Badji Mokhtar University Annaba
Electronics Department

Chapter 2: VLAN (3)

November 27, 2018 Annaba, Algeria

Outline

- Dynamic Trunking Protocol
- Security and Design
- Inter-VLAN routing

DTP

- If two Cisco switches are cabled together they can negotiate a trunk connection using Cisco's Dynamic Trunking Protocol DTP
- It is however recommended to manually configure switch ports
- Manual configuration:
  - `switchport mode access`
  - `switchport mode trunk`

- DTP configuration:
- `Switchport mode dynamic auto`: will form a trunk if the neighbour switch port is set to trunk or desirable. Trunk will not be formed if both sides are set to auto. Default on newer switches.
- `Switchport mode dynamic desirable`: will form a trunk if the neighbour switch port is set to trunk, desirable or auto. Default on older switches.
- `Switchport nonegotiate`: disables DTP.

DTP

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited Connectivity
Access	Access	Access	Limited Connectivity	Access

The proliferation of network security certifications indicates that the importance of network security is growing.

Every configuration, monitoring, maintenance, and troubleshooting procedure in a switched network must include an analysis of the security implications.

VLANs and VLAN technologies play an integral role in the design and implementation of switched networks.

Switch Spoofing Attack

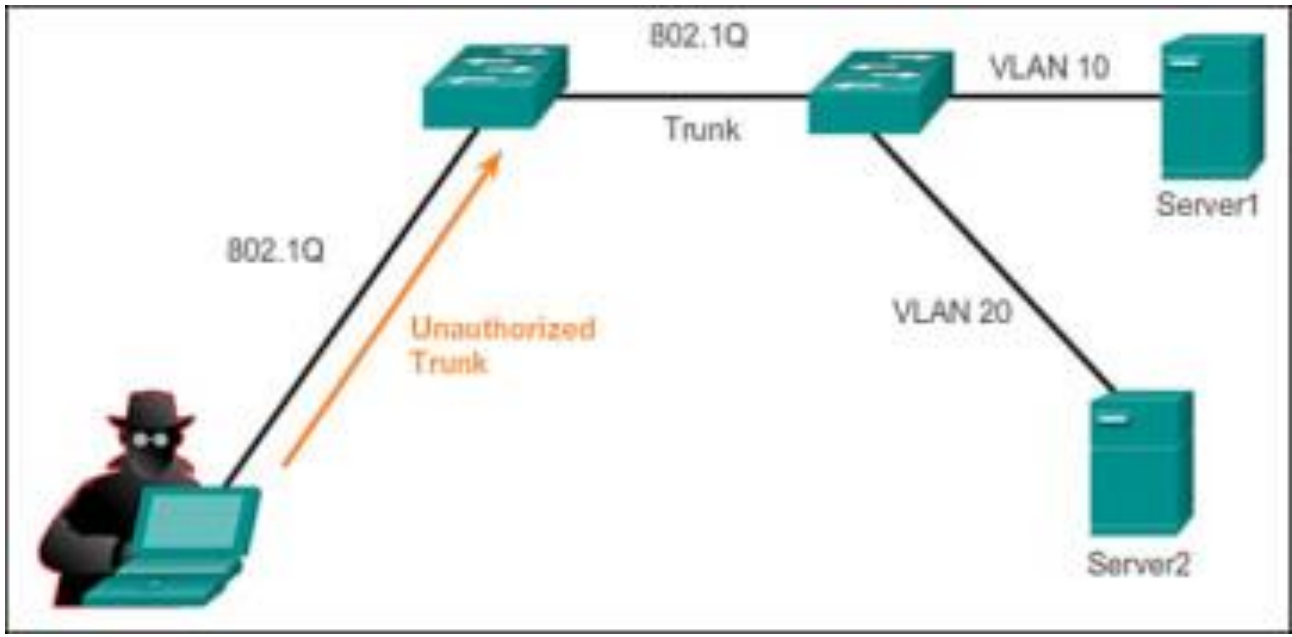
There are a number of different types of VLAN attacks in modern switched networks. The VLAN architecture simplifies network maintenance and improves performance, but it also opens the door to abuse. It is important to understand the general methodology behind these attacks and the primary approaches to mitigate them.

Switch Spoofing Attack

VLAN hopping enables traffic from one VLAN to be seen by another VLAN.

Switch spoofing is a type of VLAN hopping attack that works by taking advantage of an incorrectly configured trunk port.

By default, trunk ports have access to all VLANs and pass traffic for multiple VLANs across the same physical link, generally between switches.

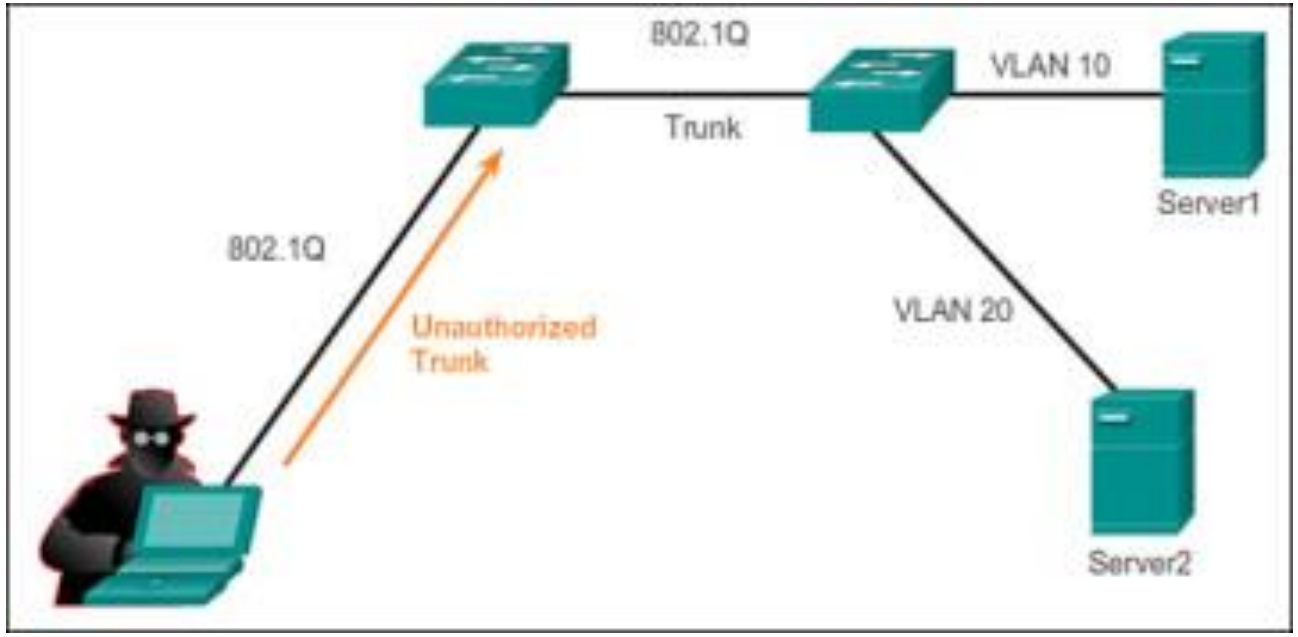


Switch Spoofing Attack

The attacker takes advantage of the fact that the default configuration of the switch port is dynamic auto.

The network attacker configures a system to spoof itself as a switch. This spoofing requires that the network attacker be capable of emulating 802.1Q and DTP messages.

By tricking a switch into thinking that another switch is attempting to form a trunk, an attacker can gain access to all the VLANs allowed on the trunk port.

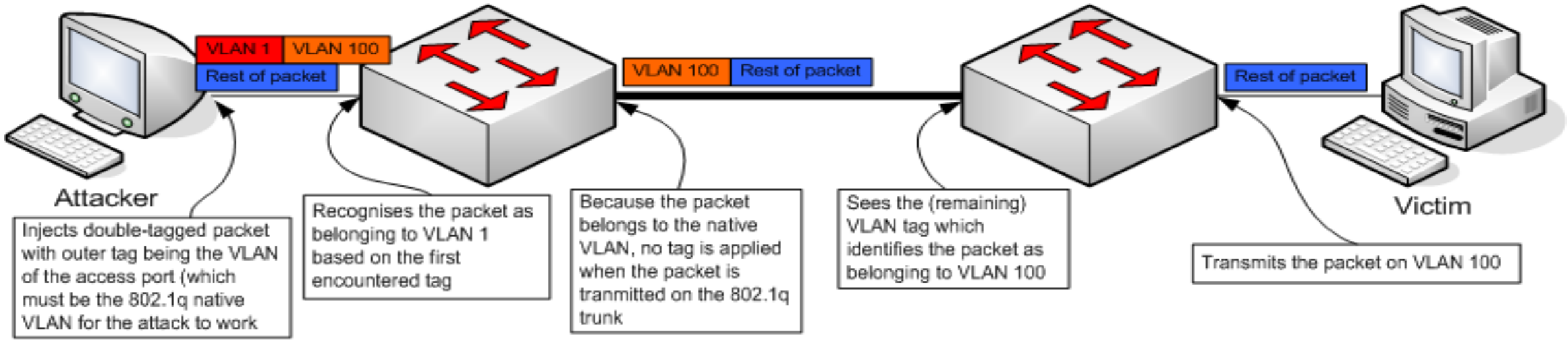


Protection: Turning off trunking on all ports, except the ones that specifically require trunking. On the required trunking ports, disable DTP and manually enable trunking.

Double-Tagging Attack

- This type of attack takes advantage of the way that hardware on most switches operates.
- Most switches perform only one level of 802.1Q deencapsulation, which allows an attacker to embed a hidden 802.1Q tag inside the frame.
- This tag allows the frame to be forwarded to a VLAN that the original 802.1Q tag did not specify.
- An important characteristic of the double-encapsulated VLAN hopping attack is that it works even if trunk ports are disabled, because a host typically sends a frame on a segment that is not a trunk link.

Double-Tagging Attack



This type of attack is unidirectional and works only when the attacker is connected to a port residing in the same VLAN as the native VLAN of the trunk port.

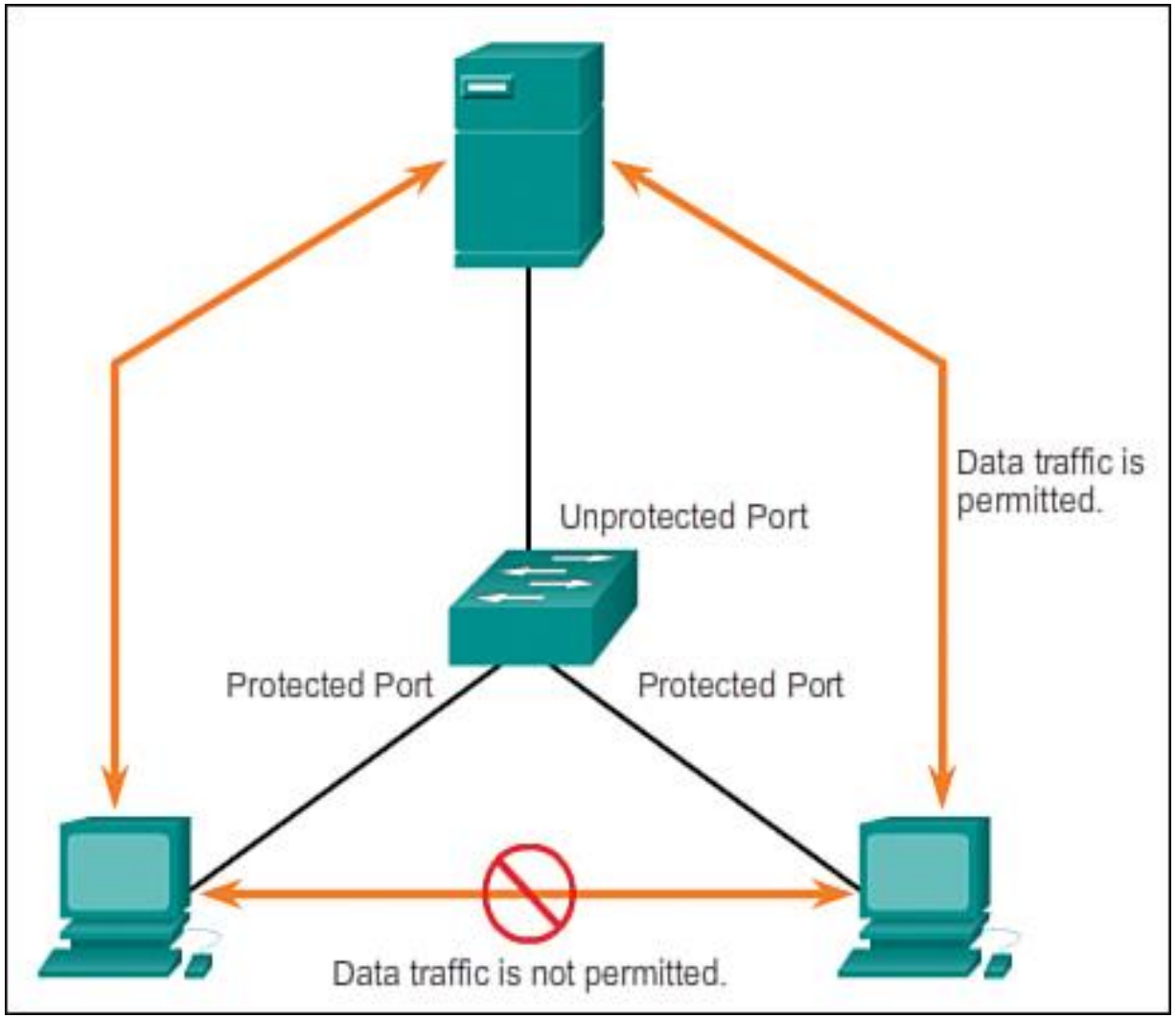
Thwarting this type of attack is not as easy as stopping basic VLAN hopping attacks.

The best approach to mitigating double-tagging attacks is to ensure that the native VLAN of the trunk ports is different from the VLAN of any user ports. In fact, it is considered a security best practice to use a fixed VLAN that is distinct from all user VLANs in the switched network as the native VLAN for all 802.1Q trunks.

PVLAN Edge

- Some applications require that no traffic be forwarded at Layer 2 between ports on the same switch so that one neighbour does not see the traffic generated by another neighbour.

- The use of the Private VLAN (PVLAN) Edge feature, also known as protected ports, ensures that there is no exchange of unicast, broadcast, or multicast traffic between these ports on the switch, as shown in the figure



PVLAN Edge

To configure the PVLAN Edge feature, enter the switchport protected command in interface configuration mode as shown in the output that follows.

- To disable protected port, use the **no switchport protected** interface configuration mode command.
- To verify the configuration of the PVLAN Edge feature, use **show interfaces** *interface-id* **switchport** global configuration mode command.

```
S1(config)# interface g0/1
S1(config-if)# switchport protected
S1(config-if)# end
S1# show interfaces g0/1 switchport
Name: G0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<output omitted>

Protected: true
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

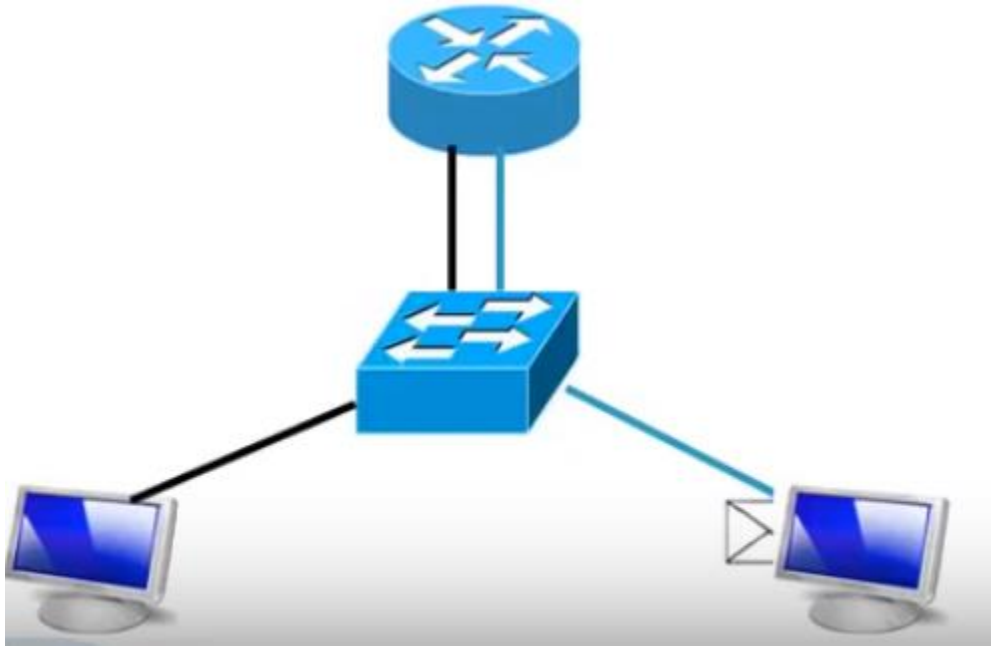
Inter-VLAN routing

- Layer 2 switches cannot forward traffic between VLANs without the assistance of a router.
- Inter-VLAN routing is a process for forwarding network traffic from one VLAN to another, using a router.

Legacy Inter-VLAN routing

- In the past:
  - Actual routers were used to route between VLANs.
  - Each VLAN was connected to a different physical router interface.
  - Packets would arrive on the router through one through interface, be routed and leave through another.
  - Because the router interfaces were connected to VLANs and had IP addresses from that specific VLAN, routing between VLANs was achieved.

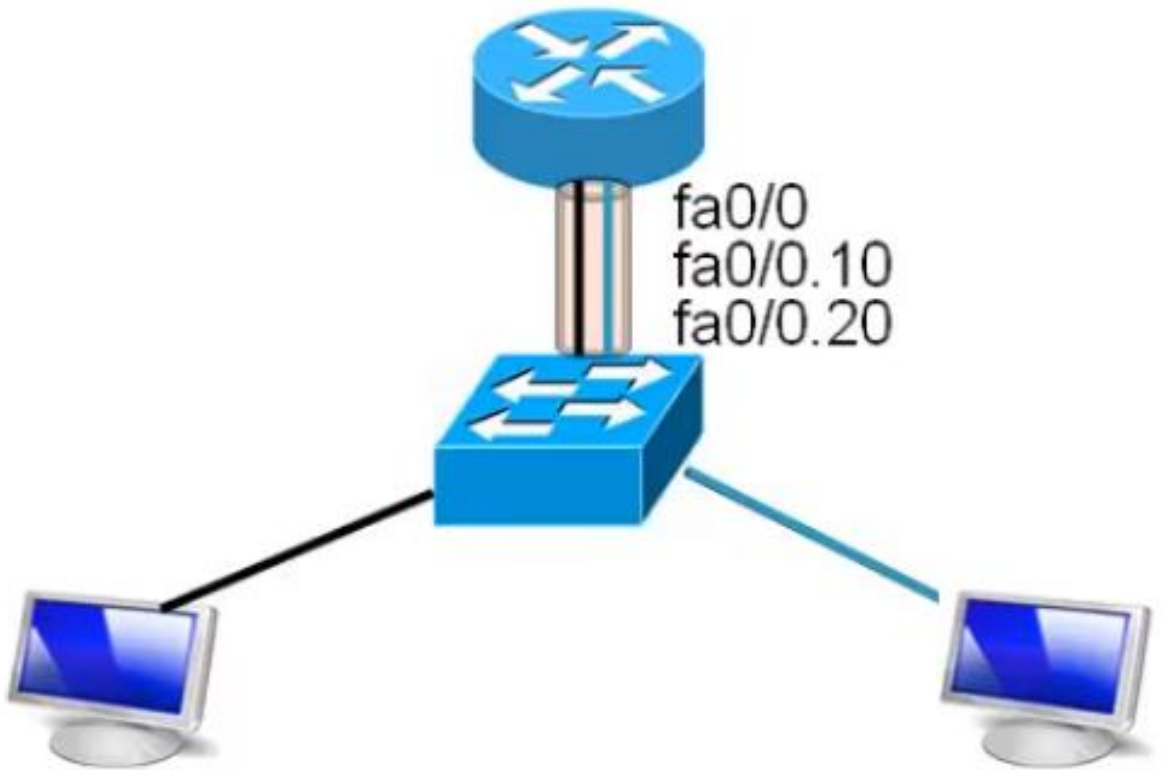
Legacy Inter-VLAN routing



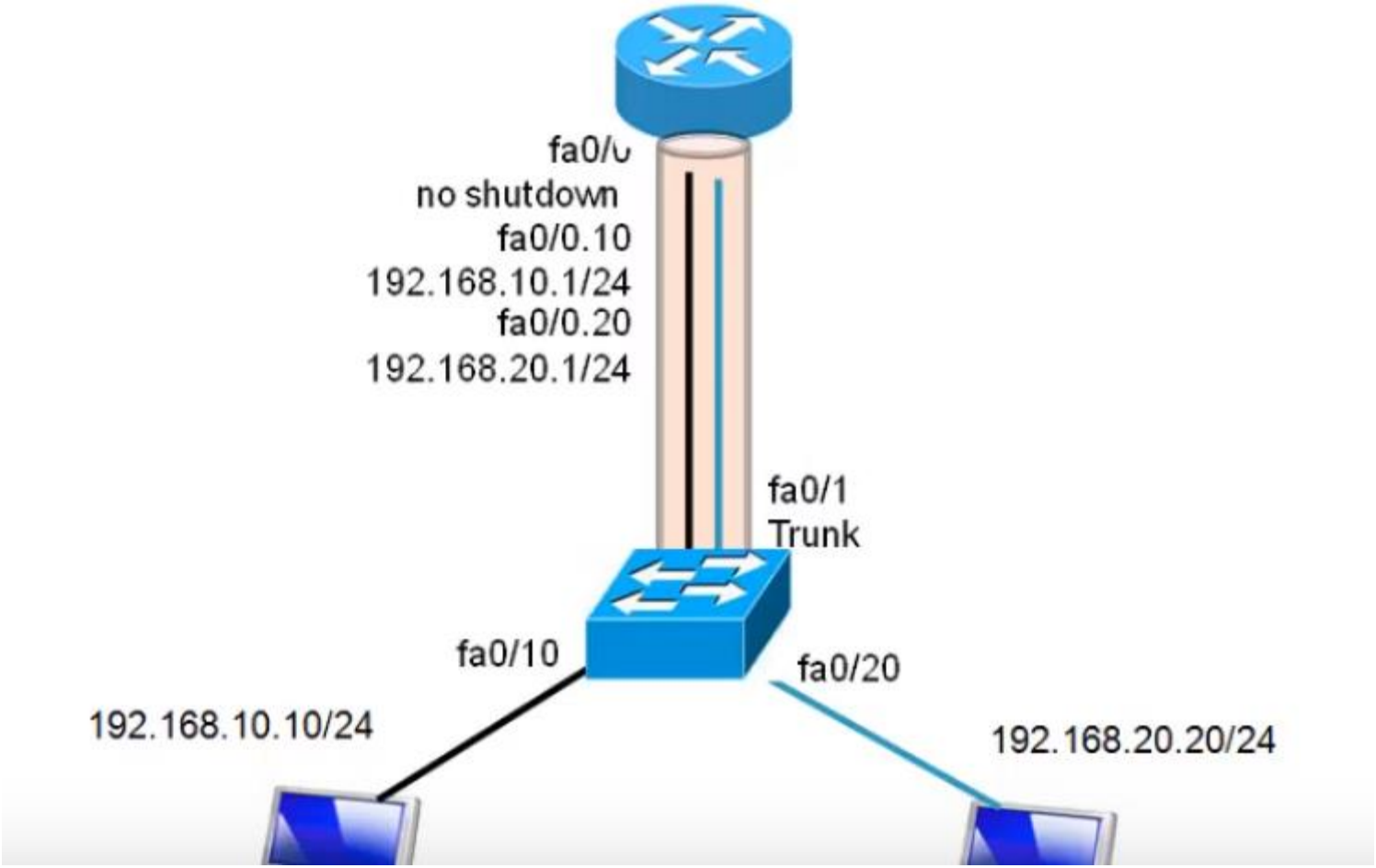
Router-on-a-Stick Inter-VLAN

- The router-on-a-stick approach uses a different path to route between VLANs.
- One of the router's physical interfaces is configured as a 802.1Q trunk port so it can understand VLAN tags.
- Logical subinterfaces are created; one subinterface per VLAN.
- Each subinterface is configured with an IP address from the VLAN it represents.
- VLAN members (hosts) are configured to use the subinterface address as a default gateway.

Router-on-a-Stick Inter-VLAN



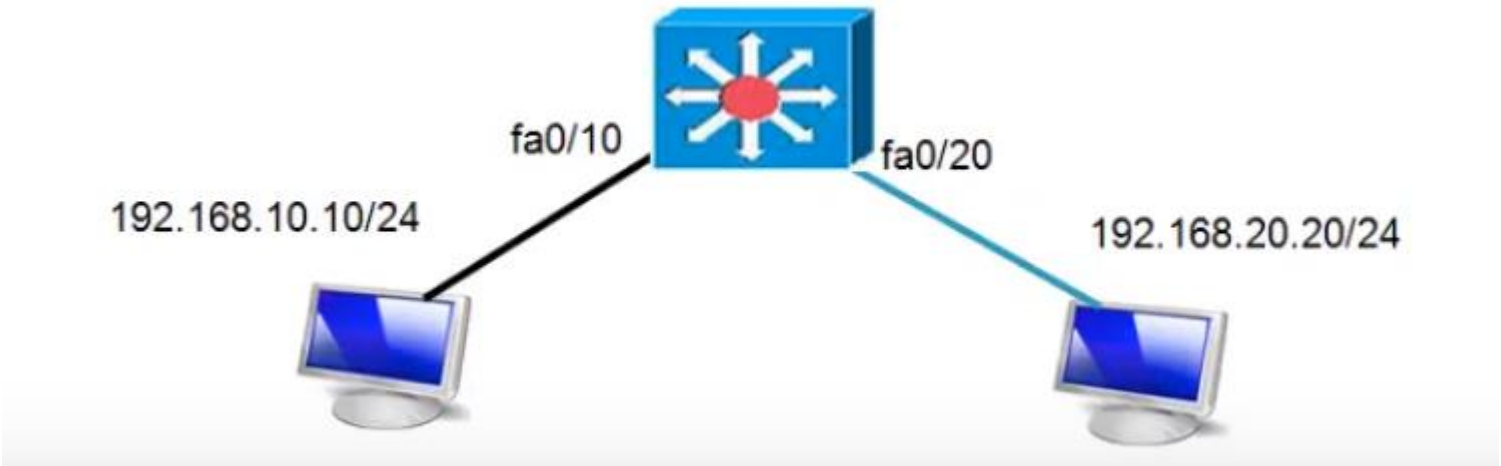
Router-on-a-Stick Inter-VLAN



Multilayer Switch Inter-VLAN

- Multilayer switches can perform Layer 2 and Layer 3 functions, replacing the need for dedicated routers.
- Multilayer switches support dynamic routing and inter-VLAN routing.
- The multilayer switch must have **IP routing** enabled.
- A switch virtual interface (SVI) exists for VLAN 1 by default. On a multilayer switch, a logical (layer 3) interface can be configured for any VLAN.
- The switch understands network-layer PDUs; therefore, can route between its SVIs, just as a router routes between its interfaces.

Multilayer Switch Inter-VLAN



Thank you for your attention