2..> (only on server)
vtp domain <domain>
vtp password <PW>
vtp pruning (only on server)

sh vtp status
sh vtp counters
sh vtp password
```

How to reset the VTP configuration revision number to 0.

- Set the VTP domain name to a bogus value
- Change the VTP mode to transparent and then back to the previous mode

To change domain name to NULL (blank) - delete vlan.dat and power cycle

if md5 mismatch and problem is not wrong password then try to sync switches making a change in the VLAN dB on a server.

```
!------------------------------
! Clear Switch
!------------------------------
delete vlan.dat
erase startup-config

Check:
sh vlan
```

If previous VLAN configuration information is still present (other than the default management VLAN 1), you must power-cycle the switch (hardware restart) instead of issuing the reload command. To powercycle the switch, remove the power cord from the back of the switch or unplug it, and then plug it back in.

```
power cycle
or
reload
```

```
!-------------------------------------------------------------
! Managing the MAC Address Table
!-------------------------------------------------------------
sh mac-address-table [dynamic]
sh mac-address-table <mac address>
clear mac-address-tabel [dynamic]

mac-address-table static <mac-address> vlan <vlan-id> int fa 0/x

!-------------------------------------------------------------
! Port Security
!-------------------------------------------------------------
int fa 0/x
 switchport port-security ! this line turns on function
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address <mac-address>
 switchport port-security violation shutdown|restrict|protect

sh port-security

if port is in (err disabled)
 1. -> shutdown (administrativly shutdown)
 2. -> no shutdown
```

shutdown	errdisable + log + snmp
restrict	drop + log + snmp
protect	drop

```
Automatic recovery:
errdisable recovery cause psecure-violation
errdisable recovery interval <sec>
```

```
!-------------------------------------------------------------
! Password Recovery - Switch
!-------------------------------------------------------------
press MODE button
    -follow instruction

flash_init
load_helper
    -rename flash:config.text flash:config.text.old
boot
    -rename flash:config.text.old flash:config.text

!-------------------------------------------------------------
! Manage IOS and Config on Switch
!-------------------------------------------------------------
sh version
sh flash
cd flash:/<dir>

copy flash tftp
copy tftp flash

copy startup-config tftp
erase nvram
copy tftp startup-config

sh boot
rename flash:/… flash:/
dir flash:/

delete flash:/…/html/*

archive tar /x tftp://<ip-of-tftp>/<ios-name> flash:/<dir>

boot system flash:/IOSname
```

SWITCH cmd - EtherChannel, InterVLAN

```
!-------------------------------------
! Inter-VLAN routing (router setup)
!-------------------------------------
int fa 0/0
 no shutdown
!
int fa 0/0.<vlan-id>
 encapsulation dot1q <vlan-id> [native]
 ip address <IP> <SM>
!
int fa x/x
 [switchport trunk encapsulation {dot1q|isl} ]
 switchport mode trunk
 switchport trunk native vlan <no>

!-------------------------------------
! Inter-VLAN routing (L3 Switch setup)
!-------------------------------------
int vlan <x>
 ip address <NET+SM>
!
int vlan <y>
 ip address <NET+SM>
!
ip routing
```

Follow these **best practices** to mitigate compromises through a switch:

- **Proactively configure unused router and switch ports:**
  - Execute the **`shutdown`** command on all unused ports and interfaces.
  - Place all unused ports in a "parking-lot" VLAN used specifically to group unused ports until they are proactively placed into service.
  - Configure all unused ports as access ports, disallowing automatic trunk negotiation.
- **Disable automatic trunk negotiation:** By default, Cisco Catalyst switches running Cisco IOS software are configured to automatically negotiate trunking capabilities. This situation poses a serious hazard to the infrastructure because an unsecured third-party device can be introduced to the network as a valid infrastructure component. Potential attacks include interception of traffic, redirection of traffic, and DoS. To avoid this risk, disable automatic negotiation of trunking and manually enable it on links that require it. Ensure that trunks use a native VLAN that is dedicated exclusively to trunk links.
- **Monitor physical device access:** Avoid rogue device placement in wiring closets with direct access to switch ports.
- **Establish port-based security:** Specific measures should be taken on every access port of any switch placed into service. Ensure that a policy is in place outlining the configuration of both used and unused switch ports. For ports enabled for end-device access, the macro **`switchport host`** takes the following actions when executed on a specific switch port:
  - Sets the switch port mode to access
  - Enables spanning tree PortFast
  - Disables channel grouping.

Note:
The **`switchport host`** command is a macro that executes several configuration commands. It does not have a **`no`** form to disable it. To return an interface to its default configuration, use the **`default interface`** *`interface-id`* global configuration command.

```
!-------------------------------------
! EtherChannel
!-------------------------------------
Fast EtherChannel (FEC) - bundle ports
FEC – up to 8 100Mb full duplex (1.6Gb)
GEC – up to 8 1Gb full duplex (16Gb)
PAgP - Cisco proprietary
LACP - 802ad - non-Cisco devices

PAgP manages EtherChannel. PAgP packets are sent every 30 seconds using multicast group
MAC address 01-00-0C-CC-CC-CC with protocol value 0x0104.
```

PAgP	LACP 802.3ad	Negotiation packets sent?	
on	on	No	All ports channeling
desirable	active	yes	actively asks to form a channel
auto	passive	yes	waits to channel , until asked

Note: When configuring EtherChannels, it can be helpful to shut down the physical interfaces being grouped on both devices before configuring them into channel groups. Otherwise, the EtherChannel Misconfig Guard may place these interfaces into error disabled state. The interfaces and port channel can be re-enabled after the EtherChannel is configured

```
!-------------------------------------
! Connect with Cisco equipment (PAgP):
!-------------------------------------
int range fa x/x – y
shutdown
description <>
switchport trunk … ! enter commands to setup trunk as needed
switchport mode trunk
channel-group 1 mode desirable
no shutdown
!
port-channel load-balance dest-mac (change default to destination mac)
sh etherchannel load-balance

!-------------------------------------
! Connect with non-Cisco equipment (LACP):
!-------------------------------------
int range fa x/x – y
shutdown
description <>
switchport trunk… ! enter commands to setup trunk as needed
channel-protocol lacp
channel-group 1 mode {on|off|passive|active}

NOTE: if channel-group X on is used
- first disable PAgP/LACP with channel-protocol off

!-------------------------------------
! Layer 3 EtherChannel:
!-------------------------------------
interface range fa x/x - y
shutdown
no switchport
channel-group 2 mode desirable
no shutdown
exit
!
interface port-channel 2
ip address <>
exit

sh etherchannel summary
sh pagp neighbor (Port Aggregation Protocol – PagP)
sh int fa0/x etherchannel
sh etherchannel x port-channel

Check if port is in err-disabled
- shutdown and no shutdown
```

SWITCH cmd - STP

28. april 2016 14:51

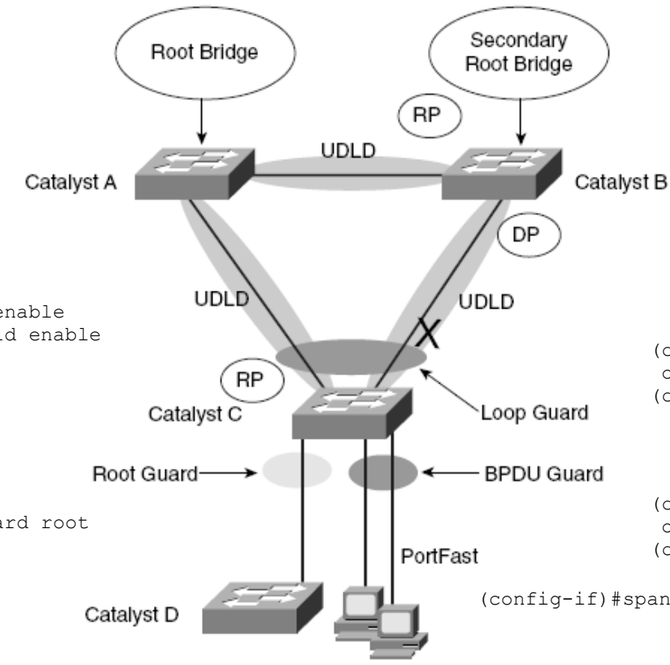
```
!--------------------------------------------------
! Spanning-tree (STP)
!--------------------------------------------------
spanning-tree mode {pvst|rapid-pvst} ! on all switches

!-------------------------------------
! Choose root switch
!-------------------------------------
spanning-tree vlan <vlan-id's> root primary|secondary [diameter 5]
! primary = 32768-8192 = 24576
! secondary = 32768-4096 = 28672
or
spanning-tree vlan <vlan-id's> priority <no>
! 32768 default priority
! increments of 4096
! 4096 -> root
! 16384 -> secondary root

!-------------------------------------
! Enable portfast
!-------------------------------------
spanning-tree portfast default
 - enables PortFast on all nontrunking ports
or
int fa 0/x
 spanning-tree portfast

!-------------------------------------
! Change Port priority
!-------------------------------------
int fa 0/x
 spanning-tree port-priority <no>

!-------------------------------------
! Change root port using spanning-tree cost
!-------------------------------------
int fa 0/x
 spanning-tree cost <no>

sh spanning-tree [vlan <vlan-id>]
sh spanning-tree summary
sh spanning-tree interface…
sh spanning-tree inconsistentports

debug spanning-tree events
```

Mb	cost
10	100
100	19
1.000	4
10.000	2

802.1D	STP	BPDU originate from root Use timers
802.1Q	CST	
802.1s	MST	
802.1w	RSTP	Don't use timers but uses handshakes

```
!-------------------------------------
! Multiple Spanning-Tree (MST)
!-------------------------------------
spanning-tree mode mst
!
spanning-tree mst configuration
 name <name>
 revision 2
 instance 2 vlan 10
 show pending
 show current
end

spanning-tree mst <instance> root primary|secondary
spanning-tree extend system-id
spanning-tree mst pre-standard

sh spanning-tree mst configuration
sh spanning-tree mst [instance [detail]]
sh spanning-tree mst interface…

sh spanning-tree [vlan NO]
sh run int fa 0/x
```

```
!-------------------------------------
! 3 steps for STP units
!-------------------------------------
  1. Elect root (according to 5 step decision sequence)
  2. Elect Root ports
  3. Elect Designated ports


!-------------------------------------
! 5 step decision sequence
!-------------------------------------
  1. Lowest BID
  2. Lowest Path Cost to root bridge
  3. Lowest sender BID
  4. Lowest Port Priority
  5. Lowest Port ID
```




```
(config)#spanning-tree udld enable
(config-if)#spanning-tree udld enable
```

```
(config-if)#spanning-tree guard root
```

```
(config)#spanning-tree loopguard default
 or
(config-if)#spanning-tree guard loop
```

```
(config)#spanning-tree portfast bpduguard default
 or
(config-if)#spanning-tree bpduguard enable
```

```
(config-if)#spanning-tree portfast
```

Protecting against **unexpected** BPDUs

Protecting against **sudden loss** of BPDUs

Root guard: Apply to ports where root is never expected. -> root-inconsistent

BPDU guard: Apply to all user ports where PortFast is enabled. -> errdisable

Loop guard: Apply to nondesignated ports but okay to apply to all ports.

UDLD: Apply to all fiber-optic links between switches (must be enabled on both ends).

Permissible combinations on a switch port:

Loop guard and UDLD
Root guard and UDLD

Not permissible on a switch port:

Root guard and Loop guard
Root guard and BPDU guard

SWITCH cmd - STP vs RSTP

7. september 2015 09:08

STP (802.1d)	**Rapid STP (802.1w)**
In stable topology **only the root** sends BPDU and relayed by others.	In stable topology **all bridges** generate BPDU every Hello (2 sec) : used as *"keepalives" mechanism.*
Port states	
Disabled ***Blocking*** ***Listening*** ***Learning*** ***Forwarding***	***Discarding*** (replace disabled, blocking and listening) **|** **|** ***Learning*** ***Forwarding***
Port roles	
Root (Forwarding) ***Designated*** (Forwarding) ***Non-Designated*** (Blocking)	***Root*** (Forwarding) ***Designated*** (Forwarding) ***Alternate*** (Discarding) ***Backup*** (Discarding)
Additional configuration to make an end node port a ***port fast*** (in case a BPDU is received).	- An ***edge port*** (end node port) is an integrated Link type which depends on the duplex : Point-to-point for full duplex & shared for half duplex).
Topology changes and convergence	
Use timers for convergence (advertised by the root): ***Hello*** (2 sec) ***Max Age*** (20 sec) ***Forward delay timer*** (15 sec)	- Introduce ***proposal and agreement*** process for synchronization ***(< 1 sec***).- Hello, Max Age and Forward delay timer used only for backward compatibility with standard STP
	Only RSTP port receiving STP (802.1d) messages will behaves as standard STP.
Slow transition (***50sec***):Blocking (20s) =>Listening (15s) =>Learning (15s) =>Forwarding	Faster transition on point-to-point and edge ports only:Less states – ***No learning state***, doesn't wait to be informed by others, instead, ***actively*** looks for possible failure by ***RLQ*** (Request Link Query) a feedback mechanism.
Use only 2 bits from the flag octet:Bit 7 : Topology Change Acknowledgment Bit 0 : Topology Change	Use other 6 bits of the flag octet (BPDU type 2/version 2):Bit 1 : Proposal Bit 2, 3 : Port role Bit 4 : Learning Bit 5 : Forwarding Bit 6 : Agreement Bit 0, 7 : TCA & TCN for backward compatibility
The bridge that discover a change in the network inform the root, that in turns informs all others by sending BPDU with TCA bit set and instruct them to clear their DB entries after **"short timer" (~Forward delay)** expire.	TC is flooded through the network, every bridge generate TC (Topology change) and inform its neighbors when it is aware of a topology change and **immediately delete old DB** entries.
If a non-root bridge doesn't receive Hello for 10*Hello (advertised from the root), start claiming the root role by generating its own Hello.	Wait for 3*Hello (advertised from the root) before deciding to act.
Wait until TC reach the root + short timer (~Forward delay) expires, then flash all root DB entries	Delete immediately local DB except MAC of the port receiving the topology changes (proposal)

SWITCH cmd - DAI, IP Source Guard

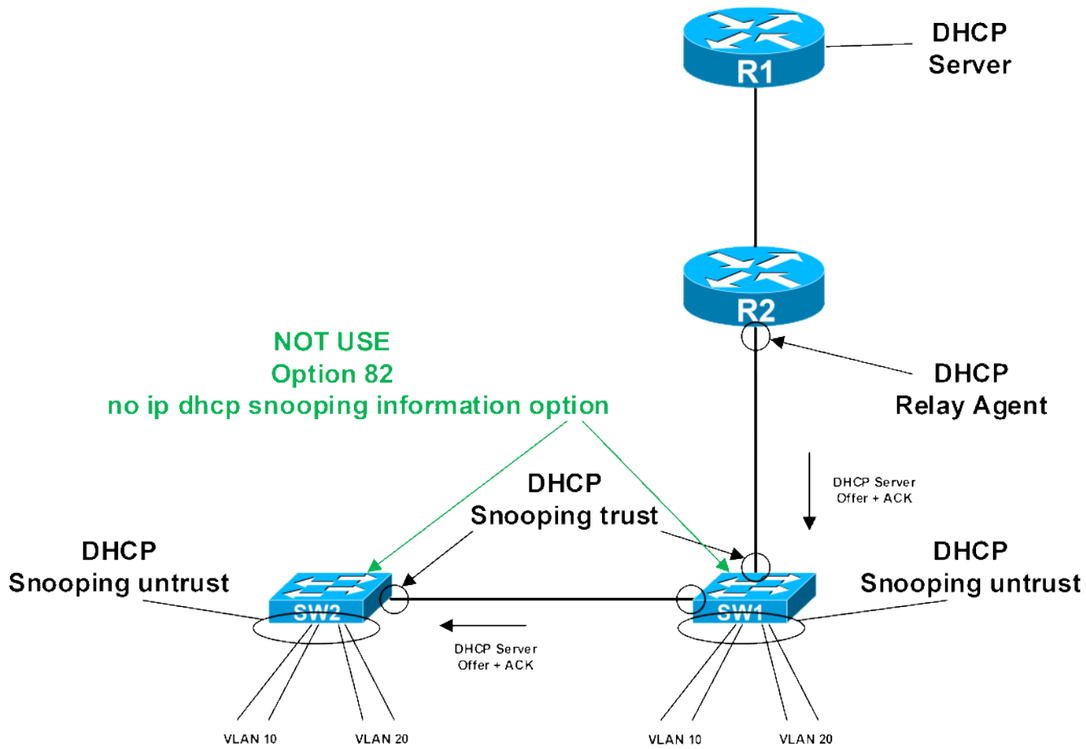
10. oktober 2016 11:37

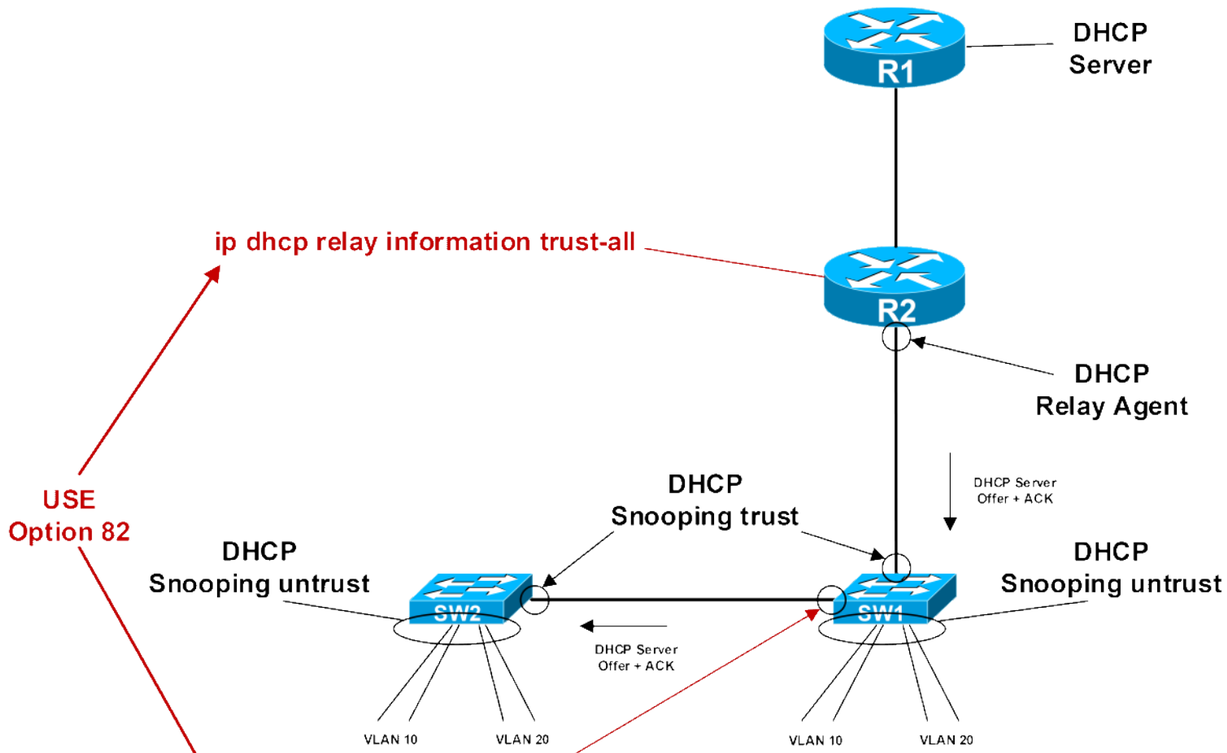
```
!-------------------------------------
! IP Source Guard
!-------------------------------------
ip dhcp snooping                                          enables DHCP snooping globally

interface ...
 ip verify source vlan dhcp-snooping port-security        enables IP source guard, source IP and source MAC address filter
exit

ip dhcp snooping vlan number [no]                         enables DHCP snooping on your VLANs

ip source binding ip-addre <IP> vlan <no> interface <int> static IP source binding
```

```
!-------------------------------------
! Dynamic ARP Inspection (DAI)
! ARP spoofing or "poisoning"
!-------------------------------------
You can also use DAI to set the rate limit of ARP packets and then err-disable the interface if the rate is exceeded

To mitigate the chances of ARP spoofing, the following procedures are recommended:
Step 1 Implement protection against DHCP spoofing.
Step 2 Enable dynamic ARP inspection.

ip arp inspection vlan <vlan_id[,vlan_id]                 enables DAI on a VLAN

interface fa x/y
 ip arp inspection trust                                  enables DAI on interface and int as trusted (default untrusted!)
 ip arp inspection validate {[src-mac] [dest-mac] [ip]}   drop ARP packets when the IP address are invalid
```

DHCP Snooping (option 82)

22 August 2018 14:54



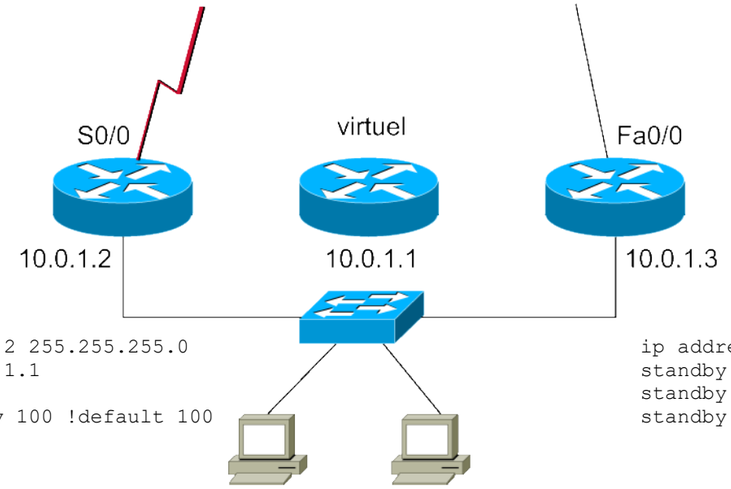



```
!-------------------------------------
! DHCP Snooping (no option 82)
!-------------------------------------
ip dhcp snooping
ip dhcp snooping vlan <>
no ip dhcp snooping information option
!
! On all links where DHCP server packets are expected
int <>
 ip dhcp snooping trust

! On all untrusted ports (optional)
int <>
 ip dhcp snooping limit rate <>


sh ip dhcp snooping [binding]
```

```
!-------------------------------------
! DHCP Snooping (use option 82)
!-------------------------------------
ip dhcp snooping
ip dhcp snooping vlan <>
ip dhcp snooping information option
!
! On all links where DHCP server packets are expected
int <>
 ip dhcp snooping trust

! On all untrusted ports (optional)
int <>
 ip dhcp snooping limit rate <>

! The following according to drawing
! ip dhcp relay information trust-all
! ip dhcp snooping information option allow-untrusted

sh ip dhcp snooping [binding]
```

SWITCH cmd - HSRP (FHRP)

4. februar 2020 09:28




```
ip address 10.0.1.2 255.255.255.0
standby 1 ip 10.0.1.1
standby 1 preempt
standby 1 priority 100 !default 100
```

```
ip address 10.0.1.3 255.255.255.0
standby 1 ip 10.0.1.1
standby 1 preempt
standby 1 priority 150
```

Gateway: 10.0.1.1

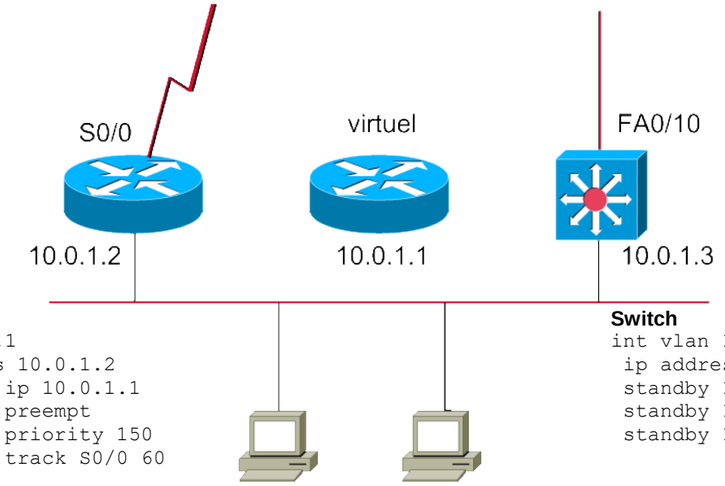
```
!-------------------------------------
! Object Tracking
!-------------------------------------
ip sla <#>
 icmp-echo <IP#>
 frequency 10
ip sla schedule <#> life forever start-time now
!
track 111 ip sla <#> reachability
!
int <>
 standby 20 track 111 decrement 30
```

```
!-------------------------------------
! Port Tracking
!-------------------------------------
standby 20 track fa 0/0 <# to decrease>
```

	HSRP	VRRP (Virtual Router Redundancy Protocol - IEEE standard)	GLBP (Gateway Load Balancing Protocol)
	1994	1999	2005
	Active-Standby	Master-Backup Master forward	AVG - Active Virtual Gateway AVF - Active Virtual Forwarder Primary-Secondary Round robin
RFC	cisco proprietary RFC 2281	RFC 2338	cisco proprietary
Hello timer	3 sec	1 sec	3
Hold timer	10	3	
	0000.0c07.acxx (ver 1)	0000.5e00.01xx	assigned by AVG 0007.b400.xxyy (up to four yy pr group xx)
		virtual IP or real IP	

```
sh standby brief
sh standby <int>
debug standby terse
```

! ***Preempt*** gives the right to claim active role
! if you have higher priority



Router

```
int fa 0/0.1
 ip address 10.0.1.2
 standby 1 ip 10.0.1.1
 standby 1 preempt
 standby 1 priority 150
 standby 1 track S0/0 60

int fa 0/0.10
 ip address 10.0.10.2
 standby 10 ip 10.0.10.1
 standby 10 preempt
 standby 10 priority 150
 standby 10 track S0/0 60

…
```

Gateway: 10.0.1.1

Switch

```
int vlan 1
 ip address 10.0.1.3
 standby 1 ip 10.0.1.1
 standby 1 preempt
 standby 1 priority 110


int vlan 10
 ip address 10.0.10.3
 standby 10 ip 10.0.10.1
 standby 10 preempt
 standby 10 priority 110

…
```

State	Definition
Initial	This state is entered through a configuration change or when an interface first becomes available.
Learn	The router has not determined the virtual IP address and has not yet seen a hello message from the active router. In this state, the router waits to hear from the active router.
Listen	The router knows the virtual IP address, but the router is neither the active router nor the standby router. It listens for hello messages from those routers.
Speak	The router sends periodic hello messages and actively participates in the election of the active and/or standby router.
Standby	The router is a candidate to become the next active router and sends periodic hello messages.
Active	The router currently forwards packets that are sent to the group virtual MAC address. The router sends periodic hello messages.

	224.0.0.2 UDP 1985	224.0.0.18 UDP 112	224.0.0.102 UDP 3222
	preemption	preemption (default)	
	int track		int track
3560 do NOT support two group on one interface. You are NOT able to run IPv4 and IPv6 HSRP on the same time. !!!3750 DO SUPPORT this!!!		Version 2 supports IPv6	Version 3 supports IPv6

SWITCH cmd - VACL, RACL, PACL, MAC ACL, dot1x, SPAN

21. februar 2020 12:45

```
!-------------------------------------
! VLAN ACL (VACL)
! Two types (IP/MAC)
! VLAN ACL applies to traffic in and out of VLAN
! - can filter on L2/3/4 information
!-------------------------------------
     int <>
      access-group mode [prefer port | merge]

     !-------------------------------------
     ! IP ACL
     ! ! - can filter on L3/4 information
     !-------------------------------------
     ip access-list [standard | extended | numbered] <NAME | number>
      …
      exit
     !
     vlan access-map <NAME>
      match [ip | mac] address <ACL>
      action {forward | drop | redirect} [log]
      exit

     !-------------------------------------
     ! MAC ACL
     ! ! - can filter on MAC (L2) information
     !-------------------------------------
     mac access-list extended <NAME>
      permit host [<source MAC> | any] [<destination MAC> | any
      exit
     !
     vlan access-map <NAME>
      match [ip | mac] address <ACL>
      action {forward | drop | redirect} [log]
      exit

     !-------------------------------------
     ! Apply the VACL to one or more VLANs
     ! in global config
     !-------------------------------------
     vlan filter <map-name> vlan-list [vlan-list | all]


show vlan access-map
show vlan filter
```

```
!-------------------------------------
! Router ACL (RACL)
! Router ACL applies to L3  port
! SVI, L3sw routed port and Routed ports)
!-------------------------------------
ip access-list [standard | extended | numbered] <NAME | number>
 …
 exit
!
interface <ID>
 ip access-group <ACL> {in|out}

sh ip access-lists
sh ip int <INT>
```

```
!-------------------------------------
! dot1x
!-------------------------------------
aaa new-model
radius-server host <hostname|ip-assress> [key <string>] !points to server

aaa authentication dot1x default [group radius] local   !Create authentication method list

dot1x system-auth-control !activates global support for 802.1X

int <>
 authentication port-control {force-authorized | force-unauthorized | auto}
 dot1x pae authenticator
 [dot1x host-mode {single-host | multi-host}] !in multi-host mode only one host need to authenticate on port
```

Note: For switches running Cisco IOS version 12.2(50)SE or later, the `dot1x port-control auto` command is replaced with the following interface-level commands:

```
authentication port-control auto
dot1x pae authenticator

sh dot1x int <>
```

```
!-------------------------------------
! Port ACL (PACL)
! Two types (IP/MAC)
! Port ACL applies to L2sw port direction IN
! - can filter on L2/3/4 information
!-------------------------------------
     int <>
      access-group mode [prefer port | merge]

     !-------------------------------------
     ! IP ACL
     ! ! - can filter on L3/4 information
     !-------------------------------------
     ip access-list [standard | extended | numbered] <NAME | number>
      …
      exit
     !
     interface <>
      ip access-group <ACL> in

     !-------------------------------------
     ! MAC ACL
     ! ! - can filter on MAC (L2) information
     !-------------------------------------
     ip access-list extended <NAME>
      permit host [<source MAC> | any] [<destination MAC> | any
      exit
     !
     interface <>
      mac access-group <ACL> in
```

```
!-------------------------------------
! SPAN Sniff traffic on a switch
!-------------------------------------
monitor session 1 source int fa 0/1
monitor session 1 destination int fa 0/10

!-------------------------------------
! RSPAN (Remote SPAN)
!-------------------------------------
Sw2:
vlan 50
name RSPANname
remote-span

monitor session 2 source int fa 0/24
monitor session 2 destination remote vlan 50

Sw1:
vlan 50
name RSPANname
remote-span

monitor session X destination int fa 0/10
monitor session X source remote vlan 50
```

SWITCH cmd - Voice

7. september 2015 09:09

```
!-------------------------------------
! Quality of Service (QoS
!-------------------------------------
mls qos                                          global command to turn on QoS - all switchports are configured as
untrusted

interface …
 switchport mode access
 switchport voice vlan <vlan-id>                 enable voice VLAN and associate a VLAN ID
 switchport access vlan 10                       accessport vlan -> native traffic use this
 mls qos trust {cos | ip-precedence | dscp}      802.1p User Priority or Class of Service (CoS) value
 mls qos trust device cisco-phone                trust the CoS value from phone (phone is trust boundary )

 mls qos cos <value>                             set cos on packets that have no CoS marking
 mls qos cos override                            set CoS on all packets

Extend trust boundary to PC:
 switchport priority extend cos <cos_value>      set CoS value to frames coming from PC attached to the IP Phone
 or
 switchport priority extend trust                trust the CoS (dot1p) from PC

 switchport priority default <0-7 default 0>

sh interfaces <interface-id> switchport          display voice parameters on interface
sh mls qos interface <interface-id>              display QoS parameters on interface

!-------------------------------------
! Auto QoS
!-------------------------------------
interface …
 auto qos voip trust                             trust CoS
 auto qos voip cisco-phone                       trust CiscoPhone

sh auto qos [interface <int_id>]

CatOS:
set qos autoqos
set port qos <port> autoqos trust [cos | dscp]
set port qos <port> autoqos voip [ciscosoftphone | ciscoipphone] [trust]

!-------------------------------------
! Power over Ethernet (PoE)
!-------------------------------------
```

3 methods

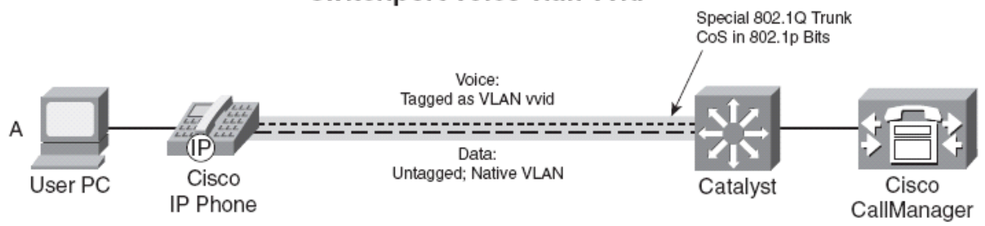
- Cisco Inline Power (ILP) - A Cisco proprietary method developed before the IEEE standard
- IEEE 802.3af - A standard-based method that offers vendor interoperability max 15,4 w pr. port
- IEEE 802.3at (PoE+): Max 25,5 w pr. port med 5 power klasser:
  - 0: no support of power classes 15,4 W
  - 1: 4 w reserved
  - 2: 7 w reserved
  - 3: 15,4 w reserved
  - 4: 51 w reserved

```
interface …
 power inline {auto [max milli-watts] | static [max milli-watts] | never

sh power inline
```

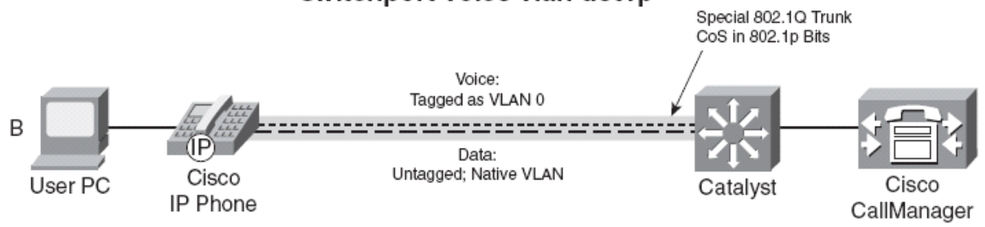
Voice VLAN - Auxilary VLAN

802.1Q or access-mode (single VLAN) port

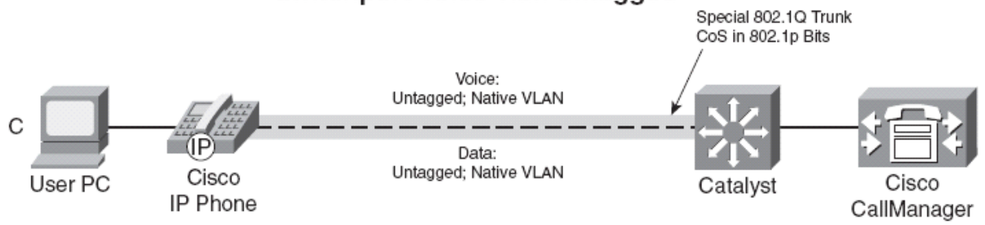
switchport voice vlan vvid



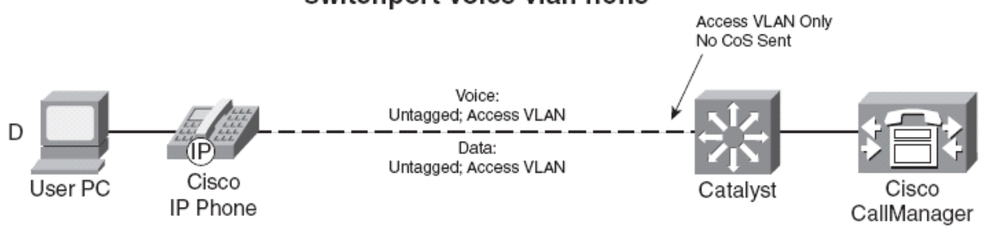
switchport voice vlan dot1p



switchport voice vlan untagged



switchport voice vlan none



SWITCH cmd - IP SLA

28. april 2016 14:54

```
************************************************************
Configure Cisco IOS IP SLA responders
************************************************************
conf t
ip sla responder
ip sla responder udp-echo ipaddress 172.16.1.1 port 5000 (SLA responder source info)
end

************************************************************************
Configure the Cisco IOS IP LSA source to measure network performance
************************************************************************
conf t
ip sla 1
icmp-echo 172.16.100.101
frequency X(in seconds)
exit

ip sla 2
icmp-echo 172.16.200.101
frequency X (in seconds)
exit

************************************************************************
Configure the Cisco IOS IP SLA for jitter
************************************************************************
conf t
ip sla 3
udp-jitter 172.16.1.101 5000
frequency X (in seconds)
exit

ip sla 4
udp-jitter 172.16.1.102 5000
frequency X (in seconds)
exit

************************************************************************************
Schedule the IP SLA operations to run indefinitely and beginnin immediately
************************************************************************************
conf t
ip sla schedule 1 life forever start-time now
ip sla schedule 2 life forever start-time now
ip sla schedule 3 life forever start-time now
ip sla schedule 4 life forever start-time now
!!!
source send control message over UDP 1967 to responder
Responder send ack
source send test packet
responder send timestamp in/out

************************************************************************************
SLA Authentication
************************************************************************************
Key Chain MYKEY
Key 1
Key-string <string>
IP sla key-chain MYKEY



show ip sla configuration <sla#>
show ip sla application
show ip sla responder
show ip sla statistic  <sla#>
```

SWITCH cmd - SNMP

28. april 2016 14:57

```
!-------------------------------------
! SNMP v2c setup
!-------------------------------------
snmp-server location Rack 1
snmp-server contact Student
snmp-server chassis-id Cisco 3960 SN FTX33333333

ip access-list standard NMS-SERVERS
 permit 172.16.99.0 0.0.0.255

snmp-server view NMS-LIMIT iso included
snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.21 excluded
snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.22 excluded
snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.35 excluded
snmp-server view NMS-LIMIT 1.3.6.1.2.1.3 excluded
snmp-server view NMS-LIMIT 1.3.6.1.6.3.15 excluded
snmp-server view NMS-LIMIT 1.3.6.1.6.3.16 excluded
snmp-server view NMS-LIMIT 1.3.6.1.6.3.18 excluded
!
snmp-server user student ccnp-switch2 v2c
snmp-server host 172.16.99.100 version 2c ccnp-switch2
snmp-server group ccnp-switch2 v2c read NMS-LIMIT access NMS-SERVERS

snmp ifmib ifindex persist

snmp-server enable traps
```

```
!-------------------------------------
! SNMP 3 setup
!-------------------------------------
snmp-server location Rack 1
snmp-server contact Student
snmp-server chassis-id Cisco 3960 SN FTX33333333

ip access-list standard NMS-SERVERS
 permit 172.16.99.0 0.0.0.255

snmp-server view NMS-LIMIT iso included
snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.21 excluded
snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.22 excluded
snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.35 excluded
snmp-server view NMS-LIMIT 1.3.6.1.2.1.3 excluded
snmp-server view NMS-LIMIT 1.3.6.1.6.3.15 excluded
snmp-server view NMS-LIMIT 1.3.6.1.6.3.16 excluded
snmp-server view NMS-LIMIT 1.3.6.1.6.3.18 excluded

snmp-server user student ccnp-switch3 v3 auth sha cisco123 priv aes 128 cisco123
snmp-server host 172.16.99.100 version 3 priv student
snmp-server group ccnp-switch3 v3 priv read NMS-LIMIT access NMS-SERVERS

snmp-server ifindex persist

snmp-server enable traps
```

```
Show snmp
Show snmp view
Show snmp group
Show snmp user
```

SWITCH cmd - NTP, DHCP, AAA

28. april 2016 14:45

```
!----------------------------------------
! NTP Server - Time from system clock
!----------------------------------------
clock set 08:00:00 Dec 16 2015
clock timezone CEST +2
clock summer-time CEST recurring

ntp authentication-key <#> md5 <PW>
ntp trusted-key <#>
ntp authenticate
ntp master <#>

access-list 1 permit 127.127.1.1 (ntp server
source address)
access-list 2 172.16.0.0 0.0.255.255

ntp access-group peer 1
ntp access-group serve-only 2

show clock
show clock detail


!----------------------------------------
! NTP Client
!----------------------------------------
ntp authentication-key <#> md5 <PW>
ntp trusted-key <#>
ntp authenticate
ntp server <IP>
clock timezone EDT +2
clock summer-time EDT recurring

show clock
show ntp associations
show ntp status
```

```
!----------------------------------------
! dhcp server
!----------------------------------------
ip dhcp excluded-address <start-IP> <end-IP>
ip dhcp pool <NAME>
 network <net> <sm>
 dns-server <dns-IP>
 default-router <gw-IP>

!----------------------------------------
! relay agent
!----------------------------------------
interface fa 0/0
 ip helper-address <dhcp-IP>

sh ip dhcp binding
sh ip dhcp pool
debug ip dhcp server events
```

```
!----------------------------------------
! AAA and Local Authentication
!----------------------------------------
aaa new-model
aaa authentication login default <local local-case enable none>
aaa authentication login <NAME> group <local local-case enable none>

Special set for special access:
aaa authentication login <NAME> local

Line vty 0 4
 login authentication <NAME> ---(all others use defaults)

debug aaa authentication

!----------------------------------------
! AAA and RADIUS Authentication
!----------------------------------------
aaa new-model
aaa authentication login default group radius none
aaa authentication login <NAME> group radius

Radius server <Server Name or IP>
Address ipv4 <IP> ---(Default ports for RADIUS is 1645+1646
Key <WORD>

Line vty 0 4
Login authentication <NAME>

End

Address ipv4 <IP> auth-port 1812 acct-port 1813

debug aaa authentication
```

SWITCH cmd - SDM Templates , TCL scripting

28. april 2016

```
!----------------------------------------
! SDM Templates
!----------------------------------------

sdm prefer <Template>

2960:
  default              Default bias
  dual-ipv4-and-ipv6   Support both IPv4 and IPv6
  lanbase-routing      Supports both IPv4 and IPv6 Static Routing
  qos                  QoS bias

3560:
  access               Access bias
  default              Default bias
  dual-ipv4-and-ipv6   Support both IPv4 and IPv6
  routing              Unicast bias
  vlan                 VLAN bias
```

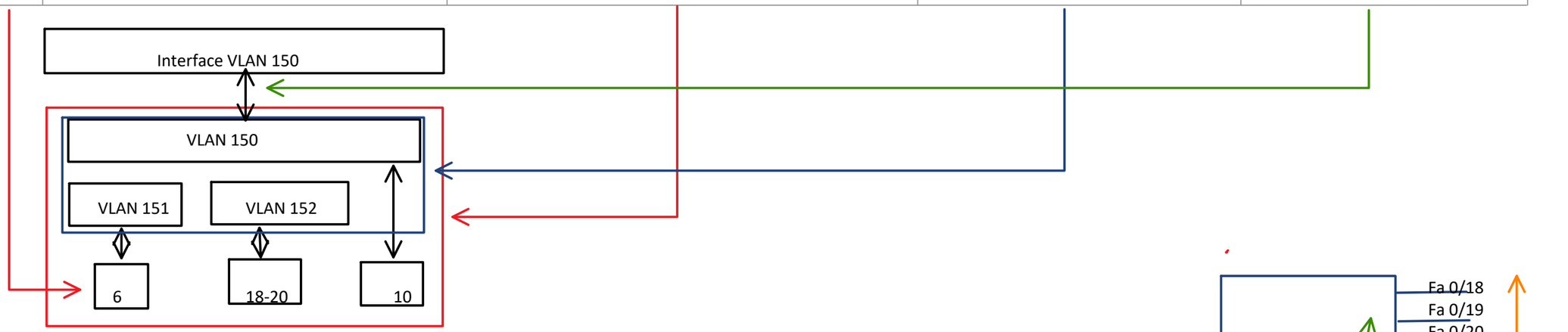
```
!----------------------------------------
! TCL scripting - PING
!----------------------------------------
tclsh

foreach address {
<IP#>
<IP#>
<IP#>
} {
ping $address }
```

```
!----------------------------------------
! TCL scripting - Clear switch completely
!----------------------------------------
tclsh
puts [ open "flash:resetsba.tcl" w+ ] {
typeahead "\n"
ios_config "hostname SW1"
ios_config "interface FastEthernet0/1" "shutdown"
ios_config "interface FastEthernet0/2" "shutdown"
ios_config "interface FastEthernet0/3" "shutdown"
ios_config "interface FastEthernet0/4" "shutdown"
ios_config "interface FastEthernet0/5" "shutdown"
ios_config "interface FastEthernet0/6" "shutdown"
ios_config "interface FastEthernet0/7" "shutdown"
ios_config "interface FastEthernet0/8" "shutdown"
ios_config "interface FastEthernet0/9" "shutdown"
ios_config "interface FastEthernet0/10" "shutdown"
ios_config "interface FastEthernet0/11" "shutdown"
ios_config "interface FastEthernet0/12" "shutdown"
ios_config "interface FastEthernet0/13" "shutdown"
ios_config "interface FastEthernet0/14" "shutdown"
ios_config "interface FastEthernet0/15" "shutdown"
ios_config "interface FastEthernet0/16" "shutdown"
ios_config "interface FastEthernet0/17" "shutdown"
ios_config "interface FastEthernet0/18" "shutdown"
ios_config "interface FastEthernet0/19" "shutdown"
ios_config "interface FastEthernet0/20" "shutdown"
ios_config "interface FastEthernet0/21" "shutdown"
ios_config "interface FastEthernet0/22" "shutdown"
ios_config "interface FastEthernet0/23" "shutdown"
ios_config "interface FastEthernet0/24" "shutdown"
ios_config "interface GigabitEthernet0/1" "shutdown"
ios_config "interface GigabitEthernet0/2" "shutdown" "end"
erase startup-config
delete /force vlan.dat
delete /force multiple-fs
ios_config "sdm prefer dual-ipv4-and-ipv6 routing"
typeahead "\n"
puts "Reloading the switch in 1 minute, type reload cancel to halt"
typeahead "\n"
reload in 1 RESETSBA.TCL SCRIPT RUN
typeahead "\n"
}
tclquit
```

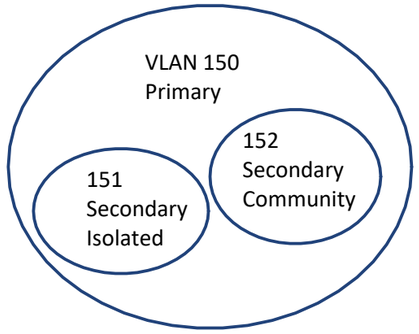
SWITCH cmd - PVLAN

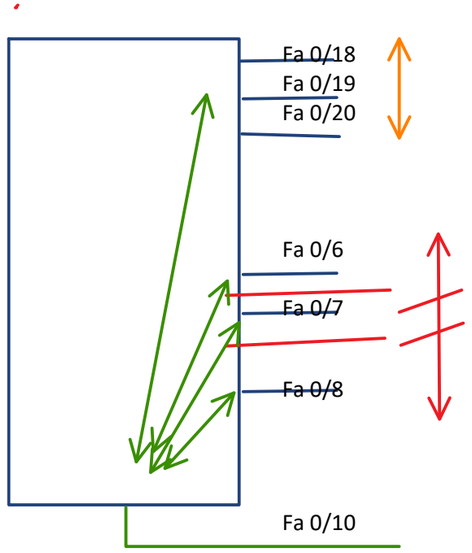
28. april 2016 15:03

Porte (L1)	Portens rolle	VLANS (L2)	PVLAN type	Mapping L2 - L3
				interface vlan 150 ip add <IP> <MASK>
6	interface fastethernet 0/6 switchport mode private-vlan host	interface fastethernet 0/6 switchport private-vlan host-association 150 151	vlan 151 private-vlan isolated	
18 - 20	interface range fastethernet 0/18 - 20 switchport mode private-vlan host	interface range fastethernet 0/18 - 20 switchport private-vlan host-association 150 152	vlan 152 private-vlan community	
10	interface fastethernet 0/10 switchport mode private-vlan promiscuous	interface fastethernet 0/10 switchport private-vlan mapping 150 151 152	vlan 150 private-vlan primary private-vlan association 151,152	
				interface vlan 150 private-vlan mapping 151-152




```
!-------------------------------------
! Private VLAN (PVLAN)
!-------------------------------------
vtp mode transparent (all VLANs must be defined on alle switches)

Or

VTP mode version 3 (supports distribution og VLAN information)

!-------------------------------------
! Private VLAN (PVLAN)
!-------------------------------------
sh interface <interface> switchport
sh vlan private-vlan
```





SWITCH cmd - IPv6

3. maj 2016 07:50

```
!-----------------------------------
! IPv6 routing på L3 switche
!-----------------------------------

Ipv6 unicast-routing
Ipv6 cef

!-----------------------------------
! IPv6 faste IP adresser
!-----------------------------------

Ipv6 unicast-routing
Ipv6 cef

Interface VLAN 100
Ipv6 add 2001:0600::1/64


!-----------------------------------
! IPv6 SLAAC tildeling af IP adresser
!-----------------------------------


!-----------------------------------
! IPv6 I/F DHCP tildeling af IP adresser
!-----------------------------------
```

```
!-----------------------------------
IPv6 DHCP server
!-----------------------------------
```

SWITCH cmd - VACL, RACL, PACL, MAC ACL, dot1x, SPAN

21. februar 2020 12:45

RETTET VERSION

```
!-------------------------------------
! VLAN ACL (VACL)
! Two types (IP/MAC)
! VLAN ACL applies to traffic in and out of VLAN
! - can filter on L2/3/4 information
!-------------------------------------
     int <>
      access-group mode [prefer port | merge]

     !-------------------------------------
     ! IP ACL
     ! ! - can filter on L3/4 information
     !-------------------------------------
     ip access-list [standard | extended | numbered] <NAME | number>
      …
      exit
     !
     vlan access-map <NAME>
      match [ip | mac] address <ACL>
      action {forward | drop | redirect} [log]
      exit

     !-------------------------------------
     ! MAC ACL
     ! ! - can filter on MAC (L2) information
     !-------------------------------------
     mac access-list extended <NAME>
      permit host [<source MAC> | any] [<destination MAC> | any
      exit
     !
     vlan access-map <NAME>
      match mac address <ACL>
      action {forward | drop | redirect} [log]
      exit

     !-------------------------------------
     ! Apply the VACL to one or more VLANs
     ! in global config
     !-------------------------------------
     vlan filter <map-name> vlan-list [vlan-list | all]


show vlan access-map
show vlan filter
```

```
!-------------------------------------
! Router ACL (RACL)
! Router ACL applies to L3  port
! SVI, L3sw routed port and Routed ports)
!-------------------------------------
ip access-list [standard | extended | numbered] <NAME | number>
 …
 exit
!
interface <ID>
 ip access-group <ACL> {in|out}

sh ip access-lists
sh ip int <INT>
```

```
!-------------------------------------
! dot1x
!-------------------------------------
aaa new-model
radius-server host <hostname|ip-assress> [key <string>] !points to server

aaa authentication dot1x default [group radius] local   !Create authentication method list

dot1x system-auth-control !activates global support for 802.1X

int <>
 authentication port-control {force-authorized | force-unauthorized | auto}
 dot1x pae authenticator
 [dot1x host-mode {single-host | multi-host}] !in multi-host mode only one host need to authenticate on port


Note: For switches running Cisco IOS version 12.2(50)SE or later, the dot1x port-control auto command is replaced with the following interface-level commands:
authentication port-control auto
dot1x pae authenticator

sh dot1x int <>
```

```
!-------------------------------------
! Port ACL (PACL)
! Two types (IP/MAC)
! Port ACL applies to L2sw port direction IN
! - can filter on L2/3/4 information
!-------------------------------------
     int <>
      access-group mode [prefer port | merge]

     !-------------------------------------
     ! IP ACL
     ! ! - can filter on L3/4 information
     !-------------------------------------
     ip access-list [standard | extended | numbered] <NAME | number>
      …
      exit
     !
     interface <>
      ip access-group <ACL> in

     !-------------------------------------
     ! MAC ACL
     ! ! - can filter on MAC (L2) information
     !-------------------------------------
     ip access-list extended <NAME>
      permit host [<source MAC> | any] [<destination MAC> | any
      exit
     !
     interface <>
      mac access-group <ACL> in
```

```
!-------------------------------------
! SPAN Sniff traffic on a switch
!-------------------------------------
monitor session 1 source int fa 0/1
monitor session 1 destination int fa 0/10

!-------------------------------------
! RSPAN (Remote SPAN)
!-------------------------------------
Sw2:
vlan 50
name RSPANname
remote-span

monitor session 2 source int fa 0/24
monitor session 2 destination remote vlan 50

Sw1:
vlan 50
name RSPANname
remote-span

monitor session X destination int fa 0/10
monitor session X source remote vlan 50
```