Candidates who are preparing for the Cisco CCIE® Routing and Switching (R&S) lab exam will find this resource helpful in learning how to properly configure link aggregation with EtherChannel, common VLAN, and Virtual Terminal Protocol (VTP). This tip sheet also explains how to identify trunk link configuration errors. The candidate should be able to meet these objectives after completing the reading:

1. Describe the best practices for configuring port channels using EtherChannel
2. Show how to configure load balancing among the ports included in an EtherChannel
3. Identify common problems with VTP, VLAN, and trunk link configurations
4. Explain trunk link problems and identify best practices for resolving trunk link problems
5. Show common problems with VTP configuration

1. Best Practices for Configuring EtherChannel

- **EtherChannel support:** All Ethernet interfaces on all modules support EtherChannel (maximum of eight interfaces), with no requirement that interfaces be physically contiguous or on the same module.

- **Speed and duplex:** Configure all interfaces in an EtherChannel to operate at the same speed and in the same duplex mode. Also, if one interface in the bundle is shut down, it is treated as a link failure, and traffic will traverse other links in the bundle.

- **Switched Port Analyzer (SPAN) and EtherChannel:** An EtherChannel will not form if one of the interfaces is a SPAN destination port.

- **Layer 3 EtherChannels:** Assign Layer 3 addresses to the port-channel logical interface, not to the physical interfaces in the channel.

- **VLAN match:** All interfaces in the EtherChannel bundle must be assigned to the same VLAN or be configured as a trunk.

- **Range of VLANs:** An EtherChannel supports the same allowed range of VLANs on all of the interfaces in a trunking Layer 2 EtherChannel.

  If the allowed range of VLANs is not the same, the interfaces do not form an EtherChannel, even when set to “auto” or “desirable” mode. For Layer 2 EtherChannels, either assign all interfaces in the EtherChannel to the same VLAN or configure them as trunks.

- **STP path cost:** Interfaces with different Spanning Tree Protocol (STP) port path costs can form an EtherChannel as long they are otherwise compatibly configured. Setting different STP port path costs does not, by itself, make interfaces incompatible for the formation of an EtherChannel.

- **Port channel versus interface configuration:** After configuring an EtherChannel, any configuration that is applied to the port-channel interface affects the EtherChannel. Any configuration that is applied to the physical interfaces affects only the specific interface that is configured.

2. Configure Load Balancing over EtherChannel

- **With source-MAC address forwarding**, when packets are forwarded to an EtherChannel, they are distributed across the ports in the channel based on the source-MAC address of the incoming packet.

  Therefore, to provide load balancing, packets from different hosts use different ports in the channel, but packets from the same host use the same port in the channel (and the MAC address learned by the switch does not change).

- **With destination-MAC address forwarding**, when packets are forwarded to an EtherChannel, they are distributed across the ports in the channel based on the destination-MAC address of the frame.

  Therefore, packets to the same destination are forwarded over the same port, and packets to a different destination are sent on a different port in the channel.

Configure the load balancing-and-forwarding method by using the **port-channel load-balance** global configuration command.

3. Common VLAN, VTP, and Trunk Link Configuration Errors

- 802.1Q Native VLAN issues
  - Native VLAN frames are carried over the trunk link untagged.
  - A native VLAN mismatch will merge traffic between VLANs.

- Resolving Issues with 802.1Q Native VLANs
  - The native VLAN interface configurations must match at both ends of the link, or the trunk may not form.
  - By default, the native VLAN will be VLAN1. For the purpose of security, the native VLAN on a trunk should be set to a specific VLAN ID (VID) that is not used for normal operations elsewhere on the network. For example:

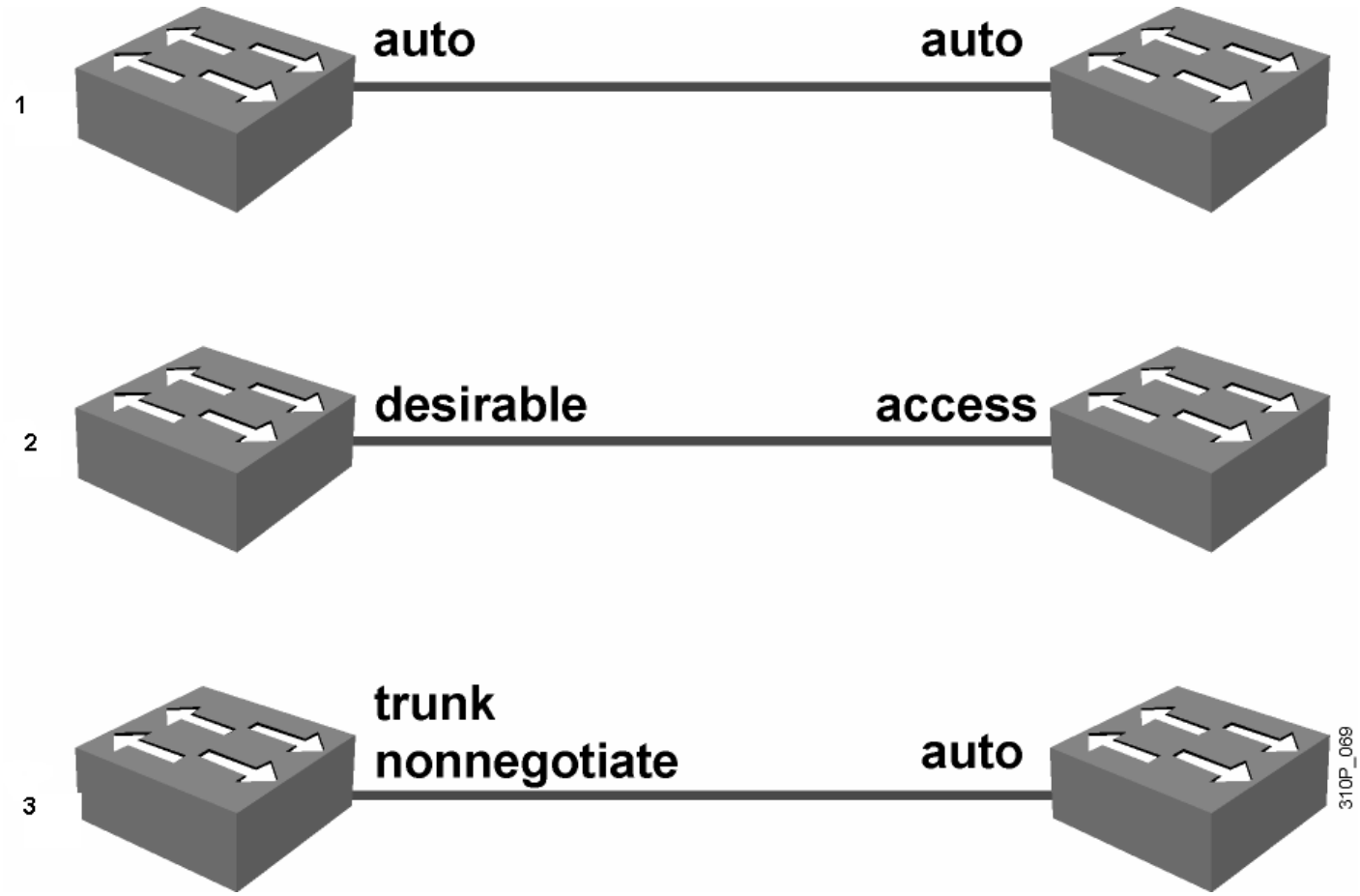
Switch(config-if)#**switchport trunk native vlan** *vlan-id*

If there is a native VLAN mismatch on either side of an 802.1Q link, Layer 2 loops may occur because VLAN1 STP bridge protocol data units (BPDUs) are sent to the IEEE STP MAC address (0180.c200.0000) untagged.

4. Explain Trunk Link Problems

- Trunks can be configured statically or autonegotiated with Dynamic Trunking Protocol (DTP).
- For trunking to be autonegotiated, the switches must be in the same VTP domain.

Some trunk configuration combinations will successfully configure a trunk, and some will not. The following three examples of the trunk configurations will not work properly.



Resolve Trunk Link Problems

- Both ends of the link are in the same VTP domain when DTP is required.
- Ensure that the trunk encapsulation type configured on both ends of the link is valid.
- To enable trunking to a device that does not support DTP, use the switchport mode trunk and switchport nonegotiate interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

Posted to the Cisco Learning Network - www.cisco.com/go/learnnetspace

Best practice is to configure **trunk** and **nonegotiate** where trunks are required.

5. Common Problems with VTP Configuration

- **Updates not received as expected:** The VTP domain and password must match.
  - The VTP domain name and password must match on a given switch to receive updates from a VTP server. The domain name is case-sensitive.
  - The VTP version must be compatible with other switches in the domain.
  - Ensure that there is at least one server in the domain.
  - Check that a trunk link exists to the VTP server.
- **Missing VLANs:** Another VTP device has overwritten configuration.
  - Upon initial configuration, the VTP server may have had a partial VLAN database, and it overwrote the existing, more complete, database on the existing switch.
  - VLANs were deleted individually at the VTP server, and those deletions will be propagated in the domain. (To avoid this scenario, ensure that any switch becoming a VTP server has a complete VLAN list.)
- **Too many VLANs:** Consider making the VTP domain smaller.
  - The VTP server has a VLAN list that is more complete than the list.