

Configuration Examples Related to VLAN Features

VLAN capabilities and features on the Catalyst 1900 and Catalyst 2820 switches might be slightly different from those on other Cisco products, such as the Catalyst 5000 series switches, the Catalyst 3000 family switches, and the Cisco 3600 routers. This appendix provides three examples of some of the VLAN similarities and differences so that you can use your switch most effectively in your network.

Limited VLAN Isolation: Temporary VLAN Cut-Through After VLAN Change

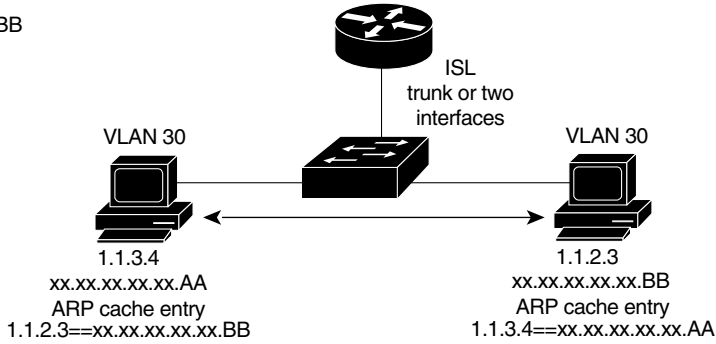
Figure A-1 illustrates the following condition:

Two stations, AA on port 1 and BB on port 2, are both in VLAN 30. The two stations have established IP communications, can ping each other, and support Telnet sessions. Through administrative action, port 2 is subsequently associated with VLAN 40. For a while, the two stations continue to communicate as they did before the VLAN change.

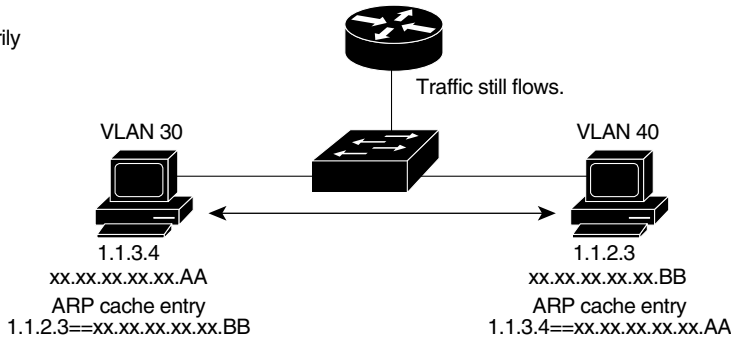
Limited VLAN Isolation: Temporary VLAN Cut-Through After VLAN Change

Figure A-1 Temporary VLAN Cut-Through After VLAN Change Example

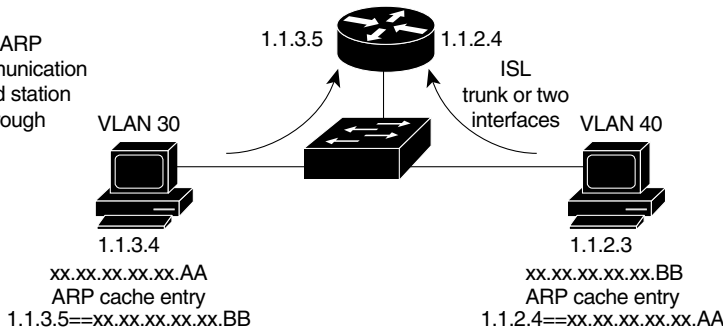
Station AA and station BB are in VLAN 30.



Station BB is temporarily moved to VLAN 40.



ARP cache cleared, or ARP cache timed out. Communication between station AA and station BB is re-established through the router.



10424

Effect of VLAN Change

Because the stations communicated before the VLAN change, the switch had previously learned the MAC addresses of both stations. Each station also contained the MAC address of the other station in its own ARP cache. For a while after the VLAN change, packets transmitted from one station to the other are sent by using the MAC addresses stored in each ARP cache. The VLAN cut-through of the switch forwards packets directly between ports 1 and 2 as before. However, the station ARP cache entries eventually time out.

After the ARP cache times out, station AA must broadcast an ARP request to obtain a new address for station BB. No communications can occur between the stations until the location of the address is resolved. (The broadcast is not forwarded to station BB because the two stations exist on different VLANs—station AA on VLAN 30 and station BB on VLAN 40.) If a router is available to forward between VLANs 30 and 40, the broadcast from station AA reaches the router interface on VLAN 30. The router responds to station AA on VLAN 30 with its own MAC address, and communication between station AA and station BB is reestablished through the router. The router communicates with station AA on VLAN 30 and with station BB on VLAN 40.

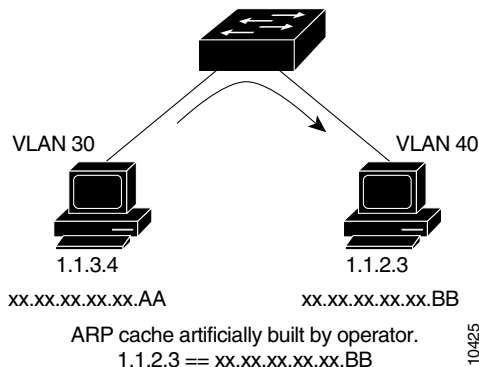
The local VLAN isolation feature of the Enterprise Edition software prevents this temporary communication of stations after VLAN changes as long as stations AA and BB are connected to the same switch.

Limited VLAN Isolation: Exposure to MAC-Level Spoofing

Figure A-2 illustrates the following condition:

Station AA on port 1 is in VLAN 30. Station BB on port 6 is in VLAN 40. The operator of station AA seeks to intentionally establish communication directly across the VLAN boundary, perhaps to bypass router access controls. In essence, the connection to be made between station AA and station BB is not permissible; it is “spoofed” because the MAC address is not learned across or between the VLANs connected to the switch.

Figure A-2 Exposure to MAC-Level Spoofing Example



Effect of MAC-Level Spoofing

The operator of station AA would first have to learn the MAC address of target station BB on VLAN 40. This task is difficult because not all traffic to and from station BB appears on VLAN 30 and is therefore not visible to station AA. However, the operator could still ascertain the MAC address of station BB by other means (such as by gaining physical access to the other station). After the address of station BB is learned, the operator could insert a static address entry for station BB into the local ARP cache of station AA and establish communication directly between the stations. This is similar to the temporary VLAN cut-through example shown in Figure A-1.

The Enterprise Edition software local VLAN isolation feature prevents this spoofing effect as long as the operator's station AA and the target station BB are connected to the same switch.

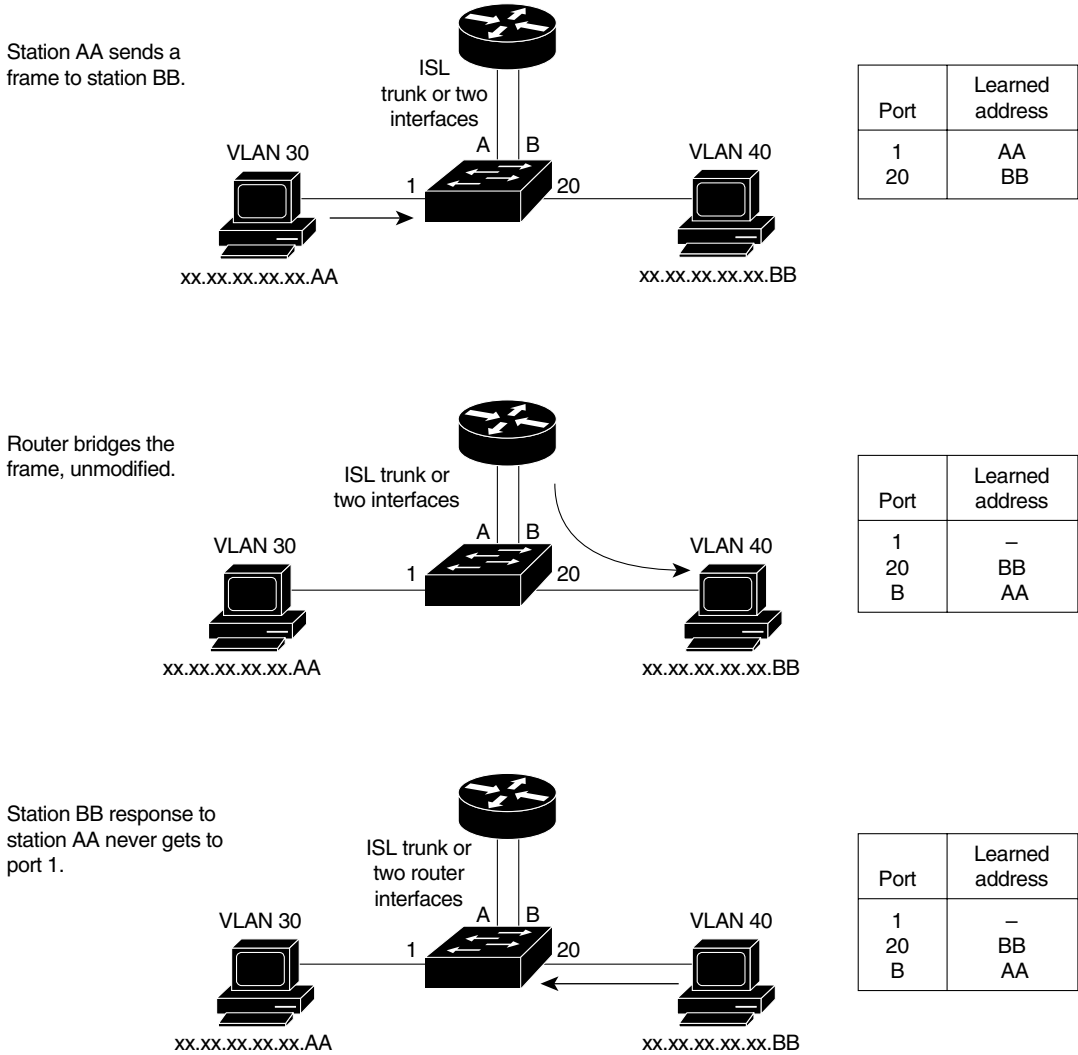
Single MAC Address Support: Bridge-Router Between VLANs

Figure A-3 illustrates the following condition:

Two stations, station AA on port 1 in VLAN 30 and station BB on port 2 in VLAN 40, need to communicate by using a non-routable protocol such as Netbios. IP traffic between the two stations will be transmitted through a router that has attachments to both VLAN 30 and VLAN 40. If these VLANs were physically separated LANs, Netbios traffic between them would be *bridged* by the router (that is, forwarded without the usual router [Layer-3] packet modifications to the MAC address headers). When bridging protocols are enabled on the router and the Catalyst 1900 and Catalyst 2820 series VLAN feature is enabled between connected stations across the switch, Netbios communication is intermittent or simply fails.

Single MAC Address Support: Bridge-Router Between VLANs

Figure A-3 Effects of Single MAC Address Support Example



10511

Effect of Bridging Protocols

The configuration just described results in duplicate MAC address handling. Duplicate MAC address handling is best understood by considering the flow of traffic from station AA to station BB.

The packet from station AA includes a destination address for BB in VLAN 30. Because station BB is on port 20 in VLAN 40, the packet is not sent directly, but instead travels to the router, which has bridging protocols enabled.

The connection between the switch and the router is most likely a trunk-port connection or two directly connected interfaces. The router forwards the packet unmodified to VLAN 40, again using the trunk-port connection to the switch. The switch can then forward the packet out port 2 to station BB, as addressed. The return packet (from BB to AA) follows the same path—across the trunk port to the router, out the trunk port again to the switch, and ultimately to station AA.

However, a confusion in the learning of MAC address AA from this same packet has occurred. When the packet first arrived on port 1, MAC address AA was learned there. When it arrived back from the bridge-router on the trunk port, MAC address AA was learned again from the trunk-port connection. In the Catalyst 1900 and Catalyst 2820 series software, the second learning of an address deletes the first learned port location, so the switch no longer associates station AA to port 1. Return packets from station BB might not reach station AA because the port association for AA could have been modified in the address table. If the packet does return, it might be because the frame was flooded through VLAN 30.

A solution is to create a static address for address AA associated with both port 1 and the trunk-port, qualified by the source port such that source ports in VLAN 30 forward directly to port 1, and source ports in other VLANs forward to the trunk-port to reach the router.

