

Cybersecurity Professional Program

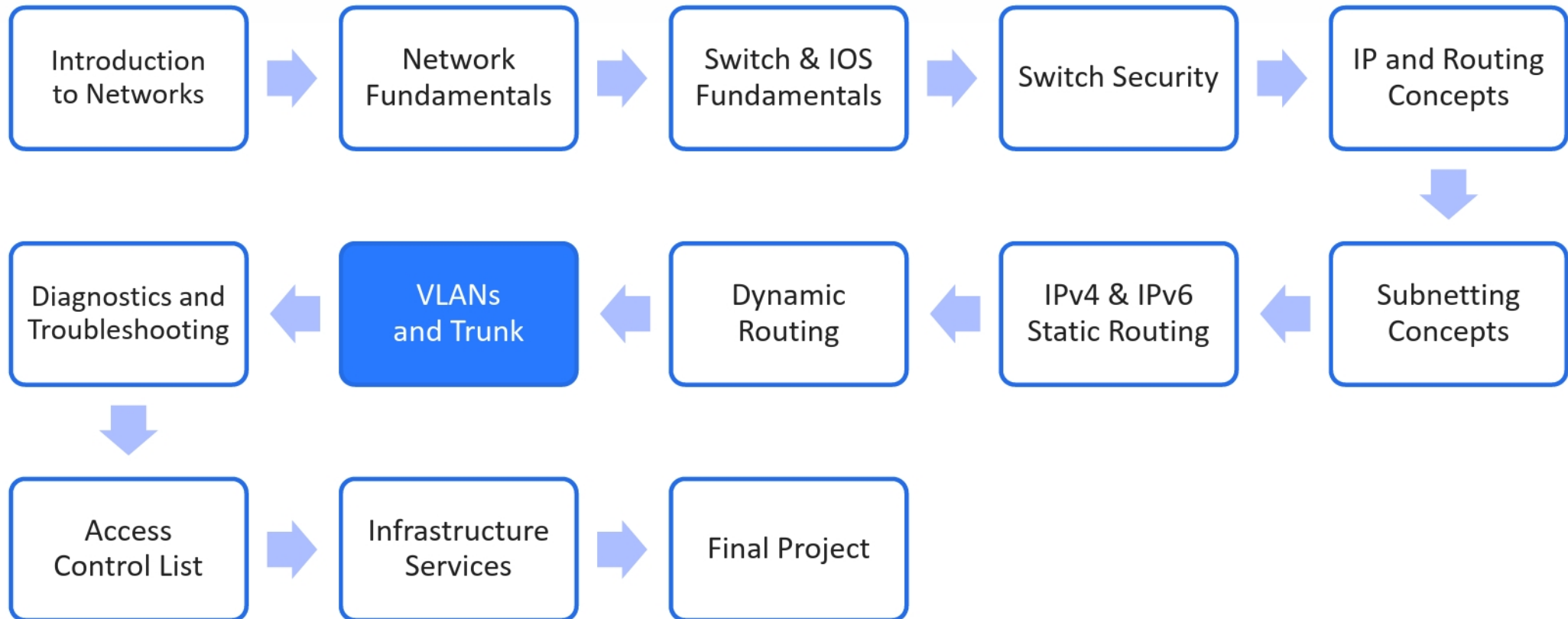
---

# VLANs & Trunk

Computer Networking

# Computer Networking Course Path

---



# Overview

---

## Lesson Objective

The objective of this lesson is to learn how to manage Virtual LANs (VLANs) and about the impact they have on modern networks. It also covers trunk protocols and the VLAN tagging process.



Virtual LANs

Trunk Protocols

Inter-VLAN Routing

VLANs & Trunk

# **VIRTUAL LANS**

## Virtual LANs

# VLANs

---

### Virtual Local Area Networks



VLAN is a common concept and practice among network administrators. Most networks today implement VLANs in one way or another.

VLAN is a Layer 2 feature that allows virtual network segmentation, meaning dividing a physical network into separate logical networks. Each logical network is a VLAN and represents a separate broadcast domain.



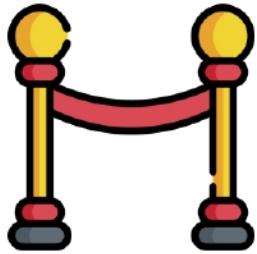
The same rules that govern LANs also apply to VLANs.

## Virtual LANs

# VLANs

---

### How do VLANs work?



Multiple ports are configured on the switch and associated with a VLAN, creating a logical barrier between end devices connected to the switch.

This enables network administrators to create several Virtual LANs on a single switch.

VLANs are logical, not physical, divisions.



Transferring data between VLANs requires a router or other Layer 3 device.

# Benefits of using VLANs

## Improved Security



VLANs help separate and isolate sensitive user data, and reduce the chance of spreading malicious data and unauthorized user access via network traffic.



## Enhanced Performance



VLANs reduce the size of broadcast domains, enhance performance, and minimize unnecessary traffic on the network.



## Simplified Management



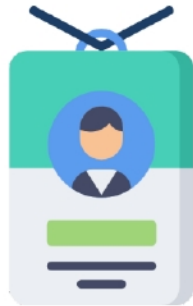
VLANs allow administrators to group end devices and users by departments (such as by job roles) rather than by physical location. This improves network policy flexibility and reduces network costs.



# VLAN ID

---

## What is a VLAN ID?



When traffic passes through a VLAN, it must be identified to keep it separate from traffic in other VLANs. A unique ID identifies a VLAN in the network.

There is complete separation between virtual networks, whereby users on VLAN 10 cannot access user data on VLAN 20.

On Cisco devices, the valid ID range for VLANs is 1 to 1005. There is also an additional extended range of valid VLAN IDs from 1006 to 4094.



The extended range of VLAN IDs from 1006 to 4094 is primarily used in large networks, such as an ISP network.

# VLAN Types

## Default VLAN



VLANs 1 and 1002-1005 are reserved and added automatically during device installation. These VLANs cannot be removed or renamed.

## Data VLAN



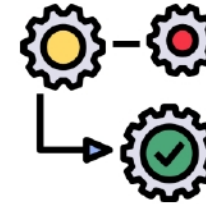
VLANs 2-1001 are commonly used for data exchanges. Their main function is to tag data traffic with an identifier.

## Voice VLAN



This type of VLAN is designed for VoIP (Voice over IP) network traffic.

## Management VLAN



Interface VLAN 1 is a management VLAN used for SVI. Management VLANs enable remote connection and conduct basic network functions.

## Native VLAN



Native VLANs are designed to forward untagged traffic, such as DTP and CDP, among switches. By default, VLAN 1 is a native and management VLAN.

# Default VLAN Settings

## Command

```
show vlan brief
```



The command shows that the switch is already pre-configured with VLAN 1, and all ports are associated with it by default.

Additional VLANs are available in the switch configuration. They are reserved and known as default VLANs.

## Command Output

```
S1#show vlan brief
```

| VLAN | Name               | Status | Ports                                                                                                                                                                                                             |
|------|--------------------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | default            | active | Fa0/1, Fa0/2, Fa0/3, Fa0/4<br>Fa0/5, Fa0/6, Fa0/7, Fa0/8<br>Fa0/9, Fa0/10, Fa0/11, Fa0/12<br>Fa0/13, Fa0/14, Fa0/15, Fa0/16<br>Fa0/17, Fa0/18, Fa0/19, Fa0/20<br>Fa0/21, Fa0/22, Fa0/23, Fa0/24<br>Gig0/1, Gig0/2 |
| 1002 | fddi-default       | active |                                                                                                                                                                                                                   |
| 1003 | token-ring-default | active |                                                                                                                                                                                                                   |
| 1004 | fddinet-default    | active |                                                                                                                                                                                                                   |
| 1005 | trnet-default      | active |                                                                                                                                                                                                                   |



# Switchport Modes

The switch interface operates in one of two main modes, Access or Trunk.

## Access



Access ports carry traffic only on the VLAN to which they belong. Access mode should only be defined on ports connected to end devices, such as PCs.

As a security-related best practice, it is highly recommended to enable Access mode for a port, before assigning it to a VLAN.



## Trunk



Trunk ports carry traffic for different VLANs and devices. The port sets unique identifier tags on the frame, using either the 802.1Q or ISL encapsulation protocols. This ensures that each frame is directed to its intended VLAN.



# VLAN Configuration

## Commands

```
vlan <id>  
name <word>
```



The example on the right shows VLAN 100 and 200 creation, whereby a valid ID is any number between 2 and 1001 (1, 1002-1005 are occupied).

It is recommended to assign an appropriate **name** to the VLAN upon creation.

## VLAN Creation

```
S1(config)#vlan 100  
S1(config-vlan)#name class_A  
S1(config-vlan)#exit  
  
S1(config)#vlan 200  
S1(config-vlan)#name class_B  
S1(config-vlan)#exit
```



# Interface Assignments

## Commands

```
switchport mode access  
switchport access vlan <id>
```



The assignment of hosts (end devices, such as PCs) to different VLANs is done by matching the interconnected interface to the appropriate VLAN.

**Tip:** Assigning multiple ports to a VLAN simultaneously can be done using the **range** command.

## Assigning Ports to VLANs

```
S1(config)#interface range fastEthernet 0/1-2  
S1(config-if)#switchport mode access  
S1(config-if)#switchport access vlan 100  
S1(config-if)#exit  
  
S1(config)#interface range fastEthernet 0/3-4  
S1(config-if)#switchport mode access  
S1(config-if)#switchport access vlan 200  
S1(config-if)#exit
```



# Verifying VLAN Configuration

By running the **show vlan brief** command, it is easy to spot the two new VLANs and the interfaces assigned to them.

To display the interface mode, use **show interfaces switchport**.

## Command Output

```
S1#show vlan brief
```

| VLAN | Name               | Status | Ports                                                                                                                                                                               |
|------|--------------------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | default            | active | Fa0/5, Fa0/6, Fa0/7, Fa0/8<br>Fa0/9, Fa0/10, Fa0/11, Fa0/12<br>Fa0/13, Fa0/14, Fa0/15, Fa0/16<br>Fa0/17, Fa0/18, Fa0/19, Fa0/20<br>Fa0/21, Fa0/22, Fa0/23, Fa0/24<br>Gig0/1, Gig0/2 |
| 100  | class_A            | active | Fa0/1, Fa0/2                                                                                                                                                                        |
| 200  | class_B            | active | Fa0/3, Fa0/4                                                                                                                                                                        |
| 1002 | fddi-default       | active |                                                                                                                                                                                     |
| 1003 | token-ring-default | active |                                                                                                                                                                                     |
| 1004 | fddinet-default    | active |                                                                                                                                                                                     |
| 1005 | trnet-default      | active |                                                                                                                                                                                     |

# Voice VLAN Configuration

## Command

```
switchport voice vlan <id>
```



Voice VLANs enable easier management of VoIP over the network.

The example on the right shows how a Voice VLAN is set up on an interface.

**Note:** VoIP settings on the network are necessary, but are not within the scope of this course.

## Voice VLAN Assignments

```
S1(config)#interface fastEthernet 0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 100
S1(config-if)#switchport voice vlan 150
S1(config-if)#exit
```



VLANs & Trunk

# TRUNK PROTOCOLS

# Trunk Mode

---

## What is Trunking?



Trunk mode is designed to transmit multiple VLAN traffic sessions, over the same physical connection, to a remote device, such as a switch or router.

This is done by tagging frames with the source VLAN, ensuring that the Trunk link forwards the VLAN frames to the same VLAN on another switch. This helps maintain the isolation of other devices.



Trunk mode makes sure that relevant information stays among devices within the same VLAN (such as switches). However, routing among VLANs still requires a router.

# Trunking Protocols

Encapsulating a VLAN tag is the responsibility of two main trunking protocols.

## Inter-Switch Link



ISL is a proprietary protocol developed by Cisco that only operates on Cisco equipment.

The protocol adds VLAN information to Ethernet frames.



## IEEE 802.1Q



802.1q or dot1q is an industry standard developed by IEEE that allows trunk link creation between various vendor switches.

Cisco uses this standard as its default trunk protocol.

Unlike ISL, 802.1q encapsulates the VLAN info in the frame.



# Trunk Configuration

The **switchport mode trunk** command sets the interface to trunk mode and creates trunk links.

To display the trunk's configuration, run the **show interfaces trunk** command.

**Note:** The **switchport mode trunk** command creates a static trunk link, without using the DTP protocol.

## Setting Up and Verifying a Trunk Link

```
S1(config)#interface gigabitEthernet 0/1
S1(config-if)#switchport mode trunk
S1(config-if)#exit
```

```
S2(config)#interface gigabitEthernet 0/1
S2(config-if)#switchport mode trunk
S2(config-if)#exit
```

```
S1#show interfaces trunk
```

| Port   | Mode | Encapsulation | Status   | Native vlan |
|--------|------|---------------|----------|-------------|
| Gig0/1 | on   | 802.1q        | trunking | 1           |

```
S2#show interfaces trunk
```

| Port   | Mode | Encapsulation | Status   | Native vlan |
|--------|------|---------------|----------|-------------|
| Gig0/1 | on   | 802.1q        | trunking | 1           |



# DTP

---

## Dynamic Trunking Protocol



DTP is a protocol developed by Cisco to automate the creation of trunk links, mainly to save time and prevent misconfiguration.

DTP operates on Cisco switches by default, and uses a special packet to "negotiate" the interconnected interfaces.

DTP is also responsible for selecting the trunk protocol on both sides.



DTP can be disabled on specific ports for security purposes (such as to prevent switch spoofing attacks).

# DTP Modes

The protocol includes two port modes for interface negotiation.

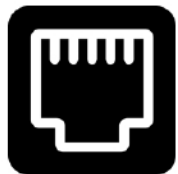
## Dynamic Auto



This mode, which is the default for every port, is passive and does not negotiate. Instead, it waits until an explicit request is received from the other side, and then establishes the trunk link.



## Dynamic Desirable



This mode actively attempts to change the mode of the interconnected interface via DTP packets, to establish a trunk link. Once a directly interconnected port is set to trunk, dynamic auto, or dynamic desirable, a link will be established.



# DTP Mode Configuration

## Command

```
switchport mode dynamic <mode>
```



The example on the right shows the configuration of DTP modes on the interconnected interfaces of the switches.

**Remember:** Dynamic Auto is the default mode.

To display the interface mode, use **show interfaces switchport**.

## Configuring DTP Modes

```
S1(config)#interface gigabitEthernet 0/1
S1(config-if)#switchport mode dynamic auto
S1(config-if)#exit

S1(config)#interface gigabitEthernet 0/1
S1(config-if)#switchport mode dynamic desirable
S1(config-if)#exit
```



# Disabling DTP

## Command

```
switchport nonegotiate
```



Since using DTP can make the switch vulnerable to a VLAN attack, it is best to disable DTP on a port connected to an end device.

Configuring the port in access mode is not enough, and **nonegotiate** is required.

To display the interface mode, use **show interfaces switchport**.

## Disabling DTP on Fa0/1

```
S1(config)#interface fastEthernet 0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport nonegotiate
S1(config-if)#exit
```

```
S1#show interfaces switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
```



# Port Configuration Options

The table below lists the results of each mode combination on opposite ends of the connection.

## Mode Negotiation Results

|                      | Dynamic<br>Auto | Dynamic<br>Desirable | Trunk | Access |
|----------------------|-----------------|----------------------|-------|--------|
| Dynamic<br>Auto      | Access          | Trunk                | Trunk | Access |
| Dynamic<br>Desirable | Trunk           | Trunk                | Trunk | Access |
| Trunk                | Trunk           | Trunk                | Trunk | ---    |
| Access               | Access          | Access               | ---   | Access |



# Native VLAN

---

## What is a Native VLAN?



Native VLANs process untagged frames when they reach trunk ports. Untagged frames are frames that do not have a source or destination VLAN. VLAN 1 is the default native VLAN.



## Why is Native VLAN Required?



Without Native VLANs, sending and receiving updates for protocols such as CDP, VTP, DTP, and STP among interconnected switches would not be possible, since trunk ports drop untagged frames.



# Important Native VLAN Points

Some essential points regarding Native VLANs:

## Best Practice



A best practice regarding Native VLANs is to re-assign them to non-default VLANs, such as VLAN 200, for security purposes. Doing so, can, for example, mitigate Double Tagging attacks.



## Identical Native VLAN



The same Native VLAN must be used on both ends of the trunk link. If not, untagged frames will not be delivered correctly, and the switch's OS will continuously send warning messages to the user, in the form of:  
"%CDP-4-NATIVE\_VLAN\_MISMATCH: **Native VLAN mismatch** discovered on GigabitEthernet0/1 (200), with S2 GigabitEthernet0/1 (1)."



# Native VLAN Configuration

## Command

```
switchport trunk native vlan <id>
```



The example on the right shows how to change the default native VLAN on two interconnected switches.

To display the Native VLAN settings use **show interfaces trunk**.

## Setting the Native VLAN

```
S1(config)#interface gigabitEthernet 0/1
S1(config-if)#switchport trunk native vlan 200
S1(config-if)#exit
```

```
S2(config)#interface gigabitEthernet 0/1
S2(config-if)#switchport trunk native vlan 200
S2(config-if)#exit
```

```
S1#show interfaces trunk
Port      Mode      Encapsulation  Status        Native vlan
Gig0/1    on        802.1q         trunking      200

S2#show interfaces trunk
Port      Mode      Encapsulation  Status        Native vlan
Gig0/1    on        802.1q         trunking      200
```



VLANs & Trunk

# **INTER-VLAN ROUTING**

# Inter-VLAN Routing Overview

## Inter-VLAN Routing



Although VLANs are logical segments, they still operate within the framework of a network, which means they are also broadcast domains.

Switches (which generally operate at Layer 2) cannot move traffic across different VLANs or broadcast domains.

Routing data among different VLANs requires a Layer 3 device (such as a router), which encapsulates and decapsulates the frames.

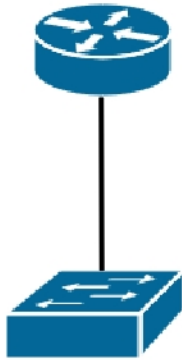


A Layer 3 switch (also known as a multilayer switch) can be used for routing among VLANs, which can also reduce the amount of network components needed to handle the traffic.

# Router-On-A-stick

---

## How Does Inter-VLAN Routing Work?



The most common technique for Inter-VLAN Routing is called Router-On-A-Stick.

This method is effective because it requires only a single physical connection between the switch and the router, avoiding the need for additional components and costs.



# Sub-Interface

## Multiple IP Addresses



Multiple IP addresses are possible because a router's single physical interface is segmented into multiple logical interfaces, called sub-interfaces.



## Logical Interface



Each sub-interface is configured with a unique IP address and subnet mask. Every sub-interface represents a default gateway for a specific VLAN.



## Sub-Interface Command

```
R1(config)#interface  
gigabitEthernet 0/0.1
```

```
R1(config)#interface  
gigabitEthernet 0/0.2
```

```
R1(config)#interface  
gigabitEthernet 0/0.3
```



Simple rule: The number of VLANs dictates the number of sub-interfaces.

# The Switch Side

## Command

```
Switchport mode trunk
```



## Enabling a Trunk on S1

```
S1(config)#interface gigabitEthernet 0/1  
S1(config-if)#switchport mode trunk  
S1(config-if)#exit
```



On the switch side, set the local interface connected to the router to trunk mode. This enables VLAN tagging towards the switch.

# Inter-VLAN Routing Configuration

**On the router side:**

1. Enter the physical interface and enable it.
2. Create a sub-interface.
3. Configure interface encapsulation on 802.1q and assign the appropriate VLAN ID.
4. Configure the VLAN's corresponding IP address and mask (default gateway).
5. Repeat this process for every VLAN.

## Router-On-A-Stick Settings

```
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#no shutdown
R1(config-if)#exit

R1(config)#interface gigabitEthernet 0/0.1
R1(config-subif)#encapsulation dot1Q 100
R1(config-subif)#ip address 10.0.0.1 255.0.0.0
R1(config-subif)#exit

R1(config)#interface gigabitEthernet 0/0.2
R1(config-subif)#encapsulation dot1Q 200
R1(config-subif)#ip address 192.168.0.1 255.255.255.0
R1(config-subif)#exit
```

# Verify Configuration

## Command Output

Use **show ip interface brief** to display the interface settings and mode.

The **show running-config** command shows additional details, such as the interface and its VLAN ID.

```
R1#show ip interface brief
Interface          IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0 unassigned      YES unset  up
GigabitEthernet0/0.1 10.0.0.1       YES manual  up
GigabitEthernet0/0.2 192.168.0.1     YES manual  up
GigabitEthernet0/1   unassigned      YES unset  administratively down
Vlan1               unassigned      YES unset  administratively down
```

# Lab NET-09-L1

Configuring VLANs, Trunks, and More  
30–60 Min.



## Mission

The objective of this exercise is to learn how to configure VLANs and trunks.

## Steps

- Configure & verify VLANs.
- Configure trunks and native VLANs.
- Configure R.O.A.S

## Environment & Tools

- OS: All platforms
- Tools: Cisco Packet Tracer 7.2.2

## Related Files

- Lab document
- NET-09-L1.pka

An overhead photograph of three people sitting around a wooden table, working on laptops. A woman on the left points at a laptop screen with a blue pen. A man in the center works on his laptop. A woman on the right works on her laptop. On the table are a smartphone, a coffee cup, and a document with charts. The image has a blue tint and a semi-transparent dark blue overlay on the left side.

QUESTIONS?



THANK YOU

---