



Romel Cabling ▾



[Home](#)

[Home](#) > [My courses](#) > [121 - ITSP2B](#) > [13 Protecting Layer 2 Protocols](#) > [Lesson Proper for Week 13](#)

Lesson Proper for Week 13

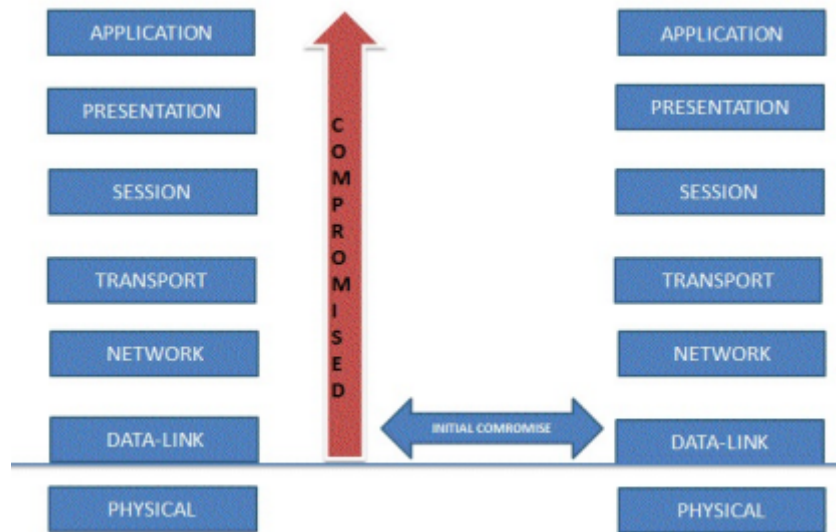
PROTECTING LAYER 2 PROTOCOLS

Traditionally, internal users have been able to connect a PC to a switched network and gain immediate access to enterprise resources. As networks grow and resources become available, it is important to limit the access that internal users receive. More technically, a user from the HR department should have a connection to the port that terminates on their respective desk. Access to switches is a convenient entry point for internal attackers whose intent is to unlawfully gain access to an enterprise network from outside the organization's premises. An attacker can set up rogue access points and protocol analyzers to launch all types of attacks. Switches have various methodologies that secure the access of attackers. Users can be authenticated as they connect and also can be authorized to perform certain configurations on a switch. In addition, Cisco switches can detect and prevent certain types of attacks. Several features can be used to validate information passing through a switch.

1. Layer 2 Attack Mitigation

All layers of TCP/IP have their own security threats and vulnerabilities. Unfortunately, if the lower layer is hacked, communications are compromised without the other layers being aware of the problem. Everything at Layer 3 and higher is encapsulated into some type of Layer 2 frame. If an attacker can interrupt, copy, redirect, or confuse the Layer 2 forwarding, they can also disrupt the functions of the upper-layer protocols:





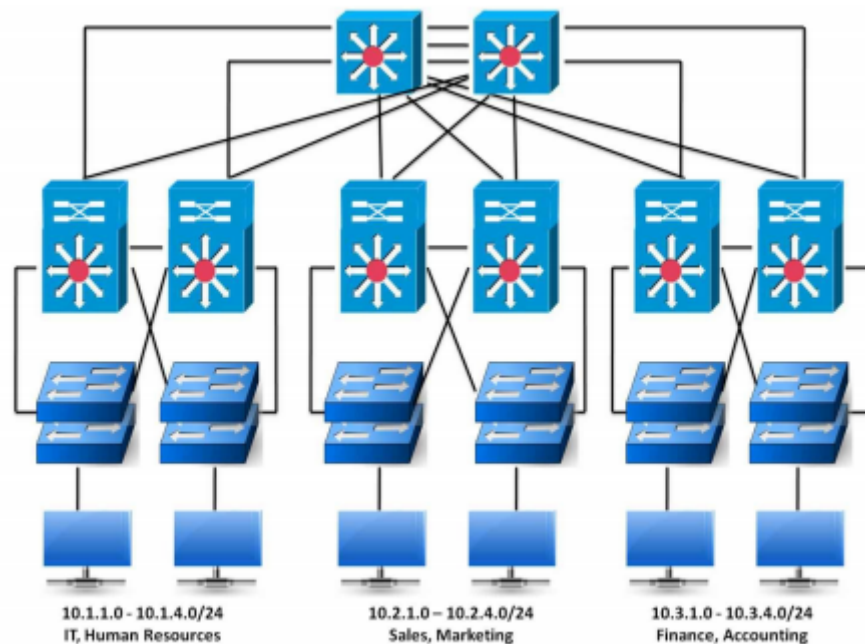
For example, an internal attacker who is connected to the network using some port-scanning tools to scan the open ports can gain access to the switch through which they can start accessing the upper-layer devices.

2. Features of the Virtual Local Area Network

Virtual Local Area Networks (VLANs) are defined as separate broadcast domains, which are local to the switch and controls broadcast, multicast, unicast, and unknown unicast frames. They are defined in an internal database (VLAN.dat) of the switch. The desired ports of a switch can be assigned to the VLANs as per the requirements. VLANs are assigned numbers for identification within a switch or among other switches in the topology. They have a variety of parameters that can be configured to identify them from each other, such as type, name, and state. There are some VLANs that are reserved for special purposes.

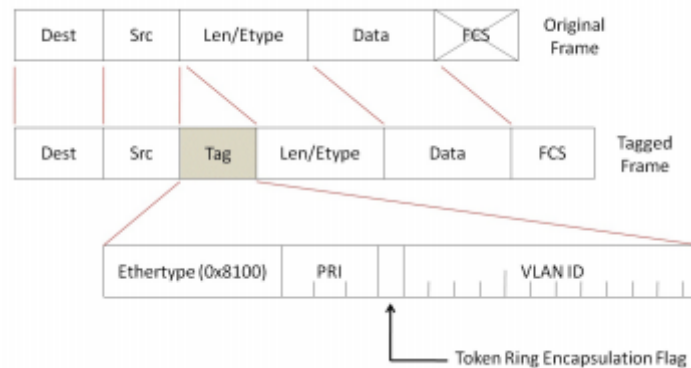
The following figure illustrates the hierarchical network diagram of Cisco's hierarchical architecture, where VLANs are generally implemented in the access layer where end users are connected. The network with IP addresses ranging from 10.1.1.0/24—10.1.4.0/24 is assigned to the VLAN named **IT** and **Human Resources**, 10.2.1.0/24 to 10.2.4.0/24 is assigned to **Sales** and **Marketing**, and 10.3.1.0/24 to 10.3.4.0/24 is assigned to **Finance** and **Accounting**:





A. VLAN Tagging

When there is a single switch in a VLAN segment, no tagging is required, since the switch is aware of the ports connected based on the CAM table. Things become a little complicated as we introduce more switches in the existing topology and the packets need to commute over one or more aggregated ports,



known as **trunks**:

A tag is a 16-bit field that is inserted into an Ethernet frame. When a switchport is encapsulated with an ISL or tagged with a 802.1Q protocol, the mechanism adds the **VLAN identification number** or **VLAN ID**.

B. Features of Trunking

VLANs are local to each other's databases and their information is not passed between switches. Trunk links provide identification for frames travelling among the switches. Some switches have the feature to negotiate the trunk links. Trunks must be configured on both the ends of the link, that is, on both the switchports.

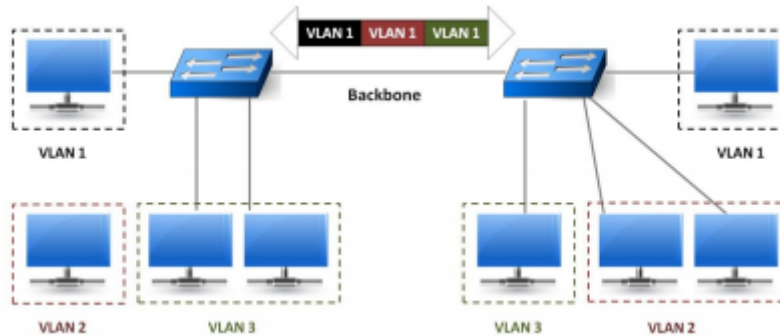
As discussed, trunks are used to pass information between VLANs among the switches. This helps communication between switches for multiple VLANs.



An access port is allowed to share the traffic of a single VLAN. For example, in switch A, if a FastEthernet 0/2 port has been assigned to VLAN 600 then that port would carry the traffic of VLAN 600 only.

A trunk port is the one that would carry the traffic of multiple VLANs over a single link, irrespective of the ports.

For example, in switch B, if a FastEthernet 0/4 port has been configured to carry the traffic of VLANs from 3-8, then they would allow any frame with that respective VLAN tagging:



In order to identify the traffic, VLAN tagging is done on the frame so that these trunk ports can mobile the frames accordingly.

There is also an automatic trunking mechanism known as DTP, the dynamic trunking protocol. This allows the trunk to be dynamically configured between two switches. All Cisco switches can use this protocol to form a trunk link. If one side of the link is the trunk, then it will send DTP signals to the other side of the link. If the signals are accepted/matched then they tend to form a trunk link.

Points to remember:

- Switches should have same trunking mechanism configured on their ends of the trunk link.
- Some iOS do not support DTP, in such cases the command—switchport mode trunk can be used to switch on trunking on that port.
- DTP does not offer any benefit when the user is trying to trunk with a non-Cisco switch.
- It is advisable to use the negotiate option when DTP is not supported and also for hardcoding the port as either access or trunk.
- Cisco 2950 and 3500XL switches do not support DTP and would always be used for configuring manual trunking.
- The 2950 and some 4000 switches support only 802.1Q trunking and provide no options for changing the trunk type.
- **Cisco Discovery Protocol (CDP)** version 2 passes native VLAN information between Cisco switches. If there is a native VLAN mismatch, a CDP error message would be displayed on the console output.

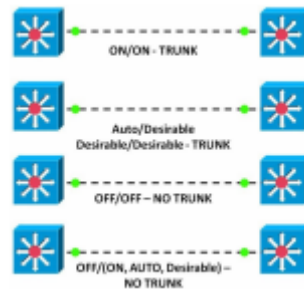
1. Trunking Modes

The following are different types of trunking modes:

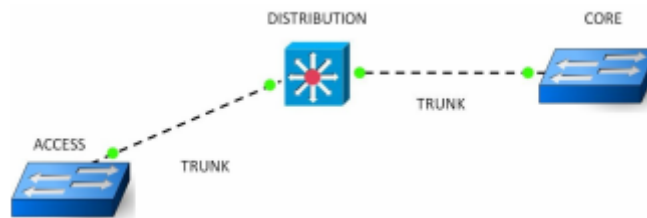


- **Mode trunk:** Trunking is ON for the mode trunk links. They will also send DTP signals that attempt to initiate a trunk with the other side. This forms a trunk with other ports in the on, auto, or desirable states, which are running DTP. A port that is in on mode always tags frames sent out from the port.
- **Mode dynamic desirable:** Mode dynamic desirable links like to become trunk links and send DTP signals that attempt to initiate a trunk. They will only become trunk links if the other side responds to the DTP signal. This forms a trunk with other ports in the on, auto, or desirable states that is running DTP.
- **Mode dynamic auto:** These links will only become trunk links if they receive a DTP signal from a link that is already trunking or desires to trunk. This will only form a trunk with other ports in the on or desirable states. This is the default mode for CatOS switches.
- **Mode nonegotiate:** Sets trunking on and disables DTP. These will only become trunks with ports in on or nonegotiate mode.
- **No switchport mode trunk:** This option sets trunking and DTP capabilities off. This is the recommended setting for any access port because it will prevent any dynamic establishments of trunk links.

The following graphic displays the possible outcome of a shared link between switches if either Switch-A or Switch-B has their port/interface configured in a particular state/trunking mode:



The following is an example with configurations to understand this concept better:



Overview of the configurations which will be apply to the above topology:

- 802.1Q is configured between the access and distribution switches
- ISL is configured between the distribution and core switches
- The core switch is configured for auto-trunking mode and negotiates the encapsulation on the link
- The trunk between the access switch is configured for VLAN 8, 9, and 10

The trunk between the core and distribution is configured for VLAN 1 and 10



On the core switch, we going to execute the following command:

```
Core(config)#interface gigabitethernet 1/1
Core(config-if)#switchport encapsulation negotiate
Core(config-if)#switchport mode dynamic auto
Core(config-if)#switchport trunk allowed vlan remove 2-1001
Core(config-if)#switchport trunk allowed vlan add 10
Core(config-if)#end
Core#copy running-configstartup-config
```

On the access switch:

```
Access(config)#interface gigabitethernet 0/1
Access(config-if)#switchport mode trunk
Access(config-if)#switchport trunk encapsulation dot1q
Access(config-if)#switchport trunk allowed vlan remove 2-1001
Access(config-if)#switchport trunk allowed vlan add 5,8,10
Access(config-if)#end
Access#copy running-configstartup-config
```

On the distribution switch:

```
Distribution(config)#interface gigabitethernet 0/1
Distribution(config-if)#switchport mode trunk
Distribution(config)#switchport trunk encapsulation ISL
Distribution(config)#switchport trunk allowed vlan remove 2-1001
Distribution(config)#switchport trunk allowed vlan add 1,10
Distribution(config)#end
Distribution#copy running-configstartup-config
```

◀ Preliminary Activity for Week 13

Jump to...



Analysis, Application, and Exploration for Week 13 ▶



Navigation

Home

 Dashboard

Site pages

My courses

121 - CC106

121 - BPM101 / DM103

121 - OAELEC2

121 - ITE3

121 - MUL101

121 - ITSP2B

Participants









Grades

General

01 Exploring Security Threats

02 Delving into Security Toolkits



- 03 Intrusion Prevention System
- 04 Understanding Security Policies I
- 05 Understanding Security Policies II
- 06 - Preliminary Examination
- 07 Deep Diving into Cryptography
- 08 Deep Diving into Cryptography: Types of Cipher
- 09 Implementing the AAA Framework
- 10 Implementing the AAA Framework: Implementing A...
- 11 Securing the Control and Management Planes
- 12 - Midterm Examination
- 13 Protecting Layer 2 Protocols
-  Preliminary Activity for Week 13
-  **Lesson Proper for Week 13**
-  Analysis, Application, and Exploration for Week 13
-  Generalization for Week 13
-  Evaluation for Week 13
-  Assignment for Week 13
- 14 Protecting the Switch Infrastructure
- 15 Exploring Firewall Technologies I
- 16 Exploring Firewall Technologies II
- 17 Cisco ASA

121 - WEB101 / CCS3218

Courses

Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.***

PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.



2nd Semester Enrollment



visit www.bcp.edu.ph

Enrollment registration is now Ongoing

For 2nd Semester SY 2021 - 2022





We are accepting new students, returnees and transferees.

"Be trained to be the best,
Be linked to success"

 bcp-inquire@bcp.edu.ph  (8)442-8601 | (8)518-8050

The banner features a blue-tinted image of a multi-story building with a 'BCP' sign on the roof. A large white diagonal banner contains the enrollment information. The bottom right corner includes a quote and a circular logo with a graduation cap. The bottom of the banner has contact information for email and phone.

Activities

-  Assignments
-  Forums
-  Quizzes
-  Resources

Bestlink College of the Philippines
College Department

Powered by [eLearning Commons](#)

