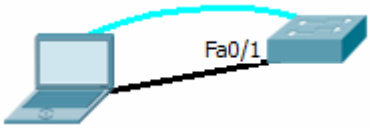
COMPUTER NETWORKS - LABORATORY 021

Subject:

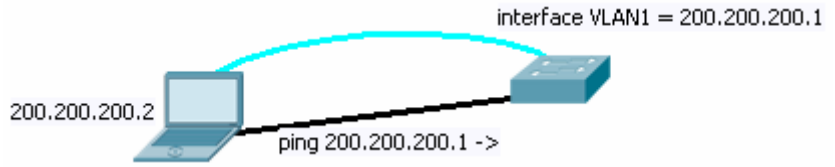
Configuring Cisco Catalyst L2 switches.
Dynamic Trunking Protocol.
Trunks, VLANs

Task A: The basic configuration of the Cisco Catalyst switch

1. Connect the PC station with the Ethernet switch Cisco Catalyst 2950, 2960, 3550, 3560, 3750, 3850 or 3950 using twisted pair cable and selected Ethernet ports. Install the console cable between the devices.



2. After receiving the CLI prompt, activate privileged mode (exec) CLI switch – with enable command (abbreviation: en).
3. Then go to switch configuration mode (using the terminal):
   Switch # configure terminal
   Switch (config) #
4. In the non-routing switch (or Layer 2 or L2 switch) the IP-enabled network interface can be defined only once – in Cisco case, directly - as an IP interface. This functionality is used only for administrative purposes (for example, via telnet connections, HTTP or SSH it's possible to configure the switch). IP addresses can not be assigned to the physical switch ports, since these are only L2. The only IP interfece is in fact virtual, and associated with one of VLANs, defined in the switch. VLAN is a collection of switch ports, selected by the administrator. Individual VLAN ports are isolated - communication between the Ethernet ports belonging to different VLANs is not possible. VLANs are numbered. A default VLAN (all switch ports are classified in it by default) is VLAN1. Since the interface VLAN could also have a number, we can assign that interface (having an IP address) to proper VLAN – by keeping the same number.
5. Configure the IP address of the VLAN1 interface and activate the interface.
   Switch (config)#interface vlan1
   Switch (config-if)#ip address 200.200.200.1 255.255.255.0
   Switch (config-if)#no shutdown
   Interface VLAN 1 can be used to communicate with outside network only via switch ports assigned to VLAN1.
   Configure an IP address of PC workstation connected to the switch via a port assigned to VLAN1 - IP addressing for all the interfaces used in a one segment of the IP network must meet generally known rules. For example, with the mask of 255.255.255.0 it may look like this:

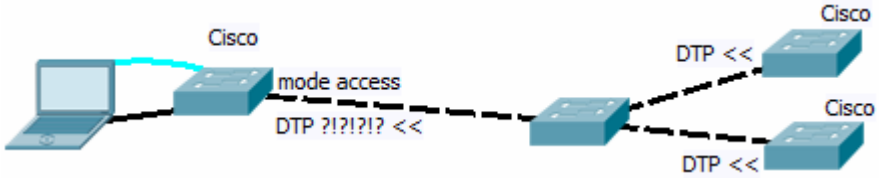


Note: If none of the physical Ethernet ports assigned to some VLAN (VLAN1 for example) is able to forward packets (none is in Forwarding state) the interface VLAN goes to down state. It is therefore necessary to connect at least one device (eg. PC station) to the ports of the switch assigned that VLAN.

6. Configuring the port mode of the port in the switch.
Each switch port can operate in one of three modes imposed by the administrator: access (port leading to DTE), trunk (port leading to another DCE), dynamic (negotiated mode automatically - depending on the type of device on the other endpoint). The selected mode depends on the type of Ethernet framing, which is used in the link (IEEE 802.3 or IEEE 802.1Q). DTE mode (for access mode) can be set with command:

Switch (config) #interface fa0/5
Switch (config-if) #switchport mode access

where fa 0/5 is a shortened identifier of Fast Ethernet port number 5 located directly in the switch chassis (number 0 indicates that). Identifiers in case of Cisco Catalyst switches are mostly 'fa' for Fast Ethernet or gi for Gigabit Ethernet ports. Dynamic port mode is selected by default. Cisco, to identify the type of port on the other side of the cable, uses a DTP (Dynamic Trunking Protocol) protocol. It does that, even if you have chosen other than the dynamic mode of port (in case of sudden change to dynamic mode by the administrator).
Caution! - it is not possible to use the DTP protocol in a mode other than the dynamic, when link goes to multiple Cisco switches at the same time (for example, through a non-Cisco switch, which does not support DTP):



Incoming (contradictory) DTP messages will make impossible to determine the mode of operation, since the switch cannot negotiate it (lack of an active dynamic mode). VTP domain (VLAN Trunking Protocol) of the switch will also interfere with another switch. The port will then be turned off and we'll see this message:
% DTP-5-DOMAINMISMATCH: Unable to perform negotiation on trunk port Fa0 / 5 because of the VTP domain mismatch.
To permanently turn off DTP for the port, and solve that problem, use the command:
Switch (config) #interface fa0/5
Switch (config-if) #switchport nonegotiate

7. Check the settings of 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

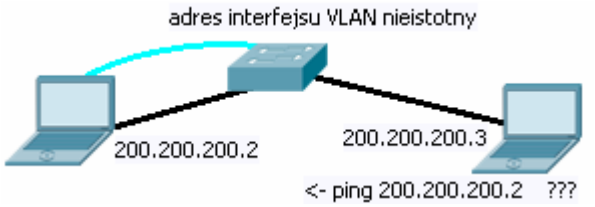
Task B: Configuring VLAN Cisco Catalyst

1. Check the current state of the database VLAN on the switch:
   Switch # show vlan
2. Create two new VLAN on selected numbers:
   Switch # conf t
   Switch (config) #vlan 20
   Switch (config-vlan) #exit
   Switch (config) #vlan 21
   Note: Manual modification of the switch port VLAN is not available in VTP CLIENT mode (VTP is VLAN Trunkig Protocol). In case of refusal, change the VTP mode:
   Switch (config)#vtp mode transparent
3. Assign individual ports to the newly created VLAN, for instance:
   Switch (config) #interface fa0/2
   Switch (config-if) #no shutdown
   Switch (config-if) #switchport mode access
   Switch (config-if) #switchport access vlan 20

   The assignment of such ports will be removed from previous VLAN at the time. In case of problems with port negotiations caused by DTP – turn off DTP operation for Ethernet port:
   Switch (config) #interface fa 0/2
   Switch (config-if) #switchport nonegotiate
4. Assign new VLAN ports using another method - by activating and configuring the entire range of ports at the same time:
   Switch (config) #interface range fa0/15 – 17
   Switch (config-if-range)# switchport mode access
   Switch (config-if-range) #switchport access vlan 20

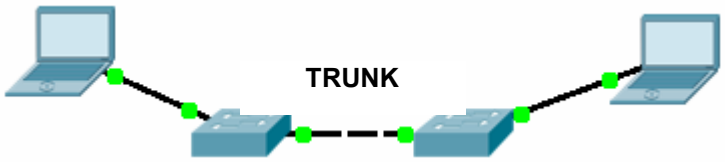
   Please note that the content of the above sample phrase "15 - 17" must be applied space keys.
5. Check previous (now deprecated) VLAN management method (this mode may not be available in some switches): Enter the command (in exec):
   Switch # vlan database
   and check the options available in VLAN Edit mode.
   Then exit editing the VLANs:
   Switch (vlan)#exit
6. Check (ping) the ability to communicate between two PC stations – via switch ports belonging to two different VLAN, and in the second case - assigned to only one VLAN.
   For this purpose:
   - connect two PCs with cables (TP -*Twisted Pair*) to two selected switch ports

- configure IP addressing both PC stations so that they are in the same IP network (in accordance with generally known principles)
- call *ping* from one PC to another (also check the ability to communicate between the switch and PCs)



Task C: Creating tagged VLANs and VLAN trunks in Cisco Catalyst

1. VLAN trunks (using IEEE 802.1Q) enables us to create VLANs that spans multiple switches. Each VLAN can be built locally but also forwarded to other switches via special links called trunks. To do that - a system of tagged frames of IEEE 802.1Q protocols must be involved. It allows a single physical connection between switch ports (trunk) to forward multiple VLAN traffic, and keep it isolated between VLANs.
2. Prepare two PC stations and two switches. connect these switches with each other via Ethernet twisted pair RJ45 crossover cable. This cable will be used to communicate simultaneously between several VLANs. Connect PC Stations one to each switch.



3. In both switches configure ports leading to another switches as trunk ports (in the example is fa0/1)
   Switch (config) #interface fa0/1
   Switch (config-if)#no shutdown
   Switch (config-if)#switchport mode trunk

   Normally, each switch port is in dynamic mode, which adapts automatically to the operating mode port of the opposite side, using the DTP (Dynamic Trunking Protocol) protocol.
   Note: Some switches (eg. The Catalyst 3550) need to explicitly point the type of encapsulation used by the port in a trunk mode (there are many) - as IEEE 802.1Q (before it is possible to run a trunk port mode):
   Switch (config-if)#switchport trunk encapsulation dot1q

4. In the next step select VLANs allowed to communicate with the trunk:
   Switch (config-if)#switchport trunk allowed vlan 1-100
   Caution: This command works with some delay.

Deleting that authorization:
Switch(config-if)#switchport trunk allowed vlan remove 10

5. Check the resulting configuration checking whether the port is classified as a trunk or not:
   Switch # show running-config
   Switch # show interface trunk
   Switch # show interface fa0/1 switchport
   Switch # show interface fa0/1 status
6. Notice that trunk port the port has been removed from all VLANs (now serves as a special port, instead of an access port):
   Switch # show vlan
7. After you configured both switches check communication
   - between two PC stations connected to the same VLAN
   - between two PC stations connected to different VLAN
   - between PC and a closer switch
   - between PC and another switch left
8. Native VLANs
   The switch port configured as a trunk is used for traffic transmitted over the link IEEE 802.1Q encapsulation. But at the same time for one of the specified VLAN it is still possible to transfer traffic in native mode (without IEEE 802.1Q encapsulation). Such traffic in the trunk is approved and is considered as a native VLAN traffic (by default it's VLAN1). The selection of native VLAN number in a switch port can be don with a command:

   Switch (config) #int fa 0/1
   Switch (config-if) #switchport trunk native vlan 10
   Note: In both of interconnected switches, the native VLAN configuration must be compatible (the same number of native VLAN must be elected)
   Verification:
   Switch # show interface fa 0/1 trunk
   or
   Switch # show interface fa 0/1 switchport

Task D: VLAN and VTP (Virtual LAN Trunking Protocol)

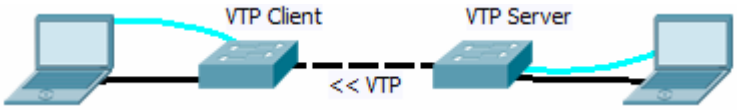
*VLAN Trunking Protocol*It enables automatic VLAN information propagation between switches inside one VTP domain.
Each of the these switches are assigned to the domain and are acting as one of three possible components:

- *server* (which is configured by the user and serves the information to VTP client switches)
- *banner* (which only forwards VTP messages on, but does not update its own VLAN base)
- *client* (which sets up its own VLAN base with incoming the VTP server messages).

Comments:

- to operate properly VTP switches must support VTP (other vendor product or other VTP domains wont are usually not compatible)

- when the switch joins the VTP domain, it automatically downloads a base of existing VLANs from the domain. It's previous VLAN base will be lost!
- link (switch ports) used to transmit information within the VTP must be configured as trunks:
  Switch (config-if) #switchport mode trunk
  Switch(config)#show int fa0/1 switchport
- Both switches must be configured the same VTP domain name, eg .:
  Switch (config) #vtp domain mydomainname
  Caution! VTP domain name used in the experiment must be unique between lab stations.
- There must be only one VTP server in a domain
- Devices participating in VTP can be protected by password:
  Switch (config) #vtp password somepass
  If the passwords in the VTP client and the server are incompatible, the switches will have incompatible MD5 hash codes (calculated on the basis of passwords and later needed to encode/decode messages VTP). Consequently, the VTP will not work.
- In case of other errors VTP revision number could be vital. Try on disabling VTP and re-enabling it with erased revision number.



Check the status of VTP:
Switch # show vtp status
Diagnostics of the VTP:
Switch # debug sw-vlan vtp events

1. Connect Cisco switches (models 2950, 2960, 3550, 3560, 3750, 3850) with TP (twisted pair) or fiber optics. One of them should be configured as a VTP server, the second - as a VTP client.
2. The VTP client must have VTP domain configured with the same name as the VTP server and VTP mode as a client:
   Switch (config) #vtp domain domena
   Switch (config) #vtp mode client
3. To trigger VTP auto update make some changes in a VLAN database:
   Switch(config)#vlan 20
   Switch (config-vlan) #exit
   Switch (config) #vlan 21
   Switch (config-vlan) #exit
   Switch (config) #vlan 22
   Switch (config-vlan) #exit
   Note: Change propagation will occur VTP only after issuing of the exit command.

   Check the results on another switch.