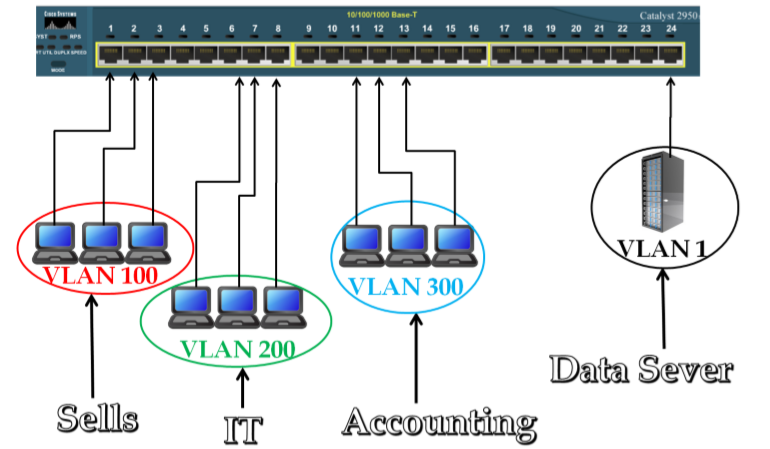
**Introduction**

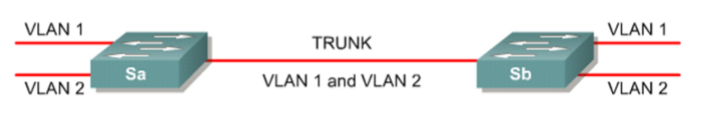
* **What is VLAN?**

Ports on switches may be assigned to one or more VLANs, allowing systems to be separated into logical groups — depending on which department they are affiliated with — and defining guidelines about how systems are permitted to communicate with each other in different groups. Such classes can vary from easy and realistic (computers in one VLAN can see the printer on that VLAN but computers beyond that VLAN can't) to complicated and legal (computers in accounting departments can't communicate with computers in sales departments, for instance).



* **What is TRUNKING?**

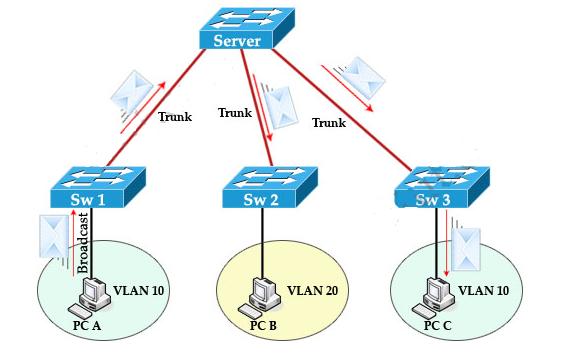
The trunk link can transfer more than one VLAN over a single switch port. Trunk link is very useful when switches are connected to other switches or when switches are connected to routers. No trunk link has been set for a specific VLAN. Alternatively, one or more VLANs or all active VLANs can be transferred between switches using one physical trunk link. It is possible to connect two switches with separate physical connections for each VLAN. Cisco supports TRUNKING on both Fast Ethernet and Gigabit Ethernet links, as well as aggregated Fast and Gigabit EtherChannel links. The role of VTP is to maintain consistency of VLAN configuration across a shared network management domain (VTP domain). To maintain consistency, we must secure VLANs in one switch, and set them up as a VTP server. Other switches act as VTP clients to receive VLAN information. Some switches can be transparent and only forward VLAN information, but they will not join any VLAN in the domain.



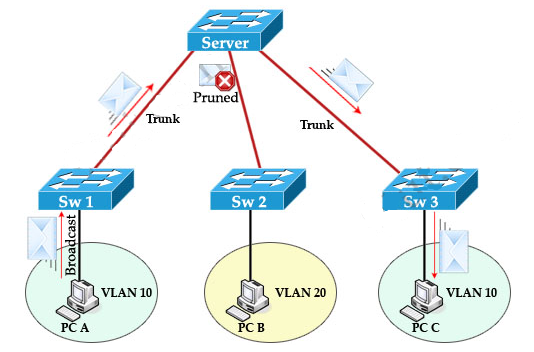
**Future Work**

* **What is VTP Pruning?**

When PC A sends a broadcast frame on VLAN 10, it travels across all trunk connections in the VTP domain. Switches Server, Sw2 and Sw3 receive broadcast frames from Computer A. However, only Sw3 has a user on VLAN 10 and it is a waste of bandwidth on Sw2. Moreover, broadcast traffic also consumes processor time in Sw2. The link between the Server and Sw2 adapters does not carry any VLAN 10 traffic so it can be "pruned".



VTP Pruning increases the efficiency of main section bandwidth by forwarding broadcasts and unicast frames on a VLAN only if the adapter on the receiving end of the trunk has ports in that VLAN. In the example below, the server switch does not send the broadcast frame to Sw2 because Sw2 does not have ports in VLAN 10.



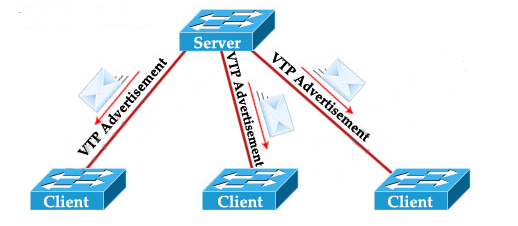
When the switch has a port associated with a VLAN, the switch sends an advertisement to its neighbors to inform it of active ports on the VLAN. For an example, Sw3 sends an advertise to Switch Server to inform it that it has an active port for VLAN 10. Sw2 has not advertised VLAN 10, so the switch server will reduce VLAN 10 on the stem to Sw2.

**Aim of VLANs TRUNKING Protocol (VTP)**

Usually we do not have flat layer in layer 2 network, and it is impossible to put all ports of switches in the same VLAN. So, there may be ways of having the same virtual LAN on different switches that are not directly related to each other. In this case, we need protocol that helps us communicate between these two VLANs. The VLAN TRUNKING protocol creates VLANs on all switches so that even if there is no use of this switch but it can still help in communicating with other switches. The role of VTP is to maintain consistency of VLAN configuration across a shared network management domain (VTP domain). To maintain consistency, we must secure VLANs in one switch, and set them up as a VTP server. Other switches act as VTP clients to receive VLAN information. Some switches can be transparent and only forward VLAN information, but they will not join any VLAN in the domain. VTP sends messages between split switches to keep VLANs on these switches for conversion properly. VTP is a Cisco-owned method for managing VLANs between switches and operating over any type of connection mechanism. VTP allows switches to sync their VLANs based on configuration revision number. VTP can prune unnecessary VLANs from trunk connections. VTP prune allows the switch not to redirect user traffic to inactive VLANs on a remote switch. This property prunes unnecessary traffic through trunk links. If VLAN traffic is needed later, VTP will dynamically add VLAN again to the trunk.

**VTP Methodology and How It Works**

For the switches to share their VLAN information with each other, they need to be configured in the same VTP domain. Only switches that belong to the same domain share their VLAN information. When a change is made to the VLAN database, it is posted to all switches via VTP ads. To maintain domain consistency, only one switch should be allowed to create, delete, or modify the new VLAN. This switch is like the "Head" of the entire VTP domain and is running in server mode. This is the default as well. Other switches are only allowed to receive and forward updates from the "Server" switch. It runs in client mode.



Sometimes, the network administrator does not want to switch to see VTP information from other switches. It can set it to transparent mode. In this mode, the switch maintains its own VLAN database and never learns VTP information from other switches however it still redirects VTP ads from server to other switches. A transparent switch can add, delete, and locally edit VLAN database. VTP ads bring VLAN information to all switches in the VTP domain. Each VTP ad is sent with a review number. This number is used to determine whether a VTP advertisement is later than the current version of this switch. Because every time you change a VLAN in the converter, the configuration review increases by one. So, the higher the review number, the better the VTP ad.

One important thing to know is that when the adapter receives a better VTP ad, it deletes the entire VTP information and copies the new information from the best VTP ad to its VLAN database. The switch is not trying to compare its VLAN database with information from received VTP ads to see and update the difference.

**VTP Modes**

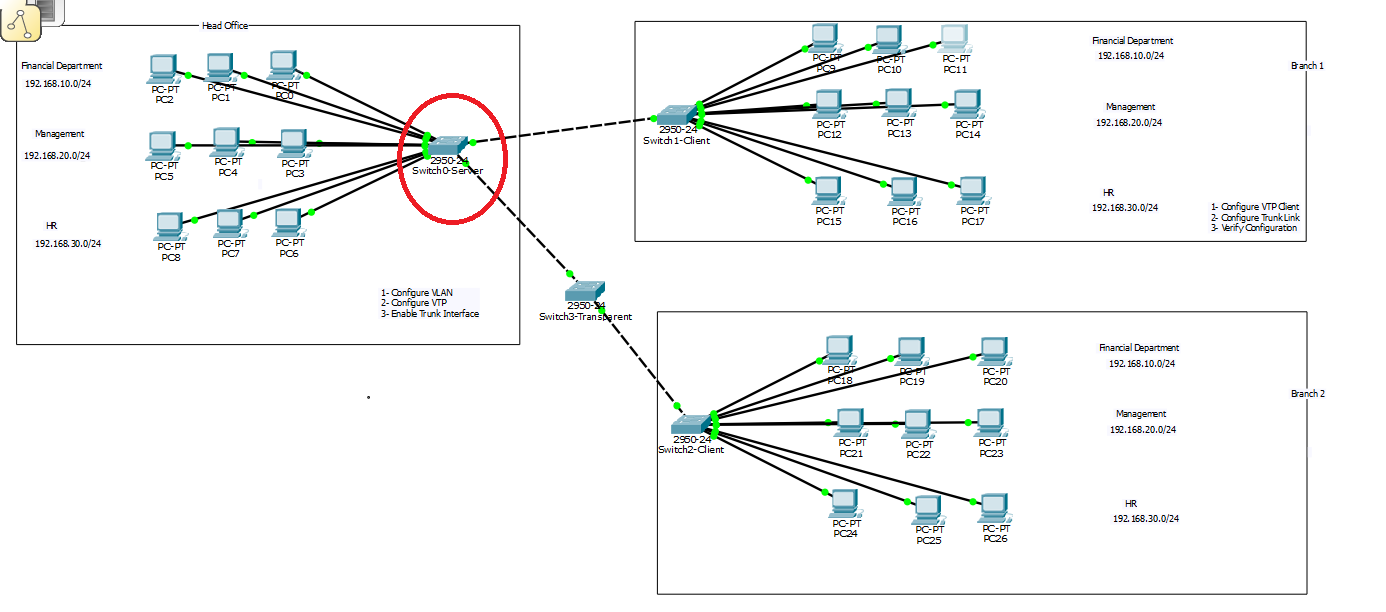
Switches can operate in one of three VTP modes: Server, Transparency, or Client. It is an optional feature. It is used to handle large organization and It does two functions:

1. Centralized management of VLAN, such as: creation, deletion, and modification

2. Controls flow of VLAN on trunk.

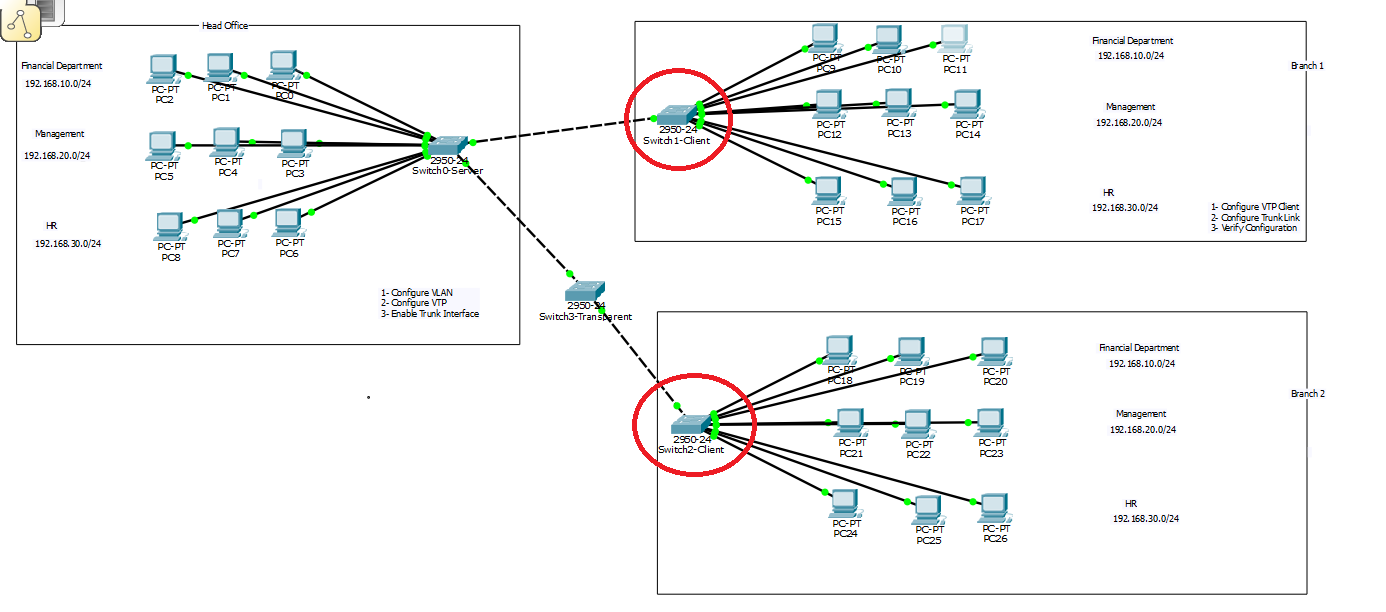
**Server:**

VTP servers have full control over creating a VLAN and modifying its domains. All VTP information was pronounced to switch sisters mostly, while VTP received information synchronized to other switches. By default, the switch is in VTP Server Mode. Note that every VTP domain must have small servers that can be created, modified, formatted, and so that VLAN can be published.

****

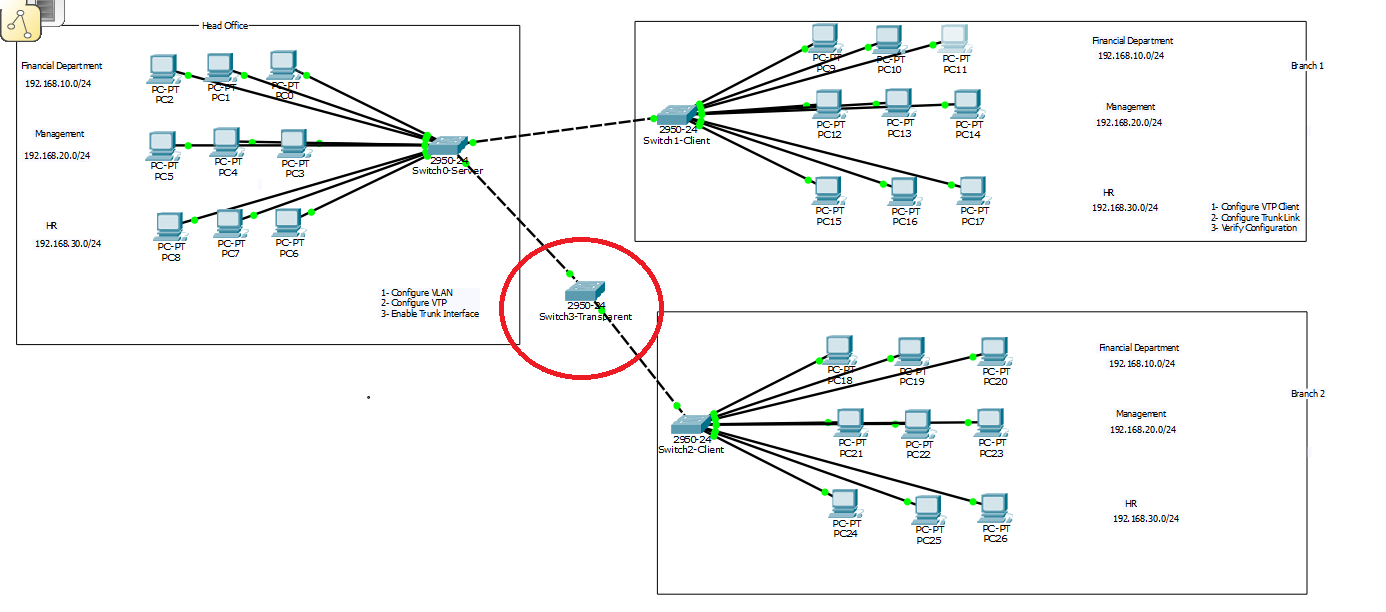
**Client:**

VTP clients do not allow the administrator to create, change, or format any VLANs. Instead, they listen to VTP ads from other switches and adjust VLAN settings accordingly. In fact, this is passive listening mode. VTP information received from the trunk connectors is forwarded to the adjacent switches in the domain.



**Transparent:**

VTP transparent switches are not involved in VTP. While in transparent mode, the switch does not announce its VLAN configuration, and the switch does not sync its VLAN database with the received ads. It is used for private use of the network. Transparent mode does not approve server announcement or client mode.



**Topology**

Both machine and network system are linked to a single cable in **Bus** topology network. This cable has exactly two endpoints and is then called topology for Linear Bus. It just transmits data in one direction. Each device has a single cable connected to it.

**Bus Topology Advantages:**

1. It is efficient.
2. Network topology requires fewer cable.
3. Usage in Small Networks.
4. It is quick to understand.
5. Easy to extend connecting two cables together
6. Easy to setup.

**Bus Topology disadvantages:**

1. The main cable fails then the whole network fails.
2. Where network traffic is high, network performance should decrease.
3. The length of the cable has limits.

**VTP Advantages**

Advantage of VTP is that it does not necessarily require manually adding a new VLAN to every network switch. By adding a VLAN to one adapter, VTP can spread this information to every other network switch, creating a consistent VLAN application. For large switched networks that contain dozens or hundreds of switches, this becomes a very important to help you in the management of your network.

**VTP Disadvantages**

When a new switch is added to the network, it is configured by default without a VTP domain name or password, but in VTP Server mode. If no VTP domain name is configured, it is assumed to be from the first VTP packet it receives. Since the new switch has a 0 VTP configuration review, it will approve any review number as newer and replace its VLAN information if the VTP passwords match.

However, if you want to connect a switch by mistake to the network using the correct VTP domain name and password but the VTP review number is higher than the network currently has, the entire VTP domain will adopt the VLAN configuration for the new switch that is likely to cause VLAN information loss on all switches in VTP domain, which leads to network failures. Because Cisco switches retain VTP configuration information separately from normal configuration, and since this issue occurs many times, it called a VTP bomb.

Before creating VLANs on the switch to be deployed via VTP, you must first set up a VTP domain. A network VTP field is a set of all adjacent switches with matching VTP settings. All switches in the same VTP domain share their VLAN information with each other, and the switch can share only one VTP management domain. Switches in different domains do not share VTP information. Unmatched VTP settings may lead to problems negotiating VLAN trunks, virtual port channels or port channels.

**Conclusion**

It is good for large organizations because it allows multiple VLANs on one link. VLAN TRUNKING Protocol manages a large network by creating VTP modes that help create VLANs without moving to all the switches again and again. It provides ease of management, availability, security.

**References**

(Rouiller, 2003) **:**

|  |
| --- |
|  |
| Rouiller, S. A. (2003). Virtual LAN Security: weaknesses and countermeasures. *available at uploads. askapache. com/2006/12/vlan-security-3. pdf*. |
| Chicago |  |

Link: <https://www.askapache.com/s/u.askapache.com/2006/12/vlan-security-32.pdf>

(Verma & Shriramwar, Security Optimization of VTP Model in an Enterprise VLAN., 2013):

|  |
| --- |
|  |
| Verma, R. O., & Shriramwar, S. S. (2013). Security Optimization of VTP Model in an Enterprise VLAN. *IJECCE*, *4*(3), 950-954. |
|  |  |

Link : <http://ijecce.org/administrator/components/com_jresearch/files/publications/IJECCE_1708_Final.pdf>

(Pappu & Deore, 2012)

Link: https://s3.amazonaws.com/academia.edu.documents/33534263/report.pdf?response-content-disposition=attachment%3B%20filename%3DA\_Seminar\_Report\_On\_VLAN\_TRUNKING\_PROTOC.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=ASIATUSBJ6BAD4VEMO5F%2F20200506%2Fus-east-1%2Fs3%2Faws4\_request&X-Amz-Date=20200506T222433Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Security-Token=IQoJb3JpZ2luX2VjEHQaCXVzLWVhc3QtMSJGMEQCIHtBRCY2KjmxF41qZP1YDoDcND817Fbm0%2FedwyPQHcqhAiBtQ9TsnNCLwDbuB%2FSibagcCrcjq%2FsiUaaao30RovnCByq9Awit%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F8BEAAaDDI1MDMxODgxMTIwMCIM%2FwA7e5H2u%2BObWR3jKpEDzrKETLSDrkEQV8EEJ%2BOSI4ewc%2FD9iQq5FflZSfDLi6aeNHdqW3cG8iyy87B5%2BwvjFiLnYmiXEiM%2BggBl6dNd9iB%2B%2Ff2pp%2FN%2Fb31xq9OIkBJdSgT9BPi5D48S%2FfZld5FUjI%2BK8IvhONE5SPYsktAVnI%2B6W5yiKLw8h4WUeFNTMfUvBIA%2BuMa6OEOXy2MxkgU9XcovEBIpqL1TfjrD05MaJ9gF7Fqn9LlED9taB5vqIF1kmAwE2poZ21QVWAUkJhp9cyRaFH2cCGiXn0Sw3LPo4D%2FDSQ3y3MhEYITRr1T49D7BvGKA%2FuB3JXwSHynCcU5uZcAVXb21jk%2FpyBJbKqVnnlefQ45OgYVFAe5gXnkyLFfgfg32TXmh0PQ%2B38lBrQ4UdGYlkV7CFzWeJjqhRX3Xaw%2FtBAaBe6Y%2FmcEl%2BjOIoSK0BqHdZRqshcVIpCzonoGNpXqbyx8RcKroe9s2Qd8XbpkFE0QdVP1s%2FCE4pnphXQmP2X215PEKhASCqHCOXAVoAphrtxz8LYCucSVWVkQkezUwr6%2FM9QU67AGNmuiS58qsQCpY62%2BH%2BnQ2C4jv13I7xcU%2FzSSZb8NGHwUlGj2hj4x0%2BM50GdTvKnilDIq0D8bBPASWrX4ZL5eNh85XlSQlsIMcoHATSDqi2tmtID%2BhcbFkY19q4qKTCsmKPc4wP6%2B6y6844FFF1BqDZ5cH%2BzyB%2FlBQvjGton%2F1gVShXrxWrarhBeF9Y7peNkltkDsKz1jc2vxRS36SsRhaXtFDjWqrzTiWij0ElusPYft7gyqxEHZwSixAn4uiy2s3w6tds8WAvI88H%2BssjTd2X7Gmebl2TagkfBwppZ0xvyWepJWX97ogzAnUZw%3D%3D&X-Amz-Signature=0c0ff8bd9dde9e3f003aee492d829f65ada8b88428a0b7516bdd89f8cf561da8

(Prasad, Reddy, Amarnath, & Puthanial, 2016):

|  |
| --- |
|  |
| Prasad, N. H., Reddy, B. K., Amarnath, B., & Puthanial, M. (2016). Intervlan Routing and Various Configurations on Vlan in a Network using Cisco Packet Tracer. *International Journal for Innovative Research in Science and Technology*, *2*(11), 749-758. |
| Chicago |  |

Link: <http://www.academia.edu/download/46216748/IJIRSTV2I11237.pdf>

(Thomas & Jyoti, 2012):

|  |
| --- |
|  |
| Thomas, V., & Jyoti, N. (2012). *U.S. Patent No. 8,156,541*. Washington, DC: U.S. Patent and Trademark Office. |
| Chicago |  |

Link: <https://patentimages.storage.googleapis.com/77/64/17/7549dce9682e0a/US8156541.pdf>

(VLAN Trunking Protocol (VTP), 2015)

Link : <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-4SY/config_guide/sup6T/15_3_sy_swcg_6T/vtp.pdf>