

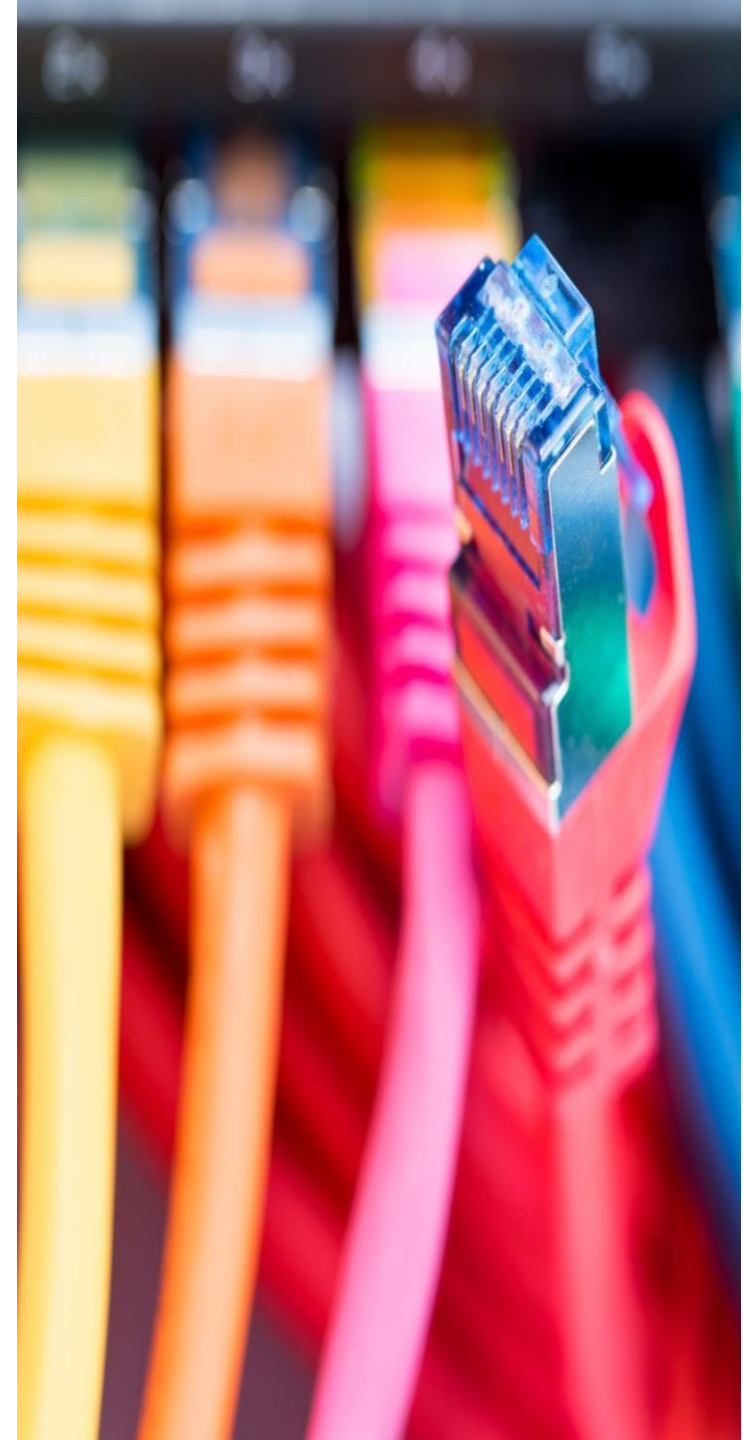


DOUBLE TAGGING

Understanding and Mitigating Sniffing Attacks!!!

What is Double Tagging?

- Double tagging, in the context of networking, typically refers to a technique used in virtual LANs (VLANs) to carry multiple VLANs over a single network link. VLANs are used to logically segment a network into smaller, isolated broadcast domains, improving network performance and security. When traffic from multiple VLANs needs to traverse the same physical network link, double tagging becomes relevant.
- Double tagging attack will work only if the attacker is connected to an interface which belongs to the native VLAN of the trunk port. Double tagging attack is unidirectional.

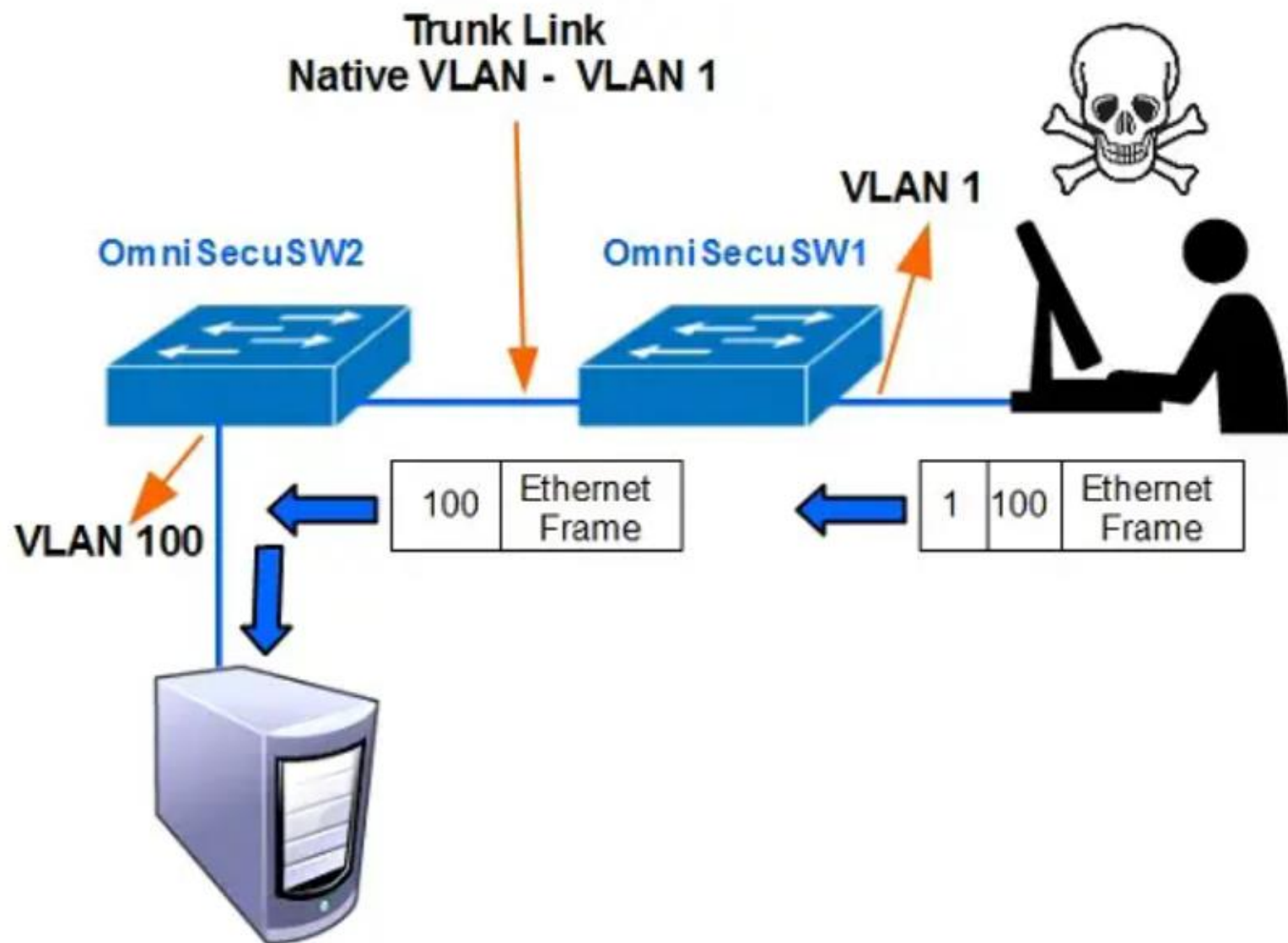


Ethernet Frame Structure

In a standard Ethernet frame, there's a field known as the "tag" or "VLAN tag" that carries VLAN information.

- The VLAN tag includes a 12-bit VLAN ID, which allows for up to 4096 different VLANs.





How Double Tagging operates

From the diagram above in figure 1.0

- Double tagging VLAN hopping attack takes advantage of 802.1Q tagging and tag removal process of many types of switches. Many switches remove only one 802.1Q tag. In Double tagging attack, an attacker changes the original frame to add two VLAN tags. An outer tag, which is of his own VLAN and an inner hidden tag of the victim's VLAN. Here the attacker's PC must belong to the native VLAN of the trunk link.
- When the double tagged frame reaches the switch (OmniSecuSW1), the switch can only see the outer tag of the VLAN that the interface really belongs to.
- The Switch OmniSecuSW1 will now remove the outer VLAN Tag and will forward to all the ports belong to native VLAN (in this example, VLAN1). One copy of that frame is forwarded to the trunk link to reach the next switch OmniSecuSW2.
- When the frame reaches OmniSecuSW2, it will open the frame to see the second tag. OmniSecuSW2 will now assume that frame belongs to VLAN 100 and it is forwarded to VLAN 100.

Setting up a simple packet tracer network environment to explain Double Tagging

Note that the attacker is in VLAN-1, a native VLAN that will be required for the double tagging attack, and the victim server is in VLAN-20. The server has a local IP address “10.0.20.11” which is not accessible from the attacker’s machine “kali-internal” on VLAN-1 as shown in Figure below:

The attacker’s machine has two interfaces and “eth2” is connected to the VLAN-1 network.

When it comes to VLAN exploitation Yersinia is the tool of choice. Yersinia provides a Proof of Concept (PoC) using ICMP packet.

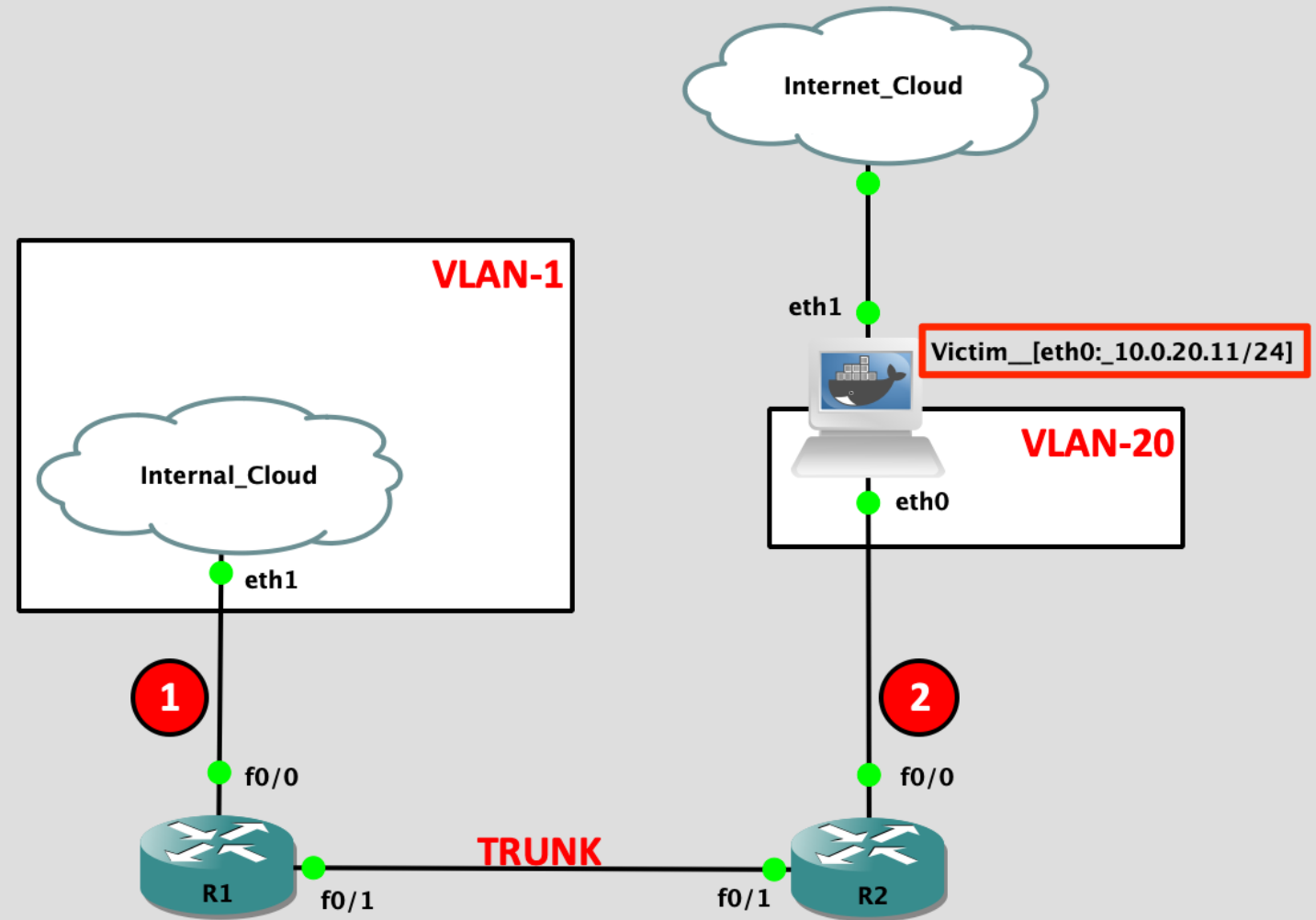


Figure 2.0

Understanding VLAN

VLANs are used to group devices on a network based on logical, rather than physical, connections.

Each VLAN operates as a separate broadcast domain, allowing for better network organization and segmentation.

Single Tagging

- In a typical VLAN setup, a switch adds a single VLAN tag to each Ethernet frame before sending it across the network.
- This single tag informs other network devices which VLAN the frame belongs to.



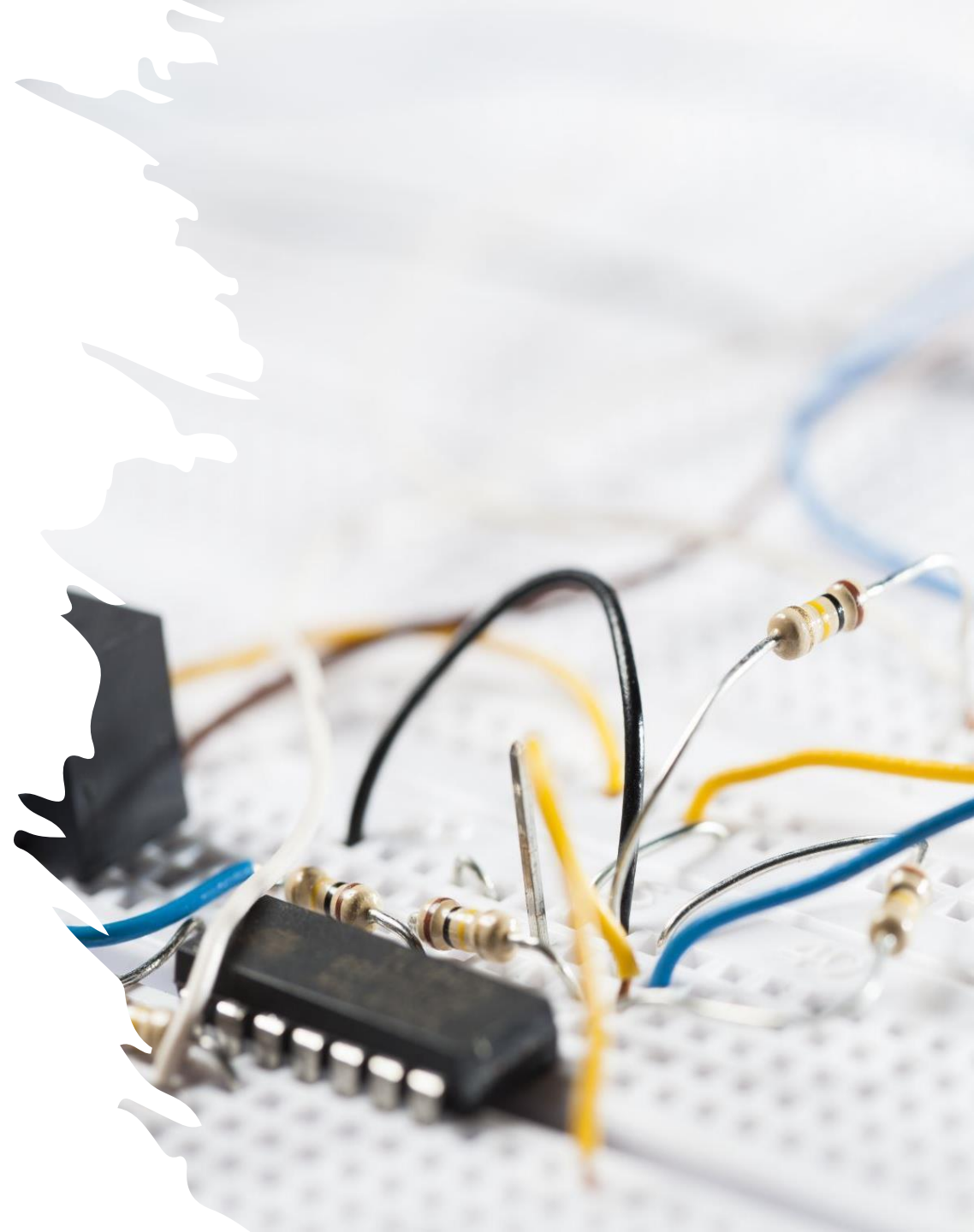
Double Tagging

In some network configurations, it becomes necessary to carry VLAN-tagged frames over an infrastructure that is already using VLAN tagging.

- For example, when frames from multiple VLANs need to traverse a service provider's network or an interconnecting link between different VLAN-aware devices.
- Double Tagging Process:

The process involves adding a second VLAN tag to the original tagged frame.

The outer tag identifies the VLAN on the broader network, while the inner tag identifies the VLAN within the local network.



Implementation of Double Tagging

Q-in-Q (802.1QinQ)

The most common implementation of double tagging is known as Q-in-Q (IEEE 802.1QinQ).

Q-in-Q adds an additional 802.1Q VLAN tag to an Ethernet frame. The outer tag contains information about the service provider's network, and the inner tag contains the original VLAN information.

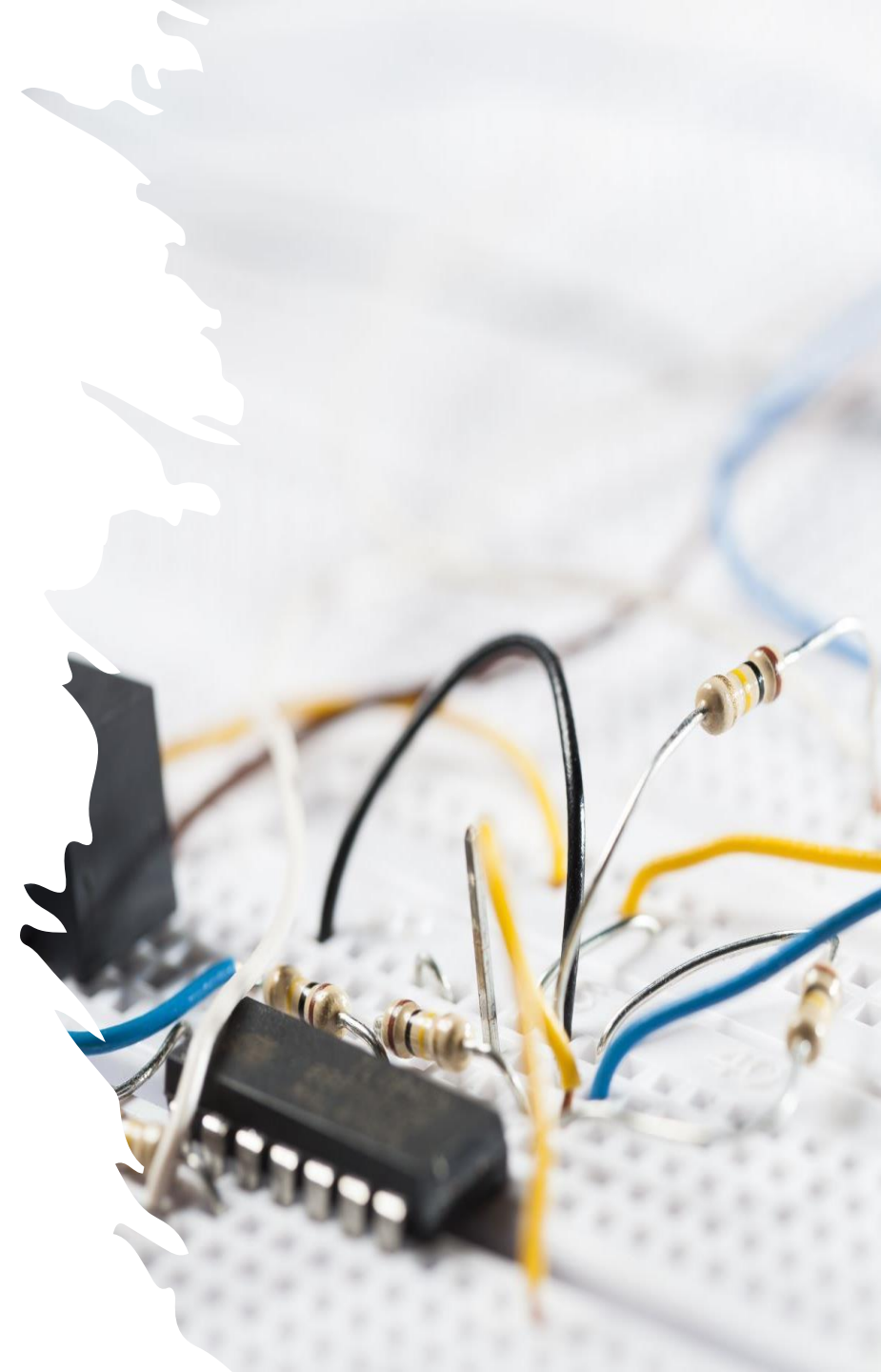
Example: Suppose you have a VLAN-tagged frame with an inner VLAN ID of 10 (original VLAN). With double tagging, it gets an additional outer VLAN ID of 20 (service provider VLAN).

The frame, when received, is first recognized by the outer VLAN ID (20), and then, within that VLAN, the inner VLAN ID (10) is used for local network segmentation.



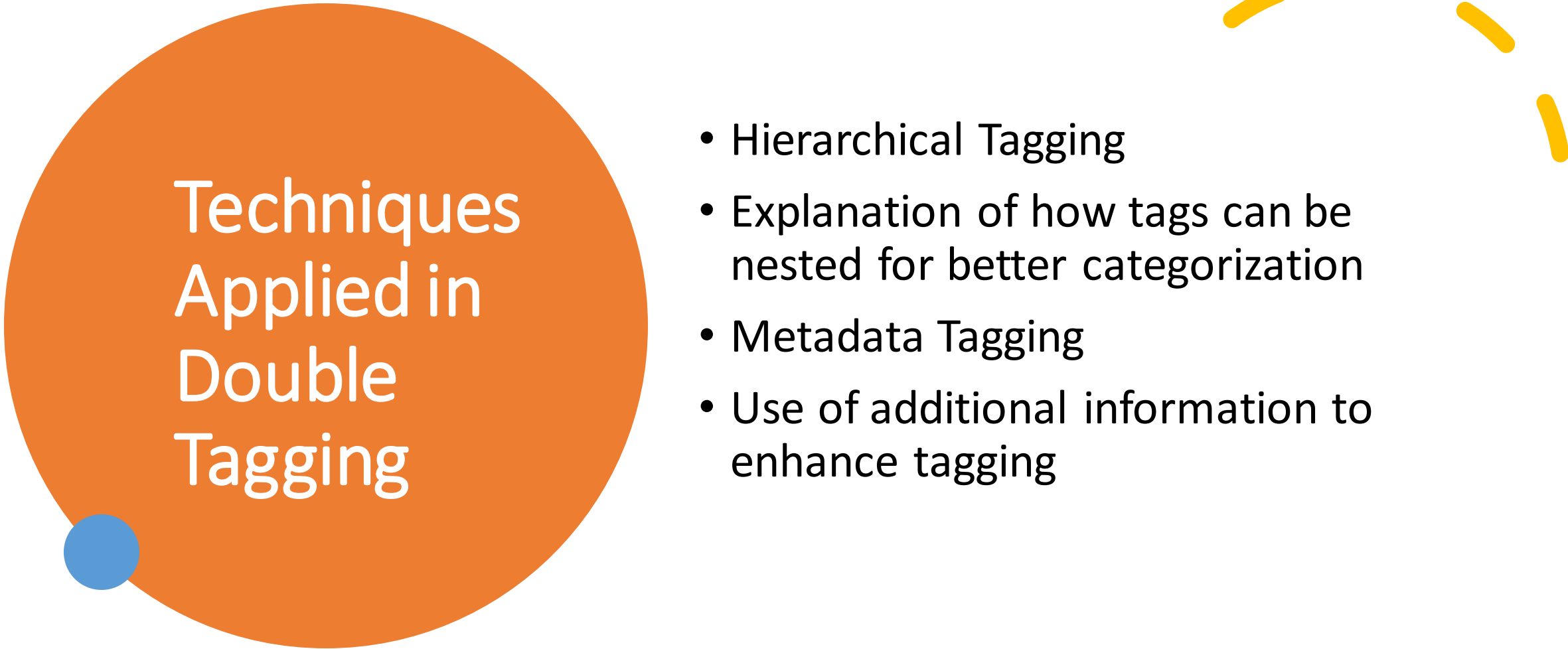
Benefits of Implementing **Q-in-Q (802.1QinQ)**

- Allows for the transportation of VLAN-tagged frames across multiple networks without losing the original VLAN information.
- Enables service providers to maintain customer VLAN information while transporting the traffic over their networks.



Benefits of Double Tagging

- Improved Search and Retrieval
- Enhanced Organization and Filtering



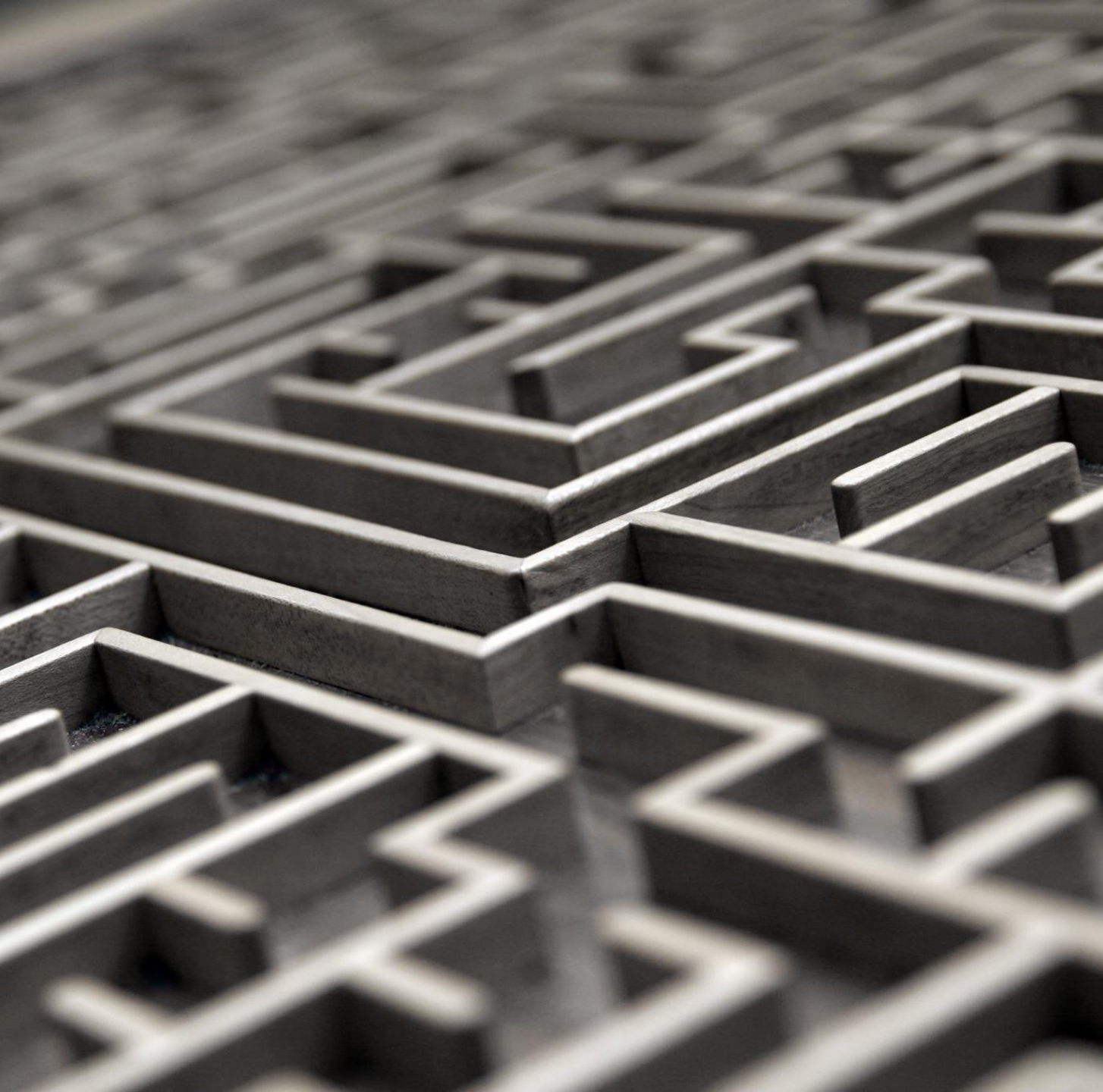
Techniques Applied in Double Tagging

- Hierarchical Tagging
- Explanation of how tags can be nested for better categorization
- Metadata Tagging
- Use of additional information to enhance tagging



Protection Measures

- Encryption of Tags
- Ensuring that tagged data is secure
- Access Control
- Restricting who can add or modify tags
- Regular Audits
- Ensuring compliance and identifying anomalies

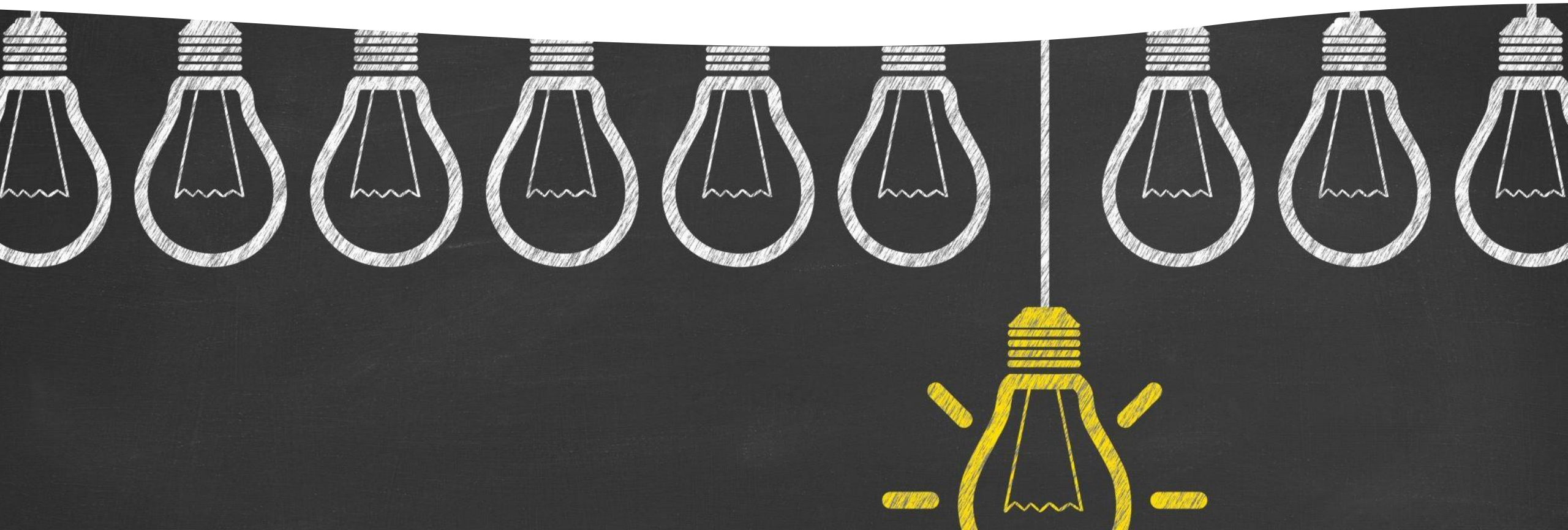


Challenges in Double Tagging

- Complexity in Implementation
- Potential for Tagging Errors

Best Practices for Implementation of Double Tagging

- Clear Tagging Policies
- Employee Training
- Regular Maintenance and Review
- Slide 11: Conclusion



Conclusion

In conclusion, double tagging, particularly through Q-in-Q, is a technique that extends VLAN capabilities across multiple networks, ensuring that VLAN information is preserved as traffic traverses' different segments of a larger network.

