LAB 4 – Enhancing Switched Network Conceptual Notes

Before beginning our activity let us first discuss basic concepts of VLAN, VLAN Membership (Static & Dynamic) and VLAN Connections (Access link & Trunk link) in detail with VLAN example and learn what VLAN is and what advantages it provides in computer network.

1. What is VLAN

VLAN is a logical grouping of networking devices. When we create VLAN, we actually break large broadcast domain in smaller broadcast domains. Consider VLAN as a subnet. Same as two different subnets cannot communicate with each other without router, different VLANs also requires router to communicate.

Advantage of VLAN

VLAN provides following advantages:-

- Solve broadcast problem
- Reduce the size of broadcast domains
- Allow us to add additional layer of security
- Make device management easier
- Allow us to implement the logical grouping of devices by function instead of location

Solve broadcast problem

When we connect devices into the switch ports, switch creates separate collision domain for each port and single broadcast domain for all ports. Switch forwards a broadcast frame from all possible ports. In a large network having hundreds of computers, it could create performance issue. Of course we could use routers to solve broadcast problem, but that would be costly solution since each broadcast domain requires its own port on router. Switch has a unique solution to broadcast issue known as VLAN. In practical environment we use VLAN to solve broadcast issue instead of router.

Each VLAN has a separate broadcast domain. Logically VLANs are also subnets. Each VLAN requires a unique network number known as VLAN ID. Devices with same VLAN ID are the members of same broadcast domain and receive all broadcasts. These broadcasts are filtered from all ports on a switch that aren’t members of the same VLAN.

Reduce the size of broadcast domains

VLAN increase the numbers of broadcast domain while reducing their size. For example we have a network of 100 devices. Without any VLAN implementation we have single broadcast domain that contain 100 devices. We create 2 VLANs and assign 50 devices in each VLAN. Now we have two broadcast domains with fifty devices in each. Thus more VLAN means more broadcast domain with less devices.

Allow us to add additional layer of security

VLANs enhance the network security. In a typical layer 2 network, all users can see all devices by default. Any user can see network broadcast and responds to it. Users can access any network resources located on that specific network. Users could join a workgroup by just attaching their system in existing switch. This could create real trouble on security platform. Properly configured VLANs gives us total control over each port and users. With VLANs, you can control the users from gaining unwanted access over the resources. We can put the group of users that need high level security into their own VLAN so that users outside from VLAN can't communicate with them.

Make device management easier

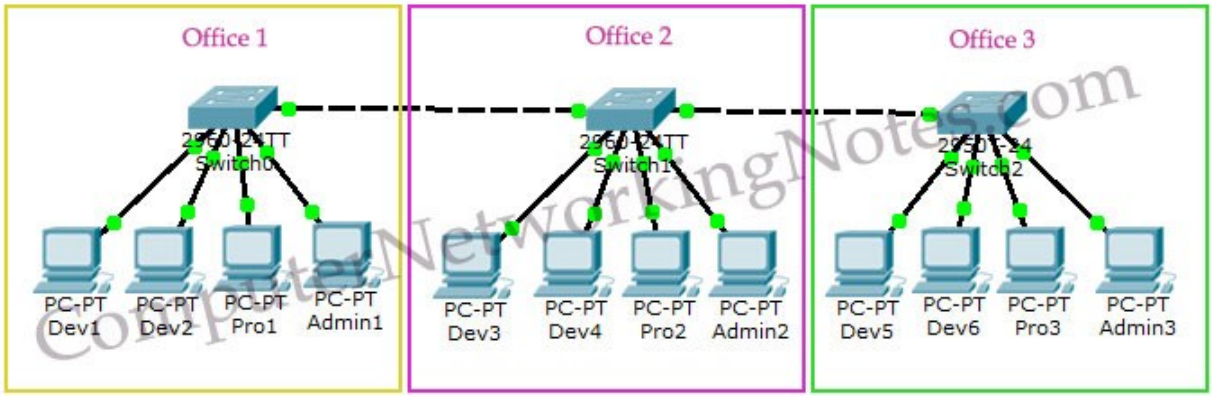
Device management is easier with VLANs. Since VLANs are a logical approach, a device can be located anywhere in the switched network and still belong to the same broadcast domain. We can VLAN. For example our company has a five story building and a single layer two network. In this scenario, VLAN allows us to move the users from one floor to another floor while keeping his original VLAN ID. The only limitation we have is that device when moved, must still be connected to the same layer 2 network.

Allow us to implement the logical grouping of devices by function instead of location

VLANs allow us to group the users by their function instead of their geographic locations. Switches maintain the integrity of your VLANs. Users will see only what they are supposed to see regardless what their physical locations are.

2. VLAN Examples

To understand VLAN more clearly let's take an example.



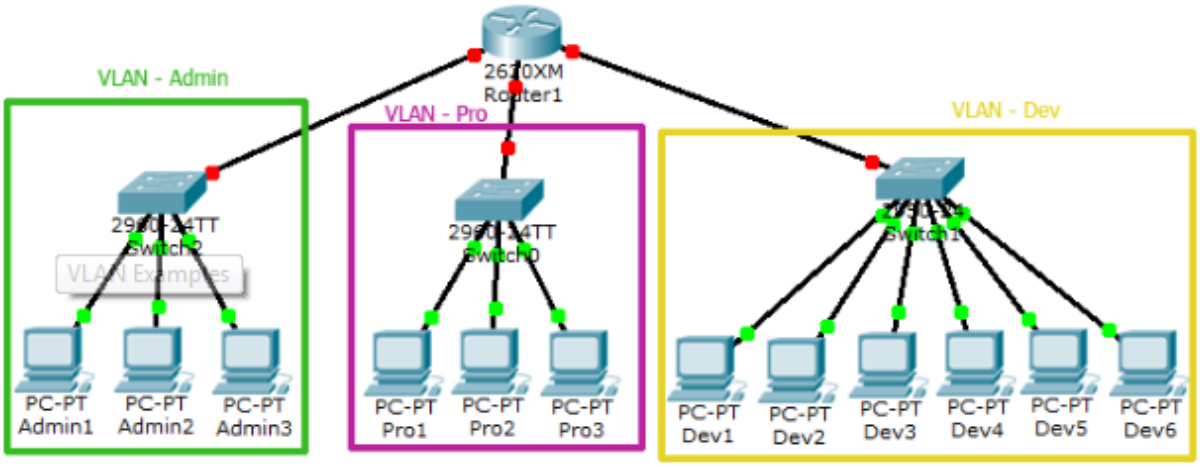
- A company has three offices.
- All offices are connected with back links.
- Company has three departments Development, Production and Administration.
- Development department has six computers.
- Production department has three computers.
- Administration department also has three computers.
- Each office has two PCs from development department and one from both production and administration department.
- Administration and production department have sensitive information and need to be separate from development department.

With default configuration, all computers share same broadcast domain. Development department can access the administration or production department resources.

With VLAN we could create logical boundaries over the physical network. Assume that we created three VLANs for our network and assigned them to the related computers.

- VLAN **Admin** for Administration department
- VLAN **Dev** for Development department
- VLAN **Pro** for Production department

Physically we changed nothing but logically we grouped devices according to their function. These groups [VLANs] need router to communicate with each other. Logically our network look likes following diagram.



With the help of VLAN, we have separated our single network in three small networks. These networks do not share broadcast with each other improving network performance. VLAN also enhances the security. Now Development department cannot access the Administration and Production department directly. Different VLAN can communicate only via Router where we can configure wild range of security options.

VLAN Membership

VLAN membership can be assigned to a device by one of two methods

1. Static
2. Dynamic

These methods decide how a switch will associate its ports with VLANs.

Static

Assigning VLANs statically is the most common and secure method. It is pretty easy to set up and supervise. In this method we manually assign VLAN to switch port. VLANs configured in this way are usually known as port-based VLANs.

Static method is the most secure method also. As any switch port that we have assigned a VLAN will keep this association always unless we manually change it. It works really well in a networking environment where any user movement within the network needs to be controlled.

Dynamic

In dynamic method, VLANs are assigned to port automatically depending on the connected device. In this method we have configure one switch from network as a server. Server contains device specific information like MAC address, IP address etc. This information is mapped with VLAN. Switch acting as server is known as VMPS (VLAN Membership Policy Server). Only high end switch can configured as VMPS. Low end switch works as client and retrieve VLAN information from VMPS.

Dynamic VLANs supports plug and play movability. For example if we move a PC from one port to another port, new switch port will automatically be configured to the VLAN which the user belongs. In static method we have to do this process manually.

VLAN Connections

During the configuration of VLAN on port, we need to know what type of connection it has.

Switch supports two types of VLAN connection

- Access link
- Trunk link

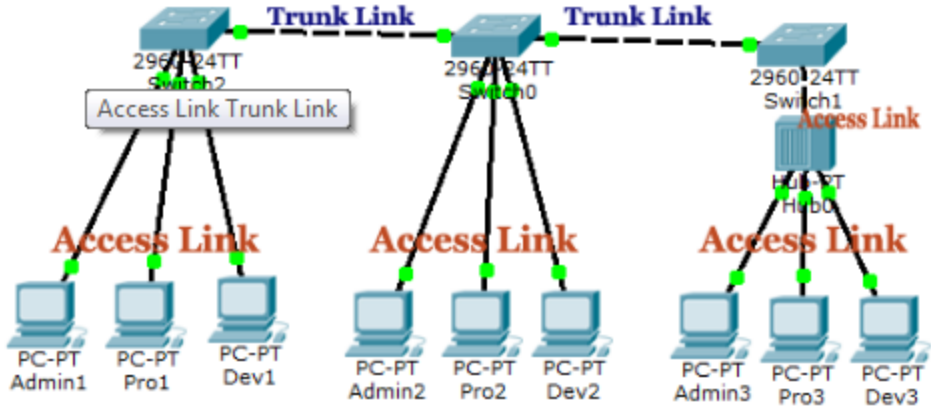
Access link

Access link connection is the connection where switch port is connected with a device that has a standardized Ethernet NIC. Standard NIC only understand IEEE 802.3 or Ethernet II frames. Access link connection can only be assigned with single VLAN. That means all devices connected to this port will be in same broadcast domain.

For example twenty users are connected to a hub, and we connect that hub with an access link port on switch, then all of these users belong to same VLAN. If we want to keep ten users in another VLAN, then we have to purchase another hub. We need to plug in those ten users in that hub and then connect it with another access link port on switch.

Trunk link

Trunk link connection is the connection where switch port is connected with a device that is capable to understand multiple VLANs. Usually trunk link connection is used to connect two switches or switch to router. Remember that VLAN can span anywhere in network, that is happen due to trunk link connection. Trunking allows us to send or receive VLAN information across the network. To support trunking, original Ethernet frame is modified to carry VLAN information.



Trunk Tagging

In trunking a separate logical connection is created for each VLAN instead of a single physical connection. In tagging switch adds the source port's VLAN identifier to the frame so that other end device can understands what VLAN originated this frame. Based on this information destination switch can make intelligent forwarding decisions on not just the destination MAC address, but also the source VLAN identifier.

Since original Ethernet frame is modified to add information, standard NICs will not understand this information and will typically drop the frame. Therefore, we need to ensure that when we set up a trunk connection on a switch's port, the device at the other end also supports the same trunking protocol and has it configured. If the device at the other end doesn't understand these modified frames it will drop them. The modification of these frames, commonly called tagging. Tagging is done in hardware by application-specific integrated circuits (ASICs).

Switch supports two types of Ethernet trunking methods:

- ISL [Inter Switch Link, Cisco's proprietary protocol for Ethernet]
- Dot1q [IEEE's 802.1Q, protocol for Ethernet]

3. Configure VTP Server and Client in Switch

Here we explain basic concepts of VTP Protocol, VTP Domain, VTP Messages and VTP modes (Server mode, Transparent mode and Client mode) in detail

VLAN Trunk Protocol (VTP) is a Cisco proprietary protocol used to share VLAN configuration across the network. Cisco created this protocol to share and synchronize their VLAN information throughout the network. Main goal of VTP is to manage all configured VLANs across the network.

Basic concepts of VTP Protocol

In our network we only have three switches. We can easily add or remove VLAN manually on all three switches. However this process could be more tedious and difficult if we have 50 switches. In a large network, we might make a mistake in VLAN configuration. We might forget to add VLAN on one of the switch, or we may assign wrong VLAN number. Vice versa we may forget to remove VLAN on one of the switch, while removing VLANs.

VTP is a life saver protocol in this situation. With VTP we can add or remove VLANs on one switch and this switch will propagate VLAN information to all other switches in network.

VTP Messages

VTP share VLANs information via VTP messages. VTP messages can only be propagate through the trunk connections. So we need to set up trunk connection between switches. VTP messages are propagated as layer 2 multicast frames.

VTP Domain

VTP domain is a group of switches that share same VLAN information. A switch can have a single domain. VTP messages include domain name. Switch only update VLAN information if it receive VTP message from same domain.

VTP Mode

VTP can be configured in three different modes.

1. Server
2. Transparent
3. Client

VTP Server Mode

VTP Server can add, modify, and delete VLANs. It will propagate a VTP message containing all the changes from all of its trunk ports. If server receives a VTP message, it will incorporate the change and forward the message from all remaining trunk ports.

VTP Transparent Mode

VTP Transparent switch can also make change in VLANs but it will not propagate these changes to other switches. If transparent switch receives a VTP message, it will not incorporate the change and forward the message as it receives, from all remaining trunk ports.

VTP Client Mode

VTP client switch cannot change the VLAN configurations itself. It can only update its VLAN configuration through the VTP messages that it receive from VTP server. When it receives a VTP message, it incorporates with the change and then forwards it from remaining trunk ports.

4. VLAN Tagging Explained with DTP Protocol

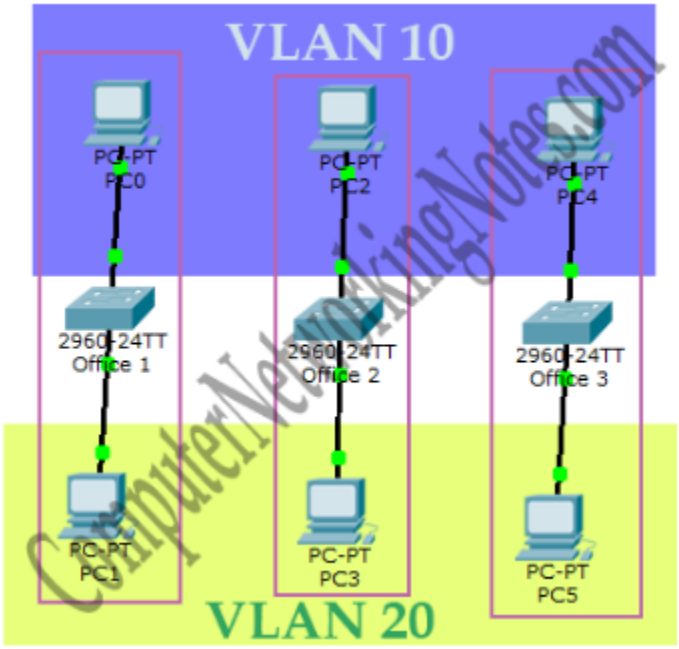
Here we explain VLAN Tagging, VLAN Trunking protocols (ISL & 802.1Q), DTP Modes (ON, DTP Mode Desirable, Auto, No-Negotiate & OFF) and VLAN Trunk configuration in detail.

In VLAN configuration a switch port can operate in two mode; access and trunk. In access mode it can carry only single VLAN information while in trunk mode it can carry multiple VLANs information. Access mode is used to connect the port with end devices while trunk mode is used to connect two switching devices.

Access Link and Trunk Link

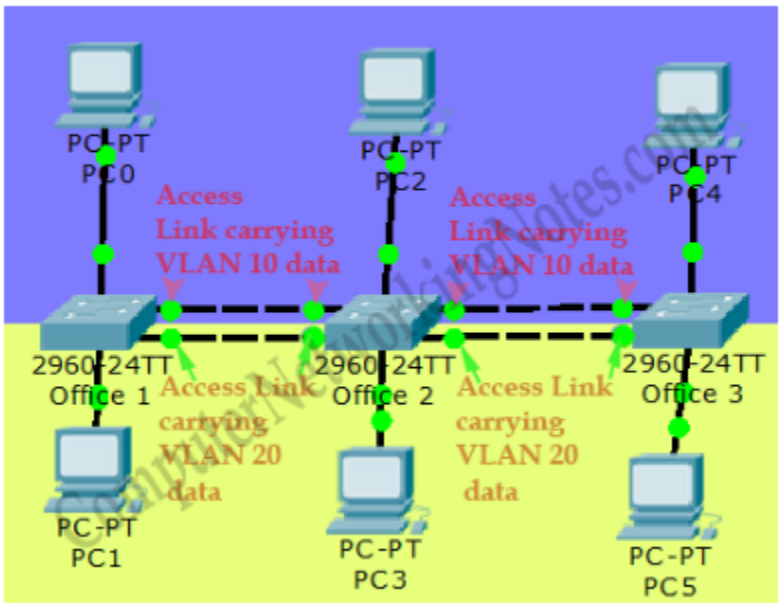
An access link can carry single VLAN information while trunk link can carry multiple VLANs information. Configuring VLANs on single switch does not require trunk link. It is required only when you configure VLANs across the multiple switches.

For example if we do not connect all switches in our network, we do not require to configure the trunk link. In this case PC0, PC2 and PC4 cannot communicate with each other. Although they all belongs to same VLAN group but they have no link to share this information.



Trunk link connections are used to connect multiple switches sharing same VLANs information.

You may think why we cannot use access link to connect these switches. Of course we can use access link to connect these switches but in that case we need to use a separate link for each VLAN. If we have two VLANs we need two links.



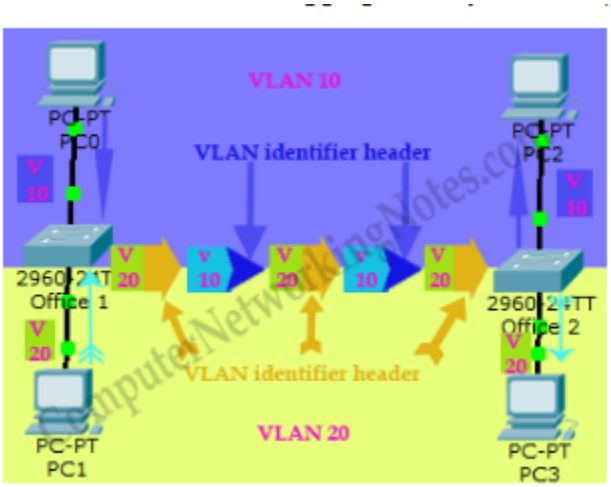
With this implementation we need links equal to VLANs that does not scale very well. For example if our design require 30 VLANs, we will have to use 30 links to connect switches.

In short

- An access link can carry single VLAN information.
- Theoretically we can use access link to connect switches.
- If we use access link to connect switches, we have to use links equal to VLANs.
- Due to scalability we do not use access link to connect the switches.
- A trunk link can carry multiple VLAN information.
- Practically we use trunk links to connect switches.

VLAN Tagging

Trunk links use VLAN tagging to carry the multiple VLANs traffic separately.



In VLAN tagging process sender switch add a VLAN identifier header to the original Ethernet frame. Receiver switch read VLAN information from this header and remove it before forwarding to the associate ports. Thus original Ethernet frame remains unchanged. Destination PC receives it in its original shape.

VLAN Tagging process with example

- PC1 generates a broadcast frame.
- Office1 switch receives it and know that it is a broadcast frame for VLAN20.
- It will forward this frame from all of its port associated with VLAN20 including trunk links.
- While forwarding frame from access links, switch does not make any change in original frame. So any other port having same VLAN ID in switch will receive this frame in original shape.
- While forwarding frame from trunk links, switch adds a VLAN identifier header to the original frame. In our case switch will add a header indicating that this frame belongs to VLAN20 before forwarding it from trunk link.
- Office2 switch will receive this frame from trunk link.
- It will read VLAN identifier header to know the VLAN information.
- From header it will learn that this is a broadcast frame and belong to VLAN20.

- It will remove header after learning the VLAN information.
- Once header is removed, switch will have original broadcast frame.
- Now office2 switch has original broadcast frame with necessary VLAN information.
- Office2 Switch will forward this frame from all of its ports associated with VLAN20 including trunk links. For trunk link same process will be repeated.
- Any device connected in ports having VLAN20 ID in Office2 switch will receive original frame.

Now we know that in VLAN tagging process sender switch adds VLAN identifier header to the original frame while receive switch removes it after getting necessary VLAN information. Switches use VLAN trunking protocol for VLAN tagging process.

VLAN Trunking Protocol

Cisco switches supports two types of trunking protocols ISL and 802.1Q.

ISL

ISL (Inter-Switch Link) is a Cisco proprietary protocol. It was developed a long time before the 802.1Q. It adds a 26-byte header (containing a 15-bit VLAN identifier) and a 4-byte CRC trailer to the frame.

802.1Q

It is an open standard protocol developed by IEEE. It inserts 4 byte tag in original Ethernet frame. Over the time 802.1Q becomes more popular trunking protocols.

Key difference between ISL and 802.1Q

- ISL was developed Cisco while 802.1Q was developed by IEEE.
- ISL is a proprietary protocol. It will works only in Cisco switches. 802.1Q is an open standard based protocol. It will works on all switches.
- ISL adds 26 bytes header and 4 byte trailer to the frame.
- 802.1Q inserts 4 byte tag in original frame.

802.1Q is a lightweight and advance protocol with several enhanced security features. Even Cisco has adopted it as a standard protocol for tagging in newer switches. 2960 Switch supports only 802.1Q tagging protocol.

VLAN Trunk Configuration

We can configure trunking in Cisco switches by two ways statically or dynamically. In static method we need to configure trunking in interface statically while in dynamic mode it automatically done by a DTP trunking protocol.

Dynamic Trunking Protocol

DTP [Dynamic Trunking Protocol] is a Cisco proprietary protocol. It automatically configures trunking on necessary ports. It operates in five modes.

DTP Modes

DTP Mode ON

In ON mode interface is set to trunk, regardless remote end supports trunking or not. On mode cause interface to generate DTP messages and tag frames based on trunk type.

DTP Mode Desirable

In Desirable mode interface will generate the DTP messages and send them to other end. Interface will work as access link until it get replies from remote end. If reply messages indicate that remote device is trunking capable, DTP will change connection link in trunk from access link. If other end does not respond to DTP message, the interface will work as access link connection.

DTP Mode Auto

In auto mode interface works as access link and passively listen for DTP messages. Interface will change connection link to trunk, if it receives a DTP message from remote end.

DTP Mode No-Negotiate

In No-Negotiate mode interface is set as trunk connection. Interface will tag frames but it will not generate DTP messages. DTP is a Cisco's proprietary protocol, thus a non Cisco device will not understand it. This mode is used to trunk connection between Cisco device and a non Cisco device.

DTP Mode OFF

In off mode interface is configured as access-link. No DTP message will be generated nor frames will be tagged.

5. How to configure VLAN VTP DTP cheat sheet

Command	Descriptions
Switch(config)#vtp mode server	Configure Switch as VTP Server
Switch(config)#vtp mode client	Configure Switch as VTP Client
Switch(config)#vtp mode transparent	Configure Switch as VTP Transparent
Switch(config)#no vtp mode Configure	Switch to default VTP Server Mode
Switch(config)#vtp domain domain-name	Set VTP Domain name.
Switch(config)#vtp password password	Set VTP password. Password is case sensitive
Switch#show vtp status	Display VTP status including general information
Switch#show vtp counters	Show VTP counters of switch
Switch(config-if) #switchport mode trunk	Change interface mode in Trunk
Switch(config)#vlan 10	Create VLAN and associate number ID 10 with it
Switch(config-vlan)#name Sales	Assign name to VLAN
Switch(config-vlan)#exit	Return in Global configuration mode from VLAN configuration mode

Switch(config)#interface fastethernet 0/1	Enter in interface configuration mode
Switch(config-if)#switchport mode access	Set interface link type to access link
Switch(config-if)#switchport access vlan 10	Assign this interface to VLAN 10
Switch#show vlan	Displays VLAN information
Switch#show vlan brief	Displays VLAN information in short
Switch#show vlan id 10	Displays information VLAN ID 10 only
Switch#show vlan name sales	Displays information about VLAN named sales only
Switch(config)#interface fastethernet 0/8	Enter in Interface configuration mode
Switch(config-if)#no switchport access vlan 10	Removes interface from VLAN 10 and reassigns it to the default VLAN - VLAN 1
Switch(config-if)#exit	Move back to Global configuration mode
Switch(config)#no vlan 10	Delete VLAN 10 from VLAN database
Switch#copy running-config startup-config	Saves the running configuration in NVRAM

6. Spanning Tree Protocol (STP)

STP is a layer 2 protocol, used for removing loops. For backup purpose we typically create backup links for important resources. In our scenario, all offices have backup links that create loops in topology. STP automatically removes layer 2 loops. STP multicasts frame that contain information about switch interfaces. These frames are called BPDU (Bridge Protocol Data Units). Switch use BPDUs to learn network topology. If it found any loop, it will automatically remove that. To remove loop, STP disables port or ports that are causing it.