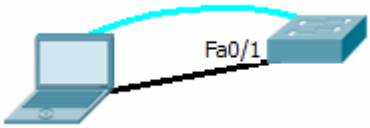
COMPUTER NETWORKS - LABORATORY 022

Subject:

Configuring Cisco Catalyst switch services
Spanning Tree Protocol
EtherChannel

Task A: Setting up communication channels to the Cisco Catalyst switch – enabling telnet and SSH servers

1. Connect the PC station with Cisco Catalyst ethernet switch (models 2950, 2960, 3550, 3560, 3750, 3850 or 3950) using twisted pair cable via selected ethernet port. Install the console cable between the devices.



Activate privileged mode (exec) on switch CLI (the *enable* command)
Then go to config mode using the terminal:
Switch>enable
Switch#
Switch#configure terminal
Switch(config)#
To establish an IP connectivity you must configure the IP address of the VLAN1 interface (assuming VLAN1 to be the administrative VLAN). Before you set up the address - check (ping), if it is not used by any other device on the local network:
Switch (config)#interface vlan1
Switch (config-if)#ip address 192.168.123.199 255.255.255.0
Switch (config-if)#no shutdown
IP addressing for all used interfaces must be defined independently meeting the generally known rules (do not copy the example above literally).
Check the switch IP interfaces:
Switch # show ip interface brief
Switch # show ip interface vlan 1

or in configuration mode:
Switch (config) #do show ip interface brief
Switch (config) #do show ip interface vlan 1

2. Enabling a Telnet server.
Setting up the virtual terminal server and launching telnet console.
Cisco Catalyst switches allow remote telnet or SSH CLI access through virtual

terminals VTY (there is usually 16 terminal lines available). When a remote user connects to the switch (via telnet) – the switch allocates to him on one of VTY lines. To configure switch for such connections you must specify the following commands:
Switch (config)#line vty 0 15
Switch (config-line)#password netpass
Switch (config-line)#login
Switch (config-line)#transport input telnet
Where these following entries are:

- Activating the VTY configuration mode (for line range 0-15)
- The establishment of a local password
- The establishment requesting a use of local password at login
- Permitting a telnet traffic

Note: The login command will be blocked when the switch has authentication mode type of new-model (integrated) enabled. Check that in your config and change if needed:
Switch #show run
...
aaa new-model
...
Switch (config)#no aaa new-model

Check a remote Telnet session from a PC to the switch (use any king of telnet client software, like Putty, connect to the switch IP address. The switch address is just an IP address of VLAN1 interface. TCP port for a telnet service has it's standard value: 23.

3. Authentication
In order to proceed privileged EXEC mode of CLI using telnet or SSH service (that's a remote connection) it is necessary to define the switch 'enable' password (logons without that password are allowed only for local connections via console):
Switch (config) #enable password pass
To remove the password use:
Switch (config) #no enable password

Check the final configuration:
Switch # show running-config
and reconnect via telnet switching to exec with 'enable' command.

4. Reconfiguring to SSH mode:
To have the SSH server operational you need to provide hostname data and user-level authentication mechanism

Specify the Internet domain name for the switch:
Switch(config) #ip domain-name domain

Change the switch hostname to other than default:
Switch(config) #hostname Mojhost

Changing the host name will modify the prompt. From now the switch will print it's name instead the default. Hostname (as the name of the device) is also propagated through the network, including CDP (Cisco Discovery Protocol) and more.
Generate RSA key and entering the key size (360-2048 bits)
Note: "Putty" SSH Client requires a key length of 512 bits:

Switch(config)#crypto key generate RSA
Check the settings:
Switch#show ip ssh

Switch user authentication mode from the "AAA Radius server" (which is the default) to use the local system account:
Switch(config)#AAA new-model
Caution: this command blocks previously written command:
Switch(config-line)#login
(authentication using single password assigned to the line is no longer available)

Define at least one user with some loginname and password:
Switch (config)#username u1 priv 15 password 0 pass
Where 0 determines a password security (value 7 means encrypted password), and 15 is the priority value assigned to that user (the highest right now).
Activate the lines to use SSH:

Switch (config) #line vty 0 15
Switch (config-line) #transport input ssh

or:

Switch (config) #line vty 0 15
Switch (config-line)#transport input all

Connect to the switch using any SSH client (eg. Putty on the PC station) validating the operation of this service (TCP SSH port has a default value of 22).

5. Restricting the access:
   It is possible to reduce the access only for certain IP addresses.
   Create the filter rule in ACL (Access Control List) system - the example below is defined for list number 55:
   Switch (config) # access-list 55 permit 192.168.1.0 0.0.0.255
   Then apply this rule to some selected lines:
   Switch (config) #line vty 0 15
   Switch (config-line) # access-class 55 in
   Switch (config-line) #exit
   Note: In the definition used above the filtering ACL rule will use a value of the IP address mask written in a bit inversion (0.0.0.255 would be the mask of 255.255.255.0).
   Reconnect to the switch using SSH client and verify the operation of restrictions set.

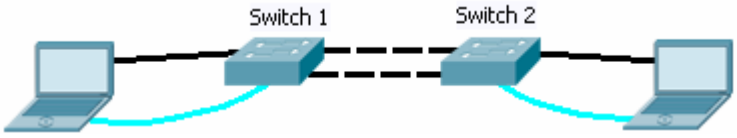
Task B: Spanning Tree Protocol

1. STP (Spanning Tree Protocol) eliminates loops in the network segments based on Ethernet is implemented in the most advanced Ethernet switches. It defines one switch to be a root bridge. Each of remaining switches does not have a root status and is looking for possible links to the root bridge, applying them into a tree structure (Spanning Tree). Then it deactivates all redundant links to the root – avoiding loops. Additionally
2. Prepare two Cisco Catalyst Ethernet switches and connect them both together with an Ethernet cable.

To check a status of spanning tree constructed by these switches (including the status of the root bridge, the BID value, BPDUs /bridge protocol data unit/ or ports) use the commands:
Switch # show spanning-tree
Switch # show spanning-tree detail
Switch # show spanning-tree vlan 1-10
Check respectively on both switches:

- the status of the root bridge,
- *root ID* (determines the root bridge – could relate to the current switch or another, the root bridge)
- *bridge ID* (specifies the current switch STP information)
- *root port*
- *designated ports*

Then add a second Ethernet connection between switches (causing a physical loop in topology).



After waiting until the Spanning Tree rebuilds, check both switches again, identifying:

- *root bridge*
- *root Port*
- *designated ports*
- *alternative ports*

3. Once a connection is established between the switches shut one of the links down:

Switch (config)#interface fa 0/5
Switch (config-if)#shutdown

and analyze the situation again.
Restarting the activity of the port:
Switch(config-if) #no shutdown

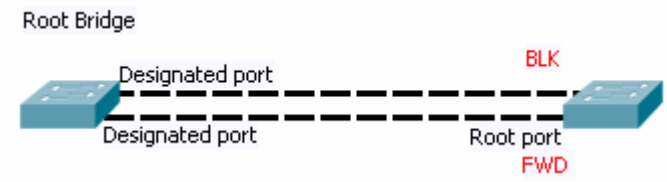
To run diagnostics on the STP in real time, issue the command:
Switch#debug spanning-tree events
(then remove link causing some changes).
To stop diagnostics:
Switch #no debug spanning-tree events

4. The Cisco switches will operate by default in the per-VLAN STP mode (there is a separate Spanning Tree instance for each VLAN). Even if VLANs are not configured, there is always VLAN1 available, which may be used by STP.

5. To transfer the status of the STP root bridge in some VLAN to your own switch use the command:
Switch (config) # spanning-tree vlan 1 root primary
This command will change the value of the STP switch priority that will be been the best in it's environment. Another variant of this command:
Switch (config) # spanning-tree vlan 1 root secondary
It specifies the priority as a "second best" - taking over the root function when the current root bridge fails.
Move the status of the STP root bridge to some other switch and back,observing results - check the status of STP:
Switch # show spanning-tree
Switch # show spanning-tree summary
Switch # show spanning-tree vlan 1 detail
Switch # show spanning-tree detail int fa 0/1

6. Another method to change the spanning tree settings is direct manipulation of the switch (bridge) priority. As you know - switch itself defines the priority of the BID (bridge ID) and sends it in BPDU - but you can define the value of the four highest bits of this BID manually:
Switch (config) # spanning-tree vlan 1 priority 16384
The default priority value is 32768.
Switch must return the root status bridge if better (superior) BPDU arrives.
It is possible to block the loss of root bridge status in this switch through some links (only with cutting all communications in these ports as an result of receiving superior PBDU):
Switch (config-if) # spanning-tree guard root
Cause that behavior upgrading the root bridge priority (as before) in the opposite switch. Check if there was a collision between the root bridge switches (root inconsistency) and, consequently the port configured with guard root option has been blocked (status: broken - BKN):
Switch # show spanning-tree vlan 1
Switch # show log
Note: In the current configuration attempt to take over the status of the root bridge still succeeds, because a second connection between switches remains in the system. It will be activated after first link was locked.

7. Changing the value of port priority:
   To force the choice some particular link from many available (alternative connections to the toot bridge) between two switches it is necessary to manipulate priorities of ports ports or links. The default value of the port priority is 128, granulation -16.



   Port priority value is transmitted through the BPDU frame to another switch, which will be looking for the best path to the root bridge and will make decision which link to use. Therefore, in order to check that, you must configure the port priority of the root bridge (priority information will be sent to another switch), which selects the proper link:
   Switch (config)#int fa 0/1
   Switch (config-if) # spanning-tree port-priority 64
   or only for a specific VLAN (and port):
   Switch (config)#int fa 0/1
   Switch (config-if) # spanning-tree vlan 1 port-priority 64
   With the the command above, change the priority of second active link. Check the effect again of both switches:
   Switch (config) #show spanning-tree
   Note: Reported port-priority includes values only being sent, but not values received (so your port-priority change will only be seen on root bridge). To check the second switch port priority value, use the command:
   Switch (config) #show spanning-tree vlan 1 detail

8. Modifying the cost value.
   Port-priority parameter discussed in preceding paragraph is meaningful only in a situation where the STP instance calculated sums of route costs on links to the root bridge the same. Value of that cost depends on a speed of the link. The default values for 16 bit variant of cost are: 100 = 10Mbps, 19 = 100Mbps, 4 = 1Gbps, 10Gbps = 2. We can modify that value (for the segment directly connected to the switch) locally:
   Switch (config) #int fa 0/1
   Switch (config-if) # spanning-tree cost 13
   or for a specific VLAN and port only:
   Switch (config) #int fa 0/1
   Switch (config-if) # spanning-tree vlan 1 cost 13
   A lower cost wins.
   Change the activity of existing links by changing it's costs. Check the effect in both switches:
   Switch (config) #show spanning-tree

9. Versions of the STP.
   In Rapid version active STP switch prepares a ready-to-activate link backup. To change between versions use these commands
   Switch (config) # spanning-tree mode PVST
   or

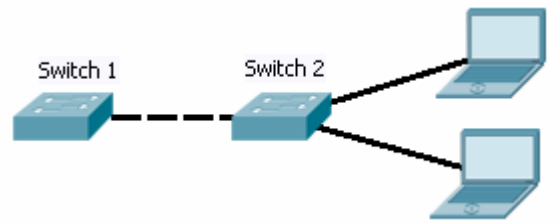
Switch (config) # spanning-tree mode rapid-PVST
where PVST means per-VLAN spanning tree.
Checking the active version (see entry in a report about the content of "ieee compatible STP" or "rstp compatible STP"):
Switch # sh spanning-tree detail

10. To turn the operation of STP off (in the switchport), use:
Switch (config) # spanning-tree portfast default
To disable STP only for some physical switch port:
Switch (config-if) # spanning-tree portfast

NOTE !: When topology loop occurs on some switch ports (not implementing STP) loop may cause the broadcast storm.

Task C: MAC address filtering.

For these experiments build a system similar to shown below, where packets sent from PC host to Switch 1 will be filtered by Switch 2.



In Layer 2 switches is not possible to assign ACL (Access Control List) rules to Ethernet interface. However, you can define a global table of MAC addresses and the rules filtering incoming traffic against these addresses:
Switch (config) #mac address-table static 0013.72b9.89fe vlan 1 drop
or (depending on the version of IOS)
Switch (config) # mac-address-table static 0013.72b9.89fe vlan 1 drop
where 1 is a VLAN identifier (in the example it would be of the default VLAN)
Check the function of this restriction, then restore movement.

I you want to see standard switch MAC address table (all addresses acquired by the switch), use:
Switch1 # show mac-address-table

It is possible to define your own (any) MAC (assigned to VLANs), defining a static MAC address for the port and the VLAN1:
Switch2 (config) # mac-address-table static int 1111.2222.3333 vlan fa0 1/5
Check the MAC table again.

Task D: Port aggregation – the EtherChannel

1. The task is to aggregate (combine together) multiple switch ports - forming to one logical link. Such link can be established between switches and it will allow us to

multiply the bandwidth. To create an EtherChannel you must define its identical configuration in both switches.

2. EtherChannel links in these switches must include (in a logical link) the same number of Ethernet ports of the same hardware kind each. Connect up to four cables as shown below:

In both switches define a new type of interface: port-channel, representing a logical aggregation of Ethernet ports:
Switch (config) #interface Port-channel 1
Check the configuration:
Switch #show ip int brief
Change a mode of ports planed to be aggregated in EhterChannel to access:
Switch (config-if) #switchport mode access

3. Before assigning switch ports to the EtherChannel - temporarily disconnect it from the opposite switch.
Caution: When link is configured to EtherChannel only on one side, it catches mis-config of the EtherChannel (the other side is not yet configured) and with this inconsistency if permanently turns off going to err-disabled state.
4. Assign selected ports to so-called “channel-group”:
Switch (config) # interface range fa0/1 - 4
Switch (config-if) #switchport mode access
Switch (config-if) # channel-group 1 mode on
wherein the channel group must be identified by a number (in the example is 1) the same as previously defined interface Port Channel (coincidence of this value of the coupling between a group of ports and interface). After you configure the port assignments - connect cables switches back to watching the process of compiling EtherChannel.

5. Check the configuration and status of EtherChannel
Switch#show etherchannel summary
From connected PC ping another PC (after setting the IP configuration properly)
Then disconnect one of the cables in EtherChannel and re-check status of the link.
Switch (cross) two another cables and check connectivity again.
Note: that after reconnection STP learning procedure takes does not take extra time anymore. The L2 link is defined as an EtherChannel now, not a physical wire.
Check the status of the active STP instance:
Switch # show spanning-tree
EtherChannel should be listed as Po1, where 1 is the number of channel-group. A cost should also be visible – calculated for whole channel-group.
Remove another cable and check the cost again.

General troubleshooting:
Switch # debug etherchannel
In case of problems with EtherChannel (misconfig, errors) switch it off and on again:

Switch (config-if) #shut
Switch (config-if) #no shut

Task E: Other basic setup commands for Cisco Catalyst switches

1. When you misspell the command in exec mode, the switch considers unknown commans as a hostname and searches for it. It then determines IP address of thet host, waiting for DNS system and blocking the console. In order to remove that behavior, use the command:
   Switch (config) #no ip domain-lookup

2. Define the host name for the switch:
   Switch (config) #hostname s0
   where s0 is a new switch host name.

3. Checking the current configuration of the switch:
   Switch # show running-config

4. Saving the config to FLASH memory:
   Switch # write memory

5. Deleting config stored in FLASH memory:
   Switch# write erase

6. Debug mode (messages from processes typed here wll be printed out in real time):
   Switch # debug ip icmp
   Disabling a debug:
   Switch # no debug all

Task F: Management of the switch via the Web

1. Turn on your web browser (PC), define an IP address in interface VLAN 1, connect your PC to that VLAN and navigate to that IP.