VLAN Trunking and Networking

In this technical brief, we discuss how the Digi Accelerated Linux operating system (DAL OS), the sophisticated software at the heart of all modern Digi networking solutions, enables this capability and provides enhanced VLAN networking capabilities across your network. Traditionally, this functionality would require much more expensive, dedicated firewall appliances.

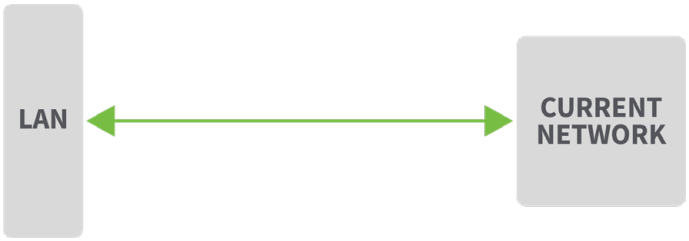
A Virtual LAN (VLAN) separates a single, physical local area network (LAN) into two or more distinct, logically separate LANs. Each device on a VLAN can only access other devices on the same VLAN and each device is unaware of any other VLAN. This strategy isolates networks from one another, even though they run over the same physical network. Trunking allows multiple VLANs to be transported over a single connection. This extends the VLAN across physical boundaries that would otherwise block lower-layer protocols such as ARP.

Application

DAL OS (Digi Accelerated Linux) devices can be used independently or as part of a larger network. When administrators want to separate devices on a common (physical) network, they often employ VLANs. Several large manufacturers recommend VLAN architectures. If your network uses VLANs to separate devices, the DAL OS device will need to use the VLAN. To achieve this, create a VLAN interface between the DAL OS device and the rest of the network.

This is all that is required if devices on the DAL LAN want access to the current network, because they can use source NATing. Traffic from the current network would use the DAL OS device as a gateway to access devices on the DAL LAN, and layer 2 communication would not pass the DAL OS device.

VLAN trunking allows the connection between the DAL OS device and the current network to carry VLAN packets with many different tags that can interact directly with devices on the DAL LAN. In fact, the DAL LAN devices become part of the VLAN that was passed through the trunk. The network now appears to the devices as:



The devices on the LAN don't realize they are, in fact, part of a VLAN. They act as if they are directly connected to the current network. Layer 2 traffic (for example, ARP) can flow directly between them.

Theory

The standard for VLANs is 802.1q, otherwise known as Dot1q. We achieve VLAN communication by adding extra information to each Ethernet frame. This extra information identifies the packet as a VLAN packet. Only interfaces configured to listen for the specific VLAN will respond to it. This works in much the same way as the MAC address in the Ethernet frame. The VLAN header is 4 bytes and is inserted in the Ether Type field. Interfaces that don't support 802.1q will ignore the packet.

For more information, visit:

www.digi.com

877-912-3444 | 952-912-3444

Standard Ethernet Frame

	Preamble	Dst Mac	Src Mac	Ether Type	Payload	CRC	GAP
Bytes	8	6	6	2	46..MTU	4	12

VLAN Ethernet Frame

	Preamble	Dst Mac	Src Mac	802.1q Header	Ether Type	Payload	CRC	GAP
Bytes	8	6	6	4	2	42..MTU	4	12

The 802.1q header is 32 bits (4 bytes) long, comprised of a 16-bit tag protocol identifier (0x8100), a 3-bit priority code, a 1-bit drop code, and a 12-bit VLAN identifier.

802.1q Header

Field	TPID	PCP	DEI	VID
Number of Bits	16	3	1	12

A VID (VLAN identifier or VLAN ID) of 12 bits means VLANs can be numbered from 1 to 4094. (VLAN IDs 0 [0x000] and 4095 [0xfff] are reserved and can't be used.) An interface communicating over a VLAN only responds when the VID matches the interface VID. Standard interfaces won't match the packet, because the Ethernet type doesn't match the standard frame type. When the frame enters an interface and matches the VID, the payload is handled in the same way as a normal Ethernet frame. Frames leaving the interface are tagged with the 802.1q header to show they are part of a VLAN. All other network functionality behaves the same as it would for standard frames.

Traditional VLANs in DAL OS

Traditionally, DAL OS created a VLAN interface that only listens for traffic on the VLAN with a configured VID. Once processed by the interface, the VLAN tags are stripped, and the packet continues as a standard Ethernet frame. Any traffic that exits the system through the VLAN interface is tagged with the correct VLAN header and can be processed by another device on the same VLAN. This works well for simple VLAN networking between two devices. One device could be a switch, so VLAN packets can be routed across a third-party VLAN. Once processed internally by the DAL OS, the packet loses the VLAN tagging and becomes simple TCP traffic. For most applications, this can suffice. However, if the DAL OS device was the VLAN router, packets must traverse DAL OS with their tagging intact.

Trunking VLANs in DAL OS

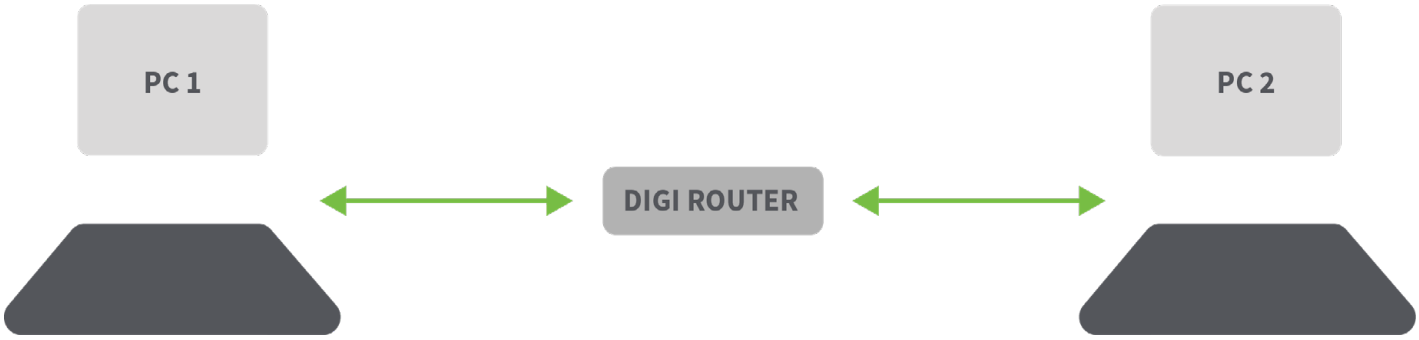
Bridges in Linux have two basic modes of operation — VLAN-aware, and VLAN-unaware. The normal mode for bridges is VLAN-unaware — these simply move packets (unaltered) between devices attached to the bridge. They don't understand VLANs and can't react to them. The second mode is VLAN-aware. In this mode, the bridge explicitly listens for VLAN-tagged packets and will route those packets to other devices it knows can handle that VLAN. Another capability is to give a default tag to an inbound VLAN-untagged packet.

An interface attached to a VLAN-aware bridge can do several things. It can allow specified VLANs to pass, tag a packet that isn't currently in a VLAN (Port VLAN ID, or PVID), strip the VLAN tag when the packet leaves the interface, or block other VLANs.

A VLAN trunk is a network connection that carries multiple VLANs and connects two routers/switches (hereinafter "switch"). This means a VLAN packet on one switch can be sent to another switch so that a device on the second switch believes the device on the first switch is on the same physical LAN. This means your VLAN could have devices in two different locations, yet both will act as if they are on a single, simple LAN. Protocols like ARP and DHCP will work, even though the devices aren't on a single physical connection.

Client Device 1 and 2 are connected via a trunk between two switches

As far as the devices are concerned, the network behaves as follows:

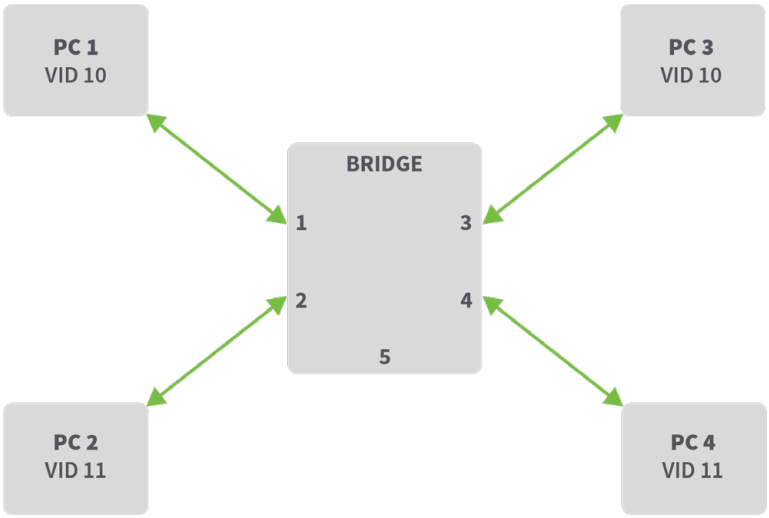


Without the VLAN trunking, ARP requests could not be serviced between Device 1 and Device 2, because they would be considered to be on different physical subnets, and hence not applicable.

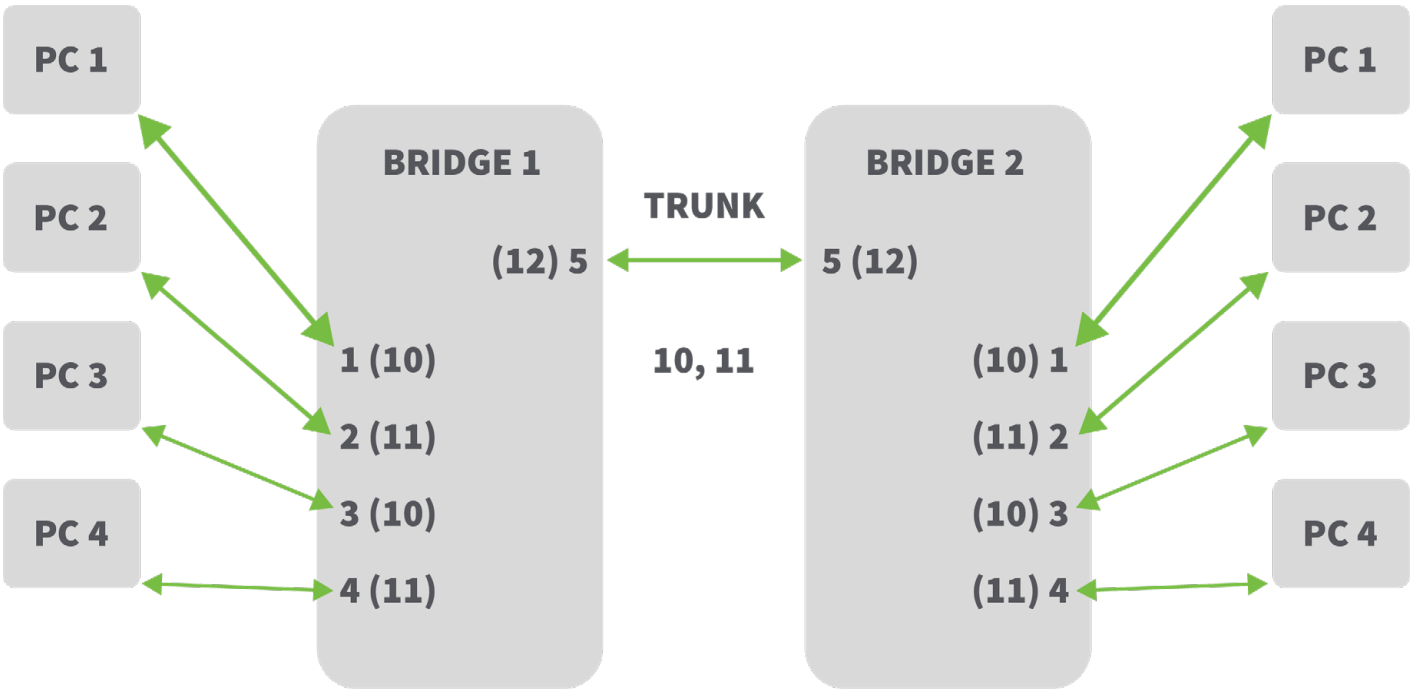
Setting up VLAN/Trunking in DAL OS

When set to VLAN-aware mode, all devices attached to the bridge specify which VLANs they support. Each interface (port) can be set up with a PVID (Port VLAN ID). It's the default VLAN ID to assign to a packet that comes in on that Ethernet port without a VLAN tag. This is the VID the packet is tagged with if it enters without a VLAN tag. Any packet tagged with the PVID leaving the bridge through the port will be stripped of the VLAN tag and allowed through. Any packet not on the correct VLAN will be ignored. Ports can support multiple VIDs, but they only have one PVID. If a port supports a VID, but it is not the PVID, the packet goes through with the VLAN tag intact. For example:

DAL VLAN Bridge Setup



In the above example, ports 1 and 3 are set to PVID 10, and ports 2 and 4 are set to PVID 11. PC 1 can communicate with PC 3, but it is isolated from PC 2 and PC 4. Similarly, PC 2 can communicate with PC 4, but it is isolated from PC 1 and PC 3. None of the PCs need any knowledge about VLANs, as the port will tag an incoming packet and strip an outgoing packet. The PC will not know it is on a VLAN and will act as if it is connected to a conventional LAN.



Port 5 can be set as a trunk and pass VIDs 10 and 11, and have its own PVID (native) of 12. If we had another switch with an identical setup and connected to the first switch via port 5, PC 1 on switch 1 could talk with PC 1 on switch 2. If we follow the packets, we will see how.

For example: A packet from PC 1 is a standard Ethernet frame with no tagging. The packet comes in through LAN1, which is attached to port 1 of the bridge. This will tag the frame with the VID 10 because the port is set up as PVID 10. The bridge sends the packet to port 3 and port 5 as they are the only ones that accept VID 10. PC 2 ignores the packet because it was not destined for it. Port 5 passes the still-tagged packet to the second switch. Then the process is reversed. On switch 2, port 5 accepts the packet, keeps the tag (because it wasn't the PVID), and sends the packet to ports 1 and 3, which both accept VID 10. When the packet leaves the interface, the VLAN tag is stripped and the devices behave as if this were a standard packet. PC 1 detects and accepts the packet that is directed toward it, and responds. This process repeats.

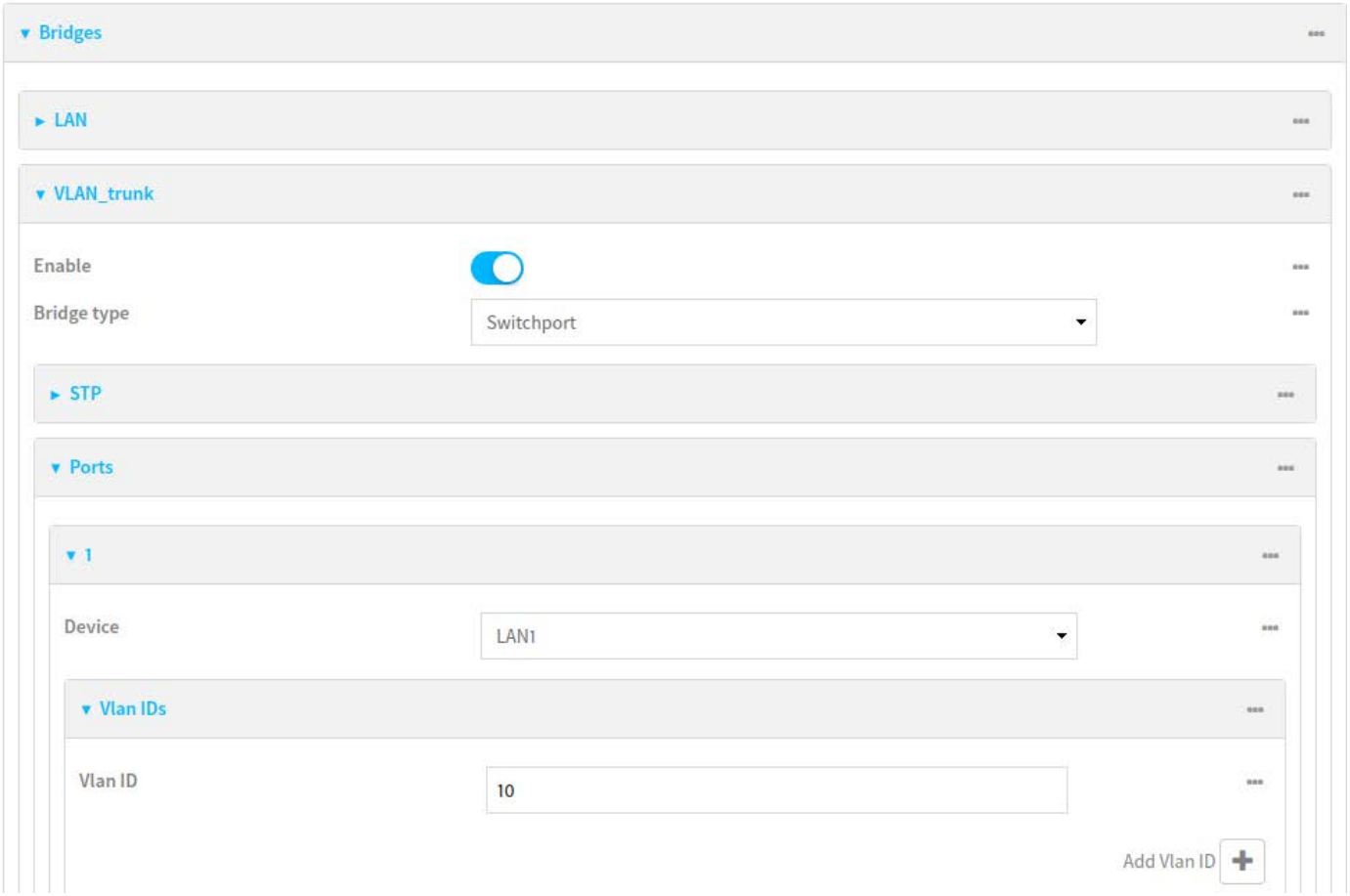
The trunk gets a PVID for two reasons. First, any untagged (i.e. non-VLAN) packets would otherwise be blocked.

Second, we need the other VLANs (10 and 11) to pass without being stripped of their VLAN tags. Only the PVID has its tag added or stripped.

In DAL OS, once a bridge is set to VLAN trunking mode, we add interfaces to the bridge, and specify a list of VIDs to support. The first VID is always the PVID. In the example above, we would set up a switchport (i.e. VLAN-aware) bridge with:

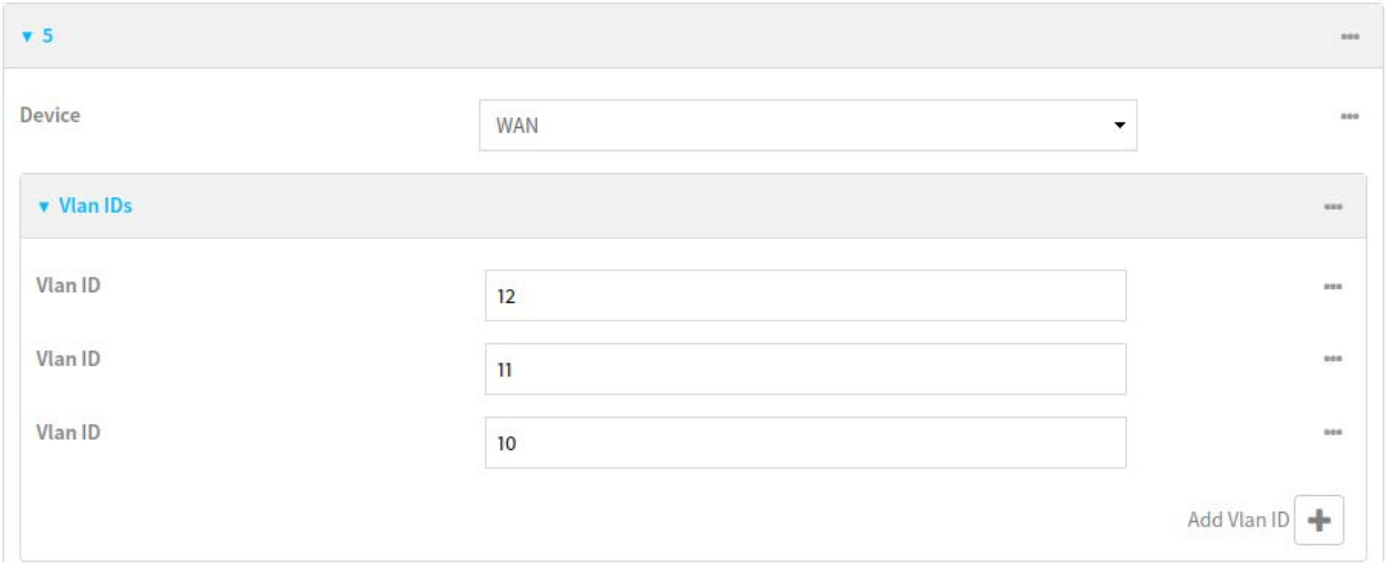
Port Name	Device	VID(s)
1	LAN1	10
2	LAN2	11
3	LAN3	10
4	LAN4	11
5	WAN	12 10 11

So, LAN1 and LAN3 have PVID set to 10 and accept no other VLANs. LAN2 and LAN4 have PVID set to 11 and accept no other VLANs. And the WAN interface is set up as a trunk, with native VID (i.e. PVID) of 12 and allowing VIDs 10 and 11 to pass.



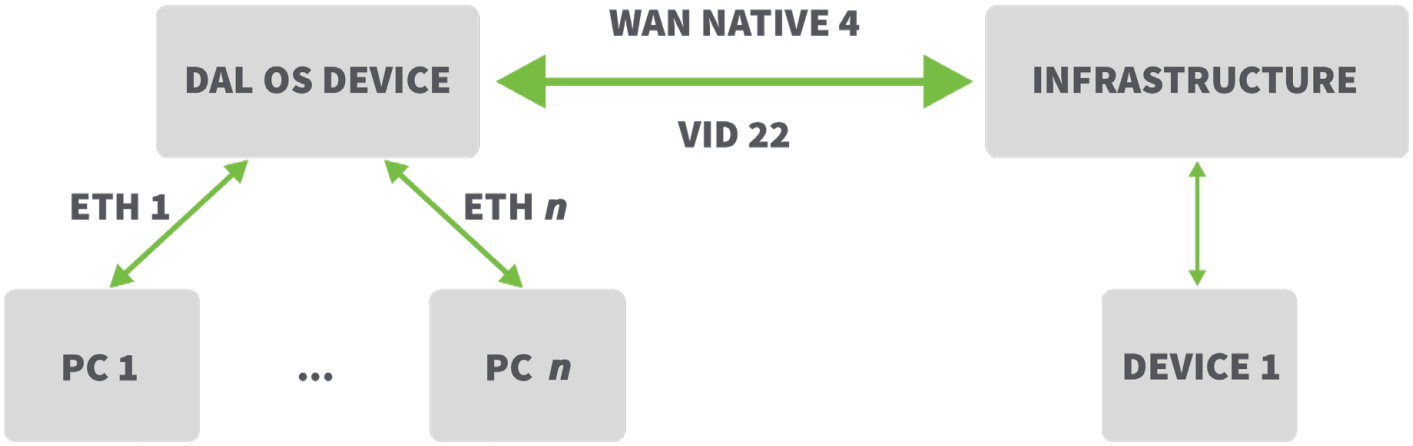
DAL OS Configuration for Switchport Bridge

The process in the screenshot above is repeated for ports 2, 3, and 4. The trunk on the WAN interface looks like this:



Example Configuration

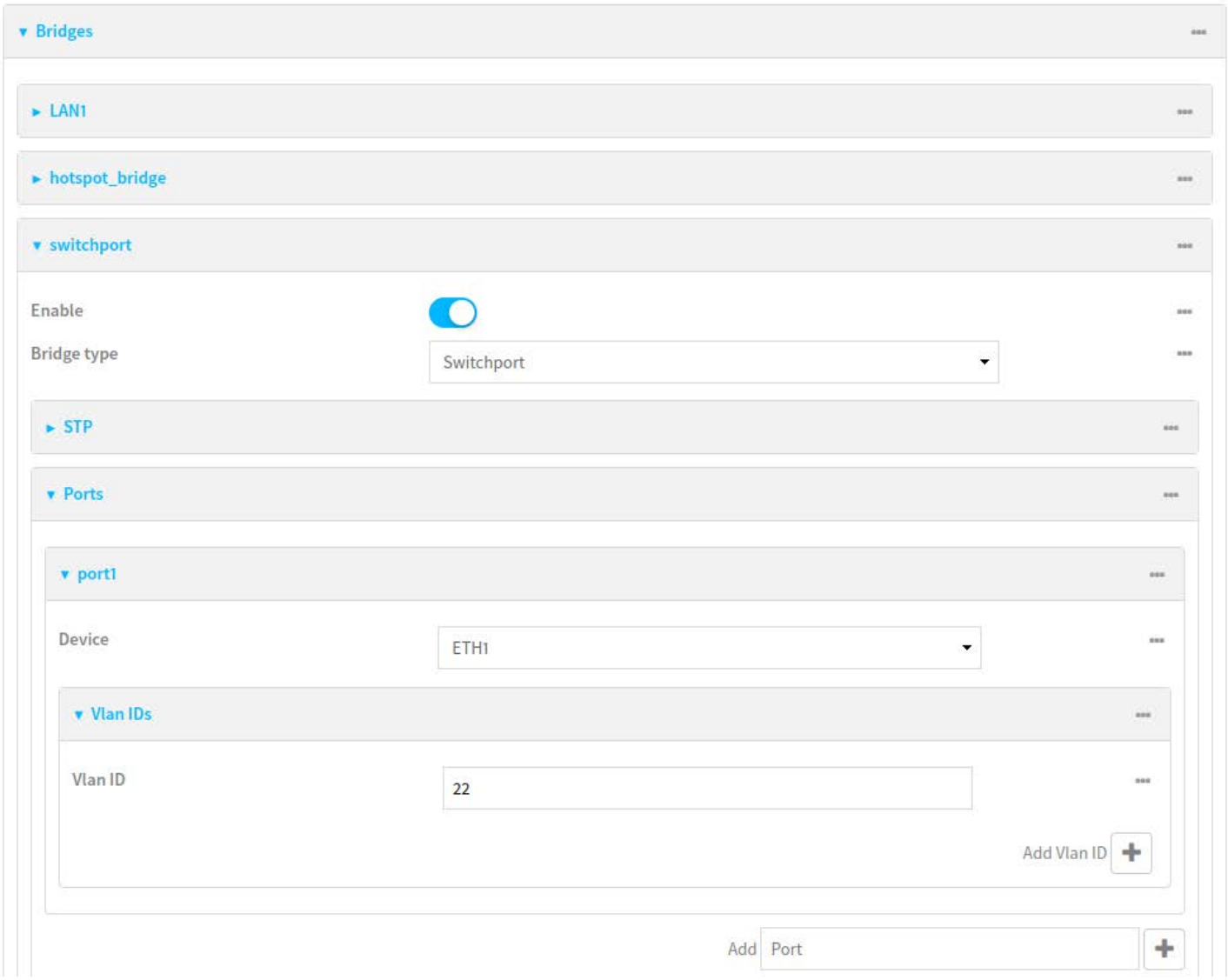
For example, suppose we want to integrate a DAL OS device into an existing VLAN solution. The infrastructure has many VLANs and has assigned the DAL device VLAN ID 22. A printer (Device 1) on the infrastructure must be accessible to the devices connected to the DAL device. The DAL device is connected to the infrastructure through a native trunk with ID 4. VLAN 22 will have IP addresses assigned by the DAL device.



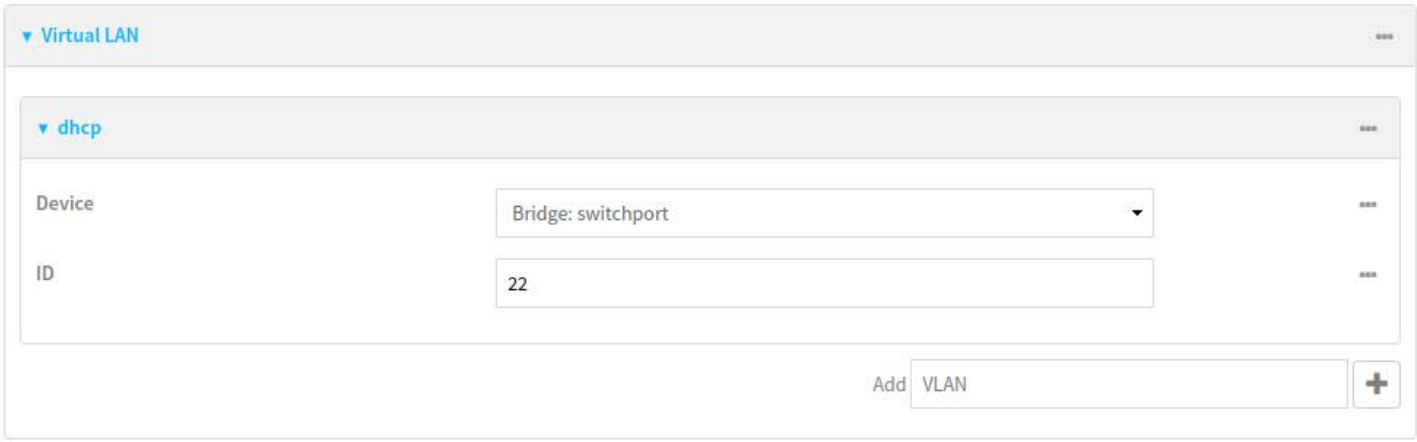
PC 1 to PC *n* and Device 1 are all on VLAN ID 22. This means PC 1 can communicate with Device 1 and all appear to be on a common subnet. We would set up a switchport bridge with the following parameters:

Port Name	VLAN ID	Device
Port 1	22	ETH 1
...	22	...
Port *n*	22	ETH *n*
Trunk	4, 22	WAN

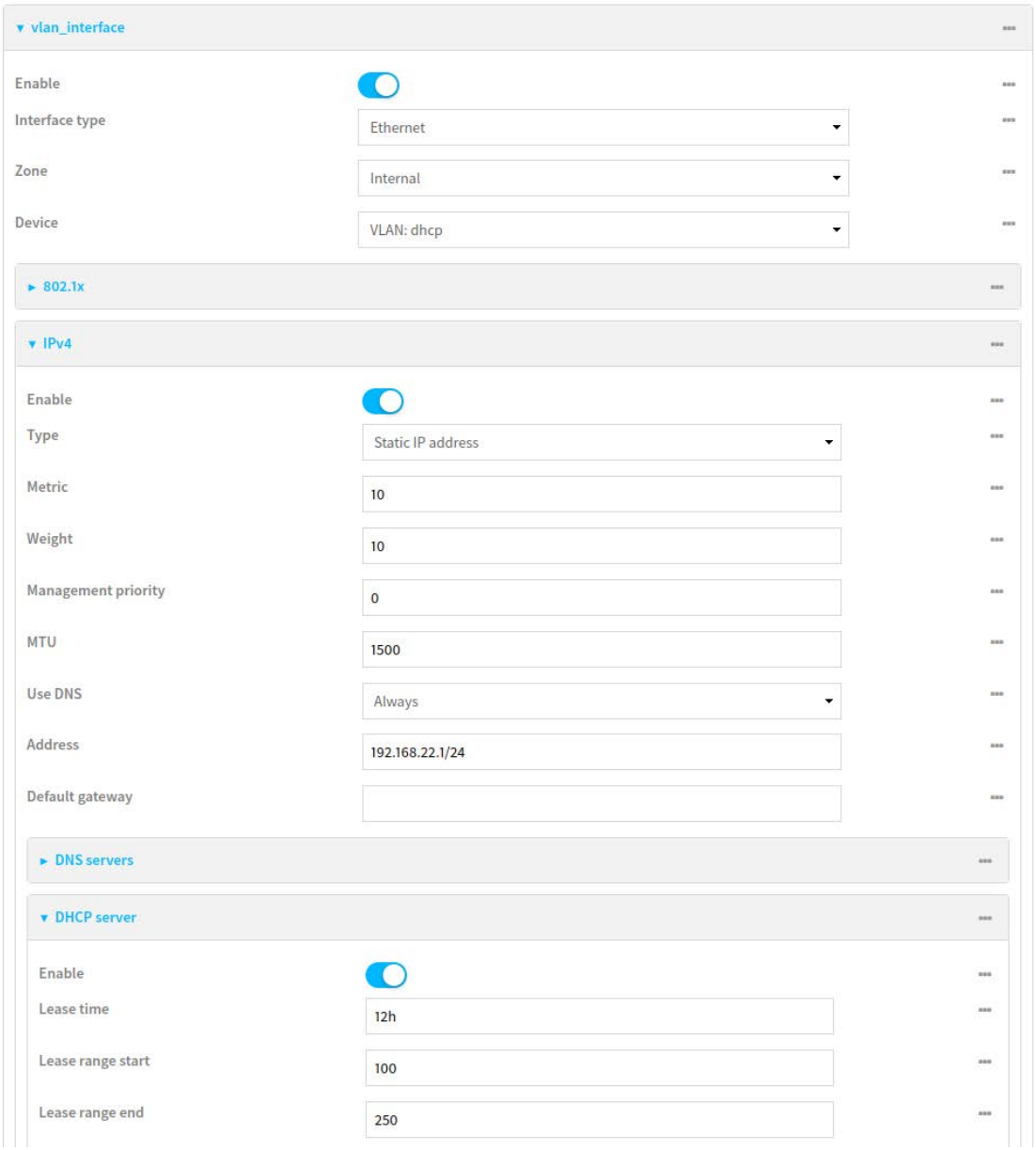
This takes care of the network. Now we need the DHCP server. Because a switchport bridge filters all packets that don't match the VLAN IDs associated with it, any system service connected with the VLAN must be on that VLAN. We create a DAL VLAN interface on the switchport bridge with a VLAN ID of 22.



We repeat this setup for all the ports required (i.e. ETH 2, ETH 3, and so on). We now create the DHCP interface by creating a VLAN interface on the switchport bridge with a VLAN ID of 22.



Next, we create the interface on the VLAN device and enable DHCP. This allows devices on VLAN 22 to access the DHCP server and obtain an address.



The devices connected to ETH 1 ... ETH *n*, as well as the printer (Device 1) can now get a DHCP address from the DAL device on VLAN 22. They can communicate with each other as if they are on a native LAN and are now integrated into the infrastructure.

Summary: The Benefits of VLAN Trunking and Networking

In many cases, the networking offered by DAL-based devices may be better suited to a customer's needs than a traditional VLAN. However, if the infrastructure already makes use of VLAN networking, the ability to integrate a DAL OS device into the customer network may be the difference between using the DAL device or not. DAL OS supports simple one-to-one VLAN interfaces, full VLAN trunking, or a combination of the two. This flexibility gives DAL-based devices a competitive edge in a crowded marketplace.

Next Steps

- Seeking the right solution to implement advanced VLAN capabilities? Contact Us
- Need assistance setting up VLANs on your Digi device? Contact Technical Support
- Want to hear about new products and announcements? Sign up for our newsletter

For more information, visit:

www.digi.com

877-912-3444 | 952-912-3444

 91004549 A3/622