



Virtual Networking on AIX 5L



Vinit Jain
IBM Corporation

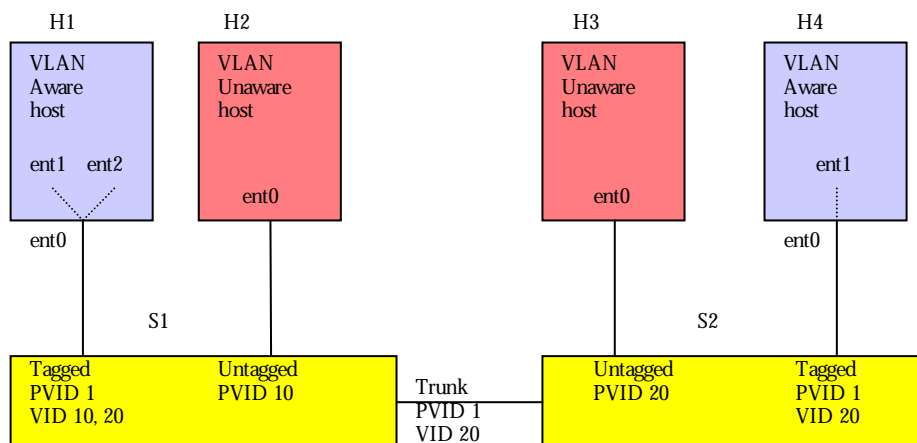
Introduction

Virtual Ethernet technology is supported on AIX 5L™ V5.3 on POWER5™ hardware. This technology enables IP-based communication between logical partitions on the same system using a VLAN capable software switch in POWER5 systems. Shared Ethernet Adapter (SEA) technology (part of the optional Virtual I/O server feature on POWER5 hardware) enables the logical partitions to communicate with other systems outside the hardware unit without assigning physical Ethernet slots to the logical partitions.

Virtual networking along with other POWER5 virtualization technologies offers greater flexibility in configuration scenarios. Workloads can be easily consolidated with more control over resource allocation. Network availability can also be improved for more systems with fewer resources using a combination of Virtual Ethernet, Shared Ethernet and link aggregation in the Virtual I/O server. When there are not enough physical slots to allocate a physical network adapter to each LPAR network access using Virtual Ethernet and a Virtual I/O server is a preferable to IP forwarding as it does not complicate the IP network topology.

1. Background Technologies

1.1 VLAN (Virtual Local Area Network)



Ethernet Switches S1 and S2 share VLAN 20 through tagged trunk ports. Hosts H1, H2 share network VLAN 10. Hosts H1, H3 and H4 share network VLAN 20.

VLAN is described by the IEEE 802.1Q standard. VLAN is a method to logically segment a physical network such that layer 2 connectivity is restricted to members that belong to the same VLAN. This separation is achieved by tagging Ethernet packets with their VLAN membership information and then restricting delivery to members of that VLAN.

The VLAN tag information is referred to as VLAN ID (VID). Ports on a switch are configured as being members of VLAN designated by the VID for that port. The default VID for a port is referred to as the Port VID (PVID). The VID can be added to an Ethernet packet either by a

VLAN aware host or by the switch in the case of VLAN unaware hosts. Therefore ports on an Ethernet switch have to be configured with information indicating whether the host connected is VLAN aware or unaware. For VLAN unaware hosts, a port is set up as untagged and the switch will tag all packets entering through that port with the Port VLAN ID (PVID). It will also untag all packets exiting that port before delivery to the VLAN unaware host. A port used to connect VLAN unaware hosts is called an untagged port, and it can only be a member of a single VLAN identified by its PVID. Hosts that are VLAN aware can insert and remove their own tags and can be members of more than one VLAN. These hosts are typically attached to ports that do not remove the tags before delivering the packets to the host, but will insert the PVID tag when an untagged packet enters the port. A port will only allow packets that are untagged or tagged with the tag of one of the VLANs the port belongs to. These VLAN rules are in addition to the regular MAC address based forwarding rules followed by a switch. Therefore, a packet with a broadcast or multicast destination MAC will also get delivered to member ports that belong to the VLAN that is identified by the tags in the packet. This mechanism ensures the logical separation of physical network based on membership in a VLAN.

As VLAN ensures logical separation at layer 2, it is not possible to have an IP network that spans multiple VLANs (different VIDs). A router that belongs to both VLAN segments and forwards packets between them is required to communicate between hosts on different VLAN segments. However a VLAN can extend across multiple switches by ensuring that the VIDs remain the same and the trunk ports are configured with the appropriate VIDs. Typically a VLAN capable switch will have a default VLAN (1) defined. The default setting for all its ports is such that they belong to the default VLAN and therefore have a PVID 1 and assume that all hosts connecting will be VLAN unaware (untagged). This setting makes such a switch equivalent to a simple Ethernet switch that does not support VLAN.

On AIX 5L, VLAN tagging and untagging is configured by creating a VLAN device (e.g. ent1) over a physical (or virtual) Ethernet device (e.g. ent0) and assigning it a VLAN tag ID. An IP address is then assigned on the resulting interface (e.g. en1) associated with the VLAN device. AIX 5L supports multiple VLAN devices over a single Ethernet device each with its own VID. Each of these VLAN devices (ent) is an endpoint to access the logically separated physical Ethernet network and the interfaces (en) associated with them are configured with IP addresses belonging to different networks.

In general, configuration is simpler when ports are untagged and only the PVID is configured because the attached hosts do not have to be VLAN aware and they do not require any VLAN configuration. However this scenario has the limitation that a host can access only a single network using a physical adapter. Therefore untagged ports with PVID only are preferred when accessing a single network per Ethernet adapter and additional VIDs should be used only when multiple networks are being accessed through a single Ethernet adapter.

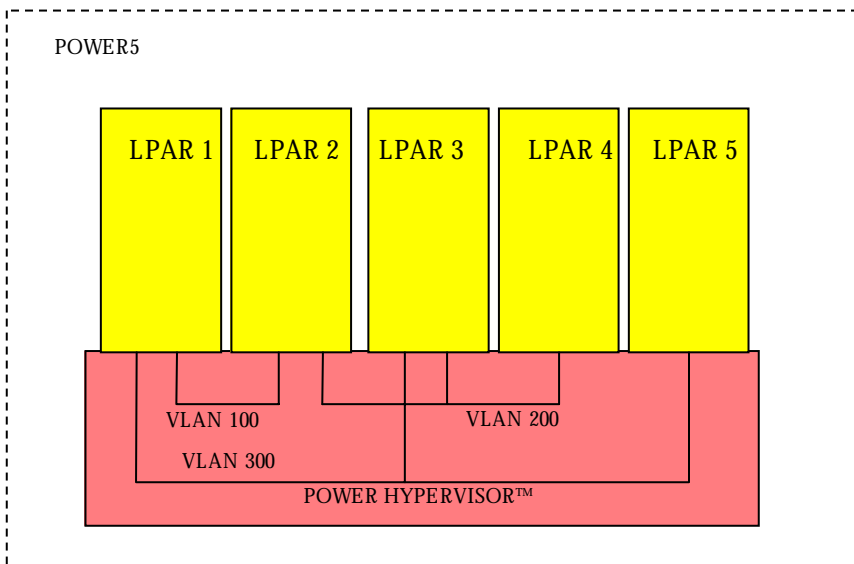
1.2 Link Aggregation

Link Aggregation (also known as EtherChannel) is a network port aggregation technology that allow several Ethernet adapters to be aggregated together to form a single pseudo Ethernet device. For example, ent0 and ent1 can be aggregated to ent3; interface en3 would then be configured with an IP address. The system considers these aggregated

adapters as one adapter. Therefore, IP is configured over them as over any Ethernet adapter. In addition, all adapters in the Link Aggregation are given the same hardware (MAC) address, so they are treated by remote systems as if they were one adapter. The main benefit of Link Aggregation is that they have the network bandwidth of all of their adapters in a single network presence. If an adapter fails, the packets are automatically sent on the next available adapter without disruption to existing user connections. The adapter is automatically returned to service on the Link Aggregation when it recovers.

2. POWER5 Network Virtualization

2.1 Virtual Ethernet Adapters



Virtual Ethernet used to communicate between partitions of the same hardware unit. LPAR 1, 2 use VLAN 100. LPAR 2, 3, 4 use VLAN 200. LPAR 1, 3, 5 use VLAN 300

POWER5 hardware supports inter-LPAR communication using virtual networking. The POWER Hypervisor on POWER5 systems supports Virtual Ethernet adapters that are connected to an IEEE 802.1q (VLAN) style Virtual Ethernet switch. Using this switch function LPARs can communicate with each other by using Virtual Ethernet adapters and assigning VIDs (VLAN ID) that enable them to share a common logical network. The Virtual Ethernet adapters are created and the VID assignments are done using the Hardware Management Console (HMC). The POWER Hypervisor transmits packets by copying the packet directly from the memory of the sender partition to the receive buffers of the receiver partition without any intermediate buffering of the packet.

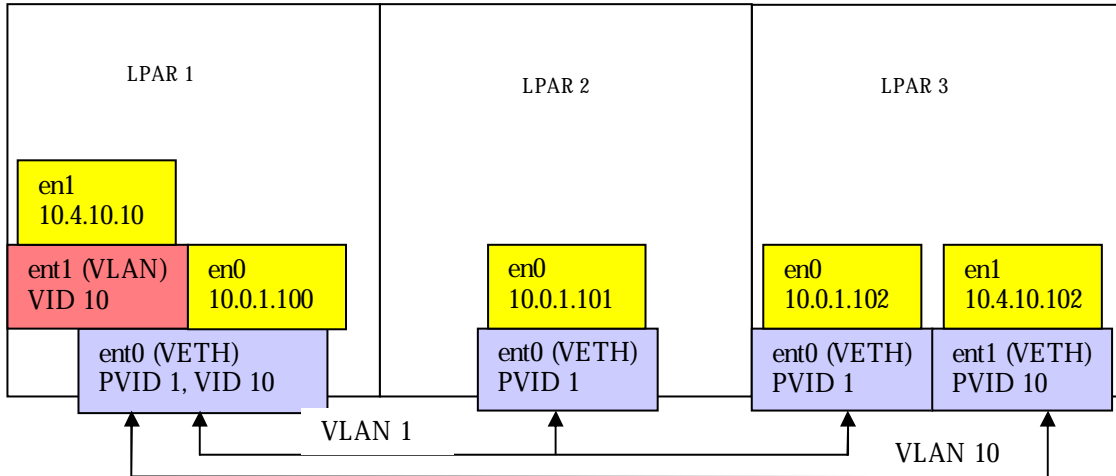
The number of Virtual Ethernet adapters per LPAR varies by operating system with AIX 5L V5.3 limiting it to 256 Virtual Ethernet per LPAR. Besides a PVID, the number of additional VID values that can be assigned per Virtual Ethernet adapter is 20 which imply that each Virtual Ethernet adapter can be used to access 21 networks. The HMC generates a locally administered Ethernet MAC address for the Virtual Ethernet adapters so that these

addresses do not conflict with physical Ethernet adapter MAC addresses. To ensure uniqueness among the Virtual Ethernet adapters, the address generation is based on the system serial number, LPAR ID and adapter ID.

For VLAN unaware operating systems, each Virtual Ethernet adapter should be created with only a PVID (no additional VID values) and the Hypervisor will ensure that packets have their VLAN tags removed before delivering to that LPAR. In the case of VLAN aware systems, one can assign additional VID values besides the PVID and the Hypervisor will only strip the tags of any packets which arrive with the PVID tag. Since the number of Virtual Ethernet adapters supported per LPAR is quite large, one can have multiple Virtual Ethernet adapters with each adapter being used to access a single network and therefore assigning only PVID and avoiding the additional VID assignments. This also has the advantage that no additional VLAN configuration is required for the operating system using these Virtual Ethernet adapters.

After creating Virtual Ethernet adapters for an LPAR using the HMC, the operating system in the partition they belong to will recognize them as a Virtual Ethernet device. These adapters appear as Ethernet adapter devices (entX) of type Virtual Ethernet. Similar to physical Ethernet adapters on AIX 5L, a VLAN device can be configured over a Virtual Ethernet adapter. A Virtual Ethernet device that only has a PVID assigned through the HMC does not require VLAN device configuration as the Hypervisor will strip the PVID VLAN tag. A VLAN device is required for every additional VLAN ID that was assigned the Virtual Ethernet adapter when it was created using the HMC so that the VLAN tags are processed by the AIX 5L VLAN device.

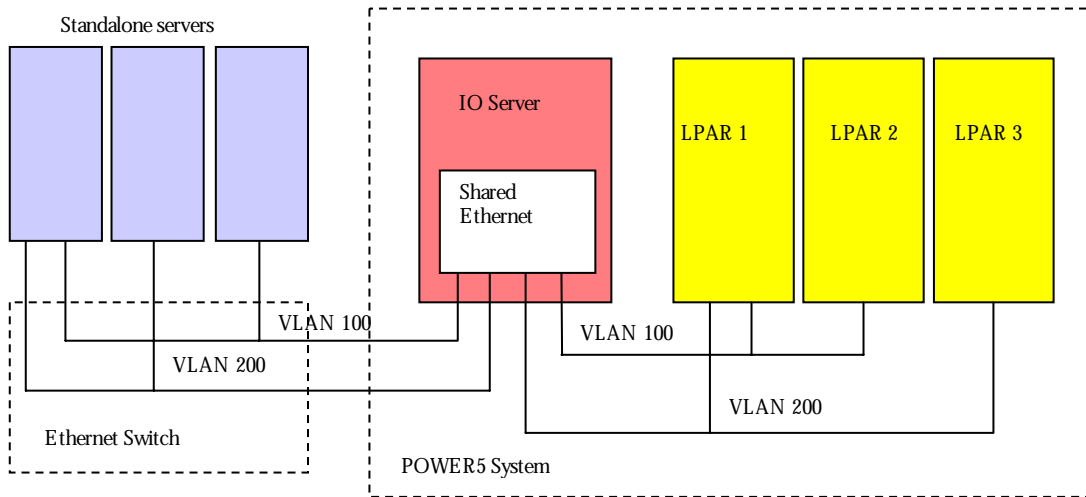
The Virtual Ethernet adapters can be used for both IPv4 and IPv6 communication and can transmit packets with a size up to 65408 bytes. Therefore, the maximum MTU for the corresponding interface can be up to 65394 (65390 with VLAN tagging). Since the Shared Ethernet Adapter (described in section 2.2) can only forward packets of size up to the MTU of the physical Ethernet adapters a lower MTU or PMTU discovery should be used when the network is being extended using the Shared Ethernet. The AIX 5L V5.3 device driver for Virtual Ethernet maintains memory pools of multiple sizes to optimally handle packets up to the maximum supported MTU. All applications designed to communicate using IP over Ethernet should be able to communicate using the Virtual Ethernet adapters. As the firmware does not understand VLAN tagged packets, the Virtual Ethernet device can be used for network boot and installation only on the network which corresponds to its PVID. Link aggregation on Virtual Ethernet networks is not supported as Virtual Ethernet adapters are limited only by system resources and do not have wire speed limitations like physical adapters.



Virtual adapters using PVID only (LPAR 2, 3) and with additional VIDs (LPAR 1)

The above picture shows a POWER5 system with three AIX 5L LPARs. LPAR 1 has a single Virtual Ethernet adapter (ent0) which was created with PVID 1 and VID 10. LPAR 1 has a VLAN device ent1 (VID 10) created over the base Virtual Ethernet adapter ent0 that is used to communicate with the VLAN 10 network. LPAR 1 can also communicate with other hosts on the VLAN 1 network using the ent0 device as the Hypervisor will strip the PVID tags before delivering packets to ent0 and add PVID tags to any packets that do not already have a tag. LPAR 2 also has a single Virtual Ethernet adapter (ent0) which was created with PVID 1 and no additional VIDs and therefore it does not need any VLAN devices configuration. It communicates over the VLAN 1 network by simply using the interface over the Virtual Ethernet device ent0. LPAR 3 has two Virtual Ethernet adapters (ent0, ent1) created with PVID 1 and PVID 10 respectively and neither has any additional VIDs defined. Therefore, LPAR 3 can communicate over both VLAN 1 and VLAN 10 networks using Virtual Ethernet devices ent0 and ent1 respectively.

2.2 Shared Ethernet Adapters



Shared Ethernet is used to extend VLAN 100 and 200 using the physical Ethernet in the Virtual I/O server

While Virtual Ethernet technology is able to provide communication between LPARs on the same system, network access outside the system requires physical adapters. One way to do this is to assign a physical network adapter to every LPAR that requires access to the outside network. However this may not always be possible due to cost or IO slot limitations especially for LPARs that do not have high network traffic flow. A special partition called the Virtual I/O server is available on POWER5 systems. As the name Virtual I/O server implies this partition is an encapsulated device partition that provides IO services like network, disk, tape and other access to the partitions without requiring each partition to own a device. There are no configuration limits on the number of Virtual I/O server partitions supported on POWER5 systems. The network access component of the Virtual I/O server is called the Shared Ethernet Adapter (SEA).

A Shared Ethernet adapter is a bridge between a physical Ethernet adapter or aggregation of physical adapters and one or more Virtual Ethernet adapters on the Virtual I/O server. A SEA enables LPARs on the Virtual Ethernet to share access to the physical Ethernet and communicate with standalone server and LPARs on other systems. The Shared Ethernet provides this access by connecting the internal Hypervisor VLANs with the VLANs on the external switches. This enables LPARs on POWER5 systems to share the IP subnet with stand alone systems and other POWER5 LPARs to allow for a more flexible network. As the Shared Ethernet processes packets at layer 2, the original MAC address and VLAN tags of the packet is visible to other systems on the physical network.

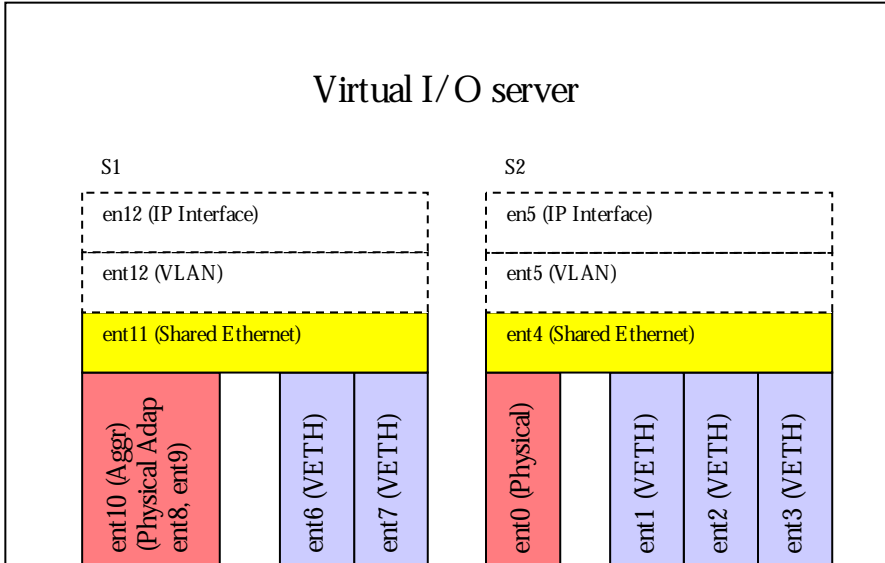
The Virtual Ethernet adapters that are used to configure a Shared Ethernet adapter are required to have the trunk setting enabled from the HMC. The trunk setting causes these Virtual Ethernet adapters to operate in a special mode so that they can deliver and accept external packets from the POWER5 internal switch to the external physical switches. The trunk setting should only be used for the Virtual Ethernet adapters that are part of a Shared Ethernet setup in the Virtual I/O server. A Virtual Ethernet adapter with the trunk setting

becomes the Virtual Ethernet trunk adapter for all the VLANs that it belongs to. Since there can only be one Virtual Ethernet adapter with the trunk setting per VLAN any overlap of the VLAN memberships should be avoided between the Virtual Ethernet trunk adapters.

Shared Ethernet Adapters (SEA) are configured in the Virtual I/O server partition. Setup of a SEA requires one or more physical Ethernet adapters assigned to the I/O partition and one or more Virtual Ethernet adapters with the trunk property defined using the HMC. The physical side of the SEA is either a single Ethernet adapter or a link aggregation of physical adapters. The link aggregation can also have an additional Ethernet adapter as a backup in case of failures on the network. The SEA setup requires the administrator to specify a default trunk adapter on the virtual side (PVID adapter) that will be used to bridge any untagged packets received from the physical side and also specify the PVID of the default trunk adapter. A single SEA setup can have up to 16 Virtual Ethernet trunk adapters and each Virtual Ethernet trunk adapter can support up to 20 VLAN networks. Therefore, it is possible for a single physical Ethernet to be shared between 320 internal VLAN. The number of Shared Ethernet Adapters that can be set up in a Virtual I/O server partition is limited only by the resource availability as there are no configuration limits.

The Shared Ethernet directs packets based on the VLAN ID tags and it learns this information based on observing the packets originating from the Virtual Ethernet adapters. Most packets including broadcast (e.g. ARP) or multicast (e.g. NDP) packets that pass through the Shared Ethernet setup are not modified. These packets retain their original MAC header and VLAN tag information. When the MTU of the physical and virtual side do not match this can result in the Shared Ethernet receiving packets that cannot be forwarded because of MTU limitations. This situation is handled by processing the packets at the IP layer by either doing IP fragmentation or reflecting ICMP errors (packet too big) to the source based on the IP flags in the packet. In the case of IPv6, the packets ICMP errors are sent back to the source as IPv6 allows fragmentation only at the source host. These ICMP errors help the source host discover the PMTU and therefore handle future packets appropriately.

The physical and virtual adapters that are part of a Shared Ethernet configuration are for exclusive use of the Shared Ethernet and therefore can not be configured with IP addresses. The Shared Ethernet adapter itself can be configured with an IP address to provide network connectivity to the Virtual I/O server. The configuration of an IP address for the Shared Ethernet adapter is optional as it is not required for the device to perform the bridge function at layer 2.

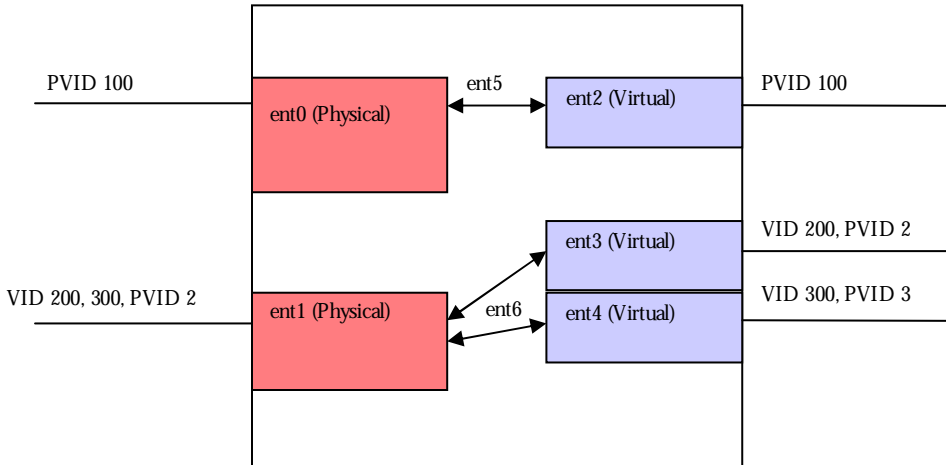


The picture above shows a Virtual I/O server partition with two Shared Ethernet Adapters S1 and S2. Shared Ethernet S2 (ent4) is set up using a physical adapter (ent0) and three virtual trunk adapters (ent1, ent2 and ent3). The VLAN networks which ent1, ent2 and ent3 represent are extended to the external network through the physical adapter ent0. One can further create VLAN devices using the Shared Ethernet Adapter ent4 and use these VLAN devices to enable the Virtual I/O server communication with LPARs on the virtual side and the standalone servers on the physical side. One VLAN device is required for each network the Virtual I/O server wishes to communicate with. The Shared Ethernet device ent4 can be used without the VLAN device to communicate with other LPARs on the VLAN network represented by the PVID of the SEA. The picture above also shows a Shared Ethernet S1 (ent11) which has been set up in the same Virtual I/O server partition as S2. The Shared Ethernet S1 uses a link aggregation (ent10) consisting of two physical adapters (ent8, ent9) instead of a single physical adapter. These physical adapters are therefore connected to aggregated ports of an Ethernet switch.

The Shared Ethernet Adapters can optionally be configured with IP addresses to provide network connectivity to the Virtual I/O server without any additionally physical resources. In the picture above, this optional configuration is shown using dotted blocks for the VLAN device and the IP interface.

3. Configuration

3.1 Shared Ethernet Adapter Configuration



The picture above shows an Virtual I/O server with two Shared Ethernet adapters ent5 and ent6 that are set up to connect internal VLAN networks to the external networks.

The Shared Ethernet adapter ent5 uses physical adapter ent0 and virtual adapter ent2. The physical adapter ent0 is connected to a physical Ethernet switch which does not have to be VLAN capable because only PVID is being used in this setup. If the switch is VLAN capable then the port that the physical adapter ent0 connects to should be set up as an untagged port with PVID 100. The virtual adapter is created with the PVID 100 and the trunk setting using the HMC. The following Virtual I/O server command will configure the Shared Ethernet and will effectively connect the LPARs using VLAN 100 to the physical network.

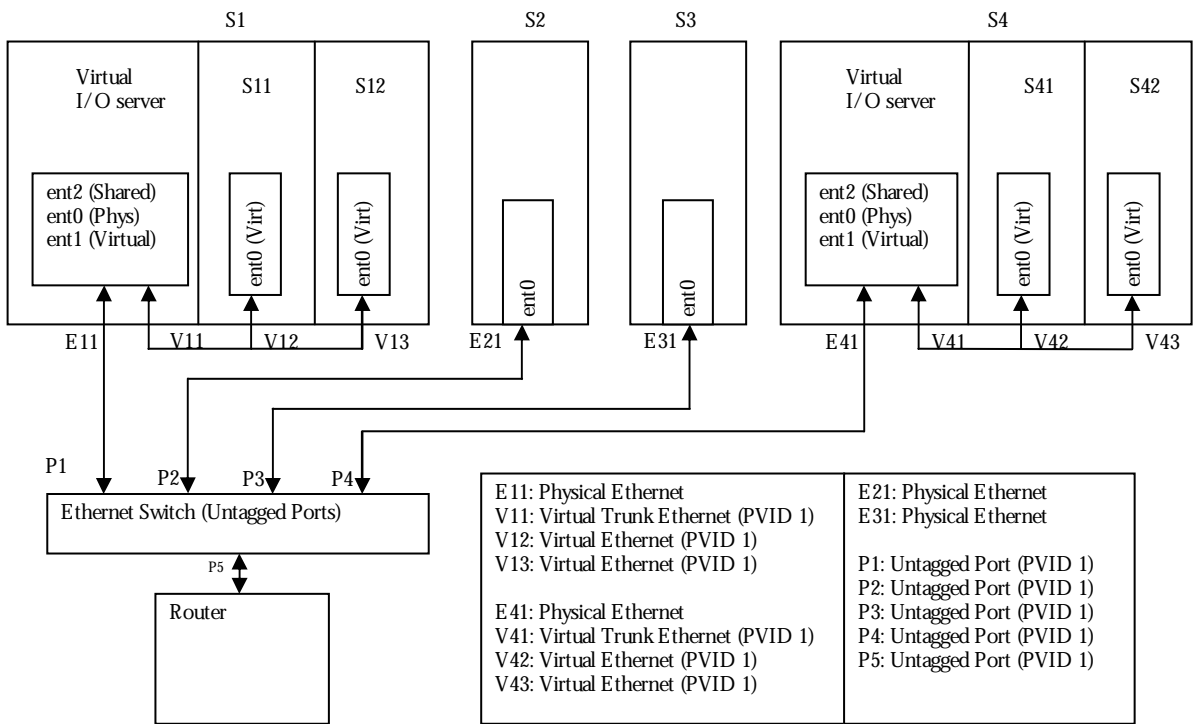
```
mkvdev -sea ent0 -vadapter ent2 -default ent2 -defaultid 100
```

The Shared Ethernet adapter ent6 uses physical adapter ent1 and virtual adapters ent3 and ent4. The physical adapter ent1 is connected to a physical Ethernet switch which is VLAN capable and the port should be set up as a tagged port with PVID 2, VID 200 and VID 300. The virtual adapter ent3 is created with PVID 2 and VID 200 and the trunk setting using the HMC. The virtual adapter ent4 is created with PVID 3 and VID 300 and the trunk setting using the HMC. The Shared Ethernet can only provide PVID connectivity to one of the virtual adapters and the VLAN 2 was chosen as the default PVID in this example. The PVID 3 for virtual adapter ent4 is used only because one cannot create a virtual adapter without a PVID and any other unused PVID value could have been used here. The following Virtual I/O server command will configure the Shared Ethernet and will effectively connect the LPARs on VLAN 2, 200 and 300 to the physical network.

```
mkvdev -sea ent1 -vadapter ent3 ent4 -default ent3 -defaultid 2
```

3.2 Simple Network Setup

A simple network setup describes the simplest case where only PVID is used, the packets are not tagged and a single internal network is connected to a single external network. The picture below shows how a simple network can be set up using IO partition Shared Ethernet adapters. This setup shows a single logical subnet with each server having exactly one adapter to communicate with other systems on the subnet without going through a router. There are no VLAN tagged ports set up on the Ethernet switch and all Virtual Ethernet adapters are defined using a single default PVID and no additional VIDs.



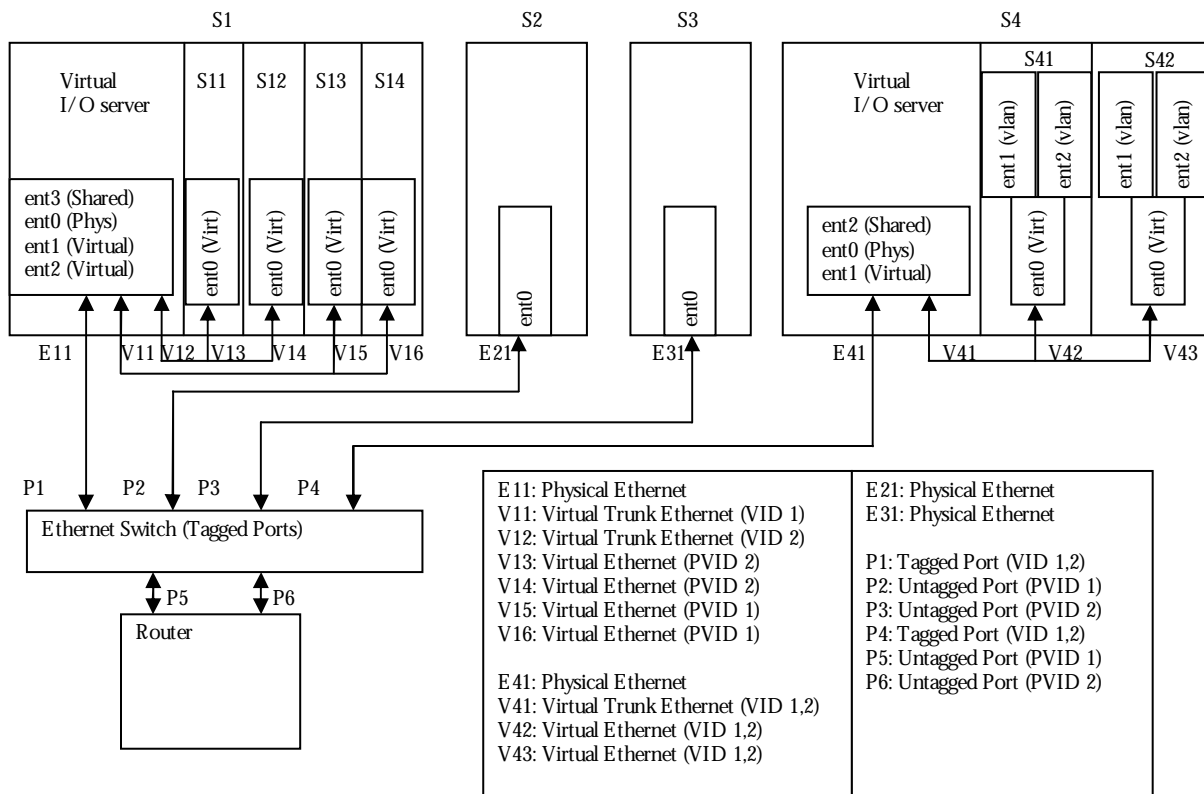
High level description of the steps required to set up the above configuration:

- Set up an Ethernet switch with untagged ports (usually the default setting) or use a switch that does not support VLAN.
- For system S1, using the HMC create a Virtual Ethernet adapter (V11) for the Virtual I/O server with trunk setting and PVID 1 and no additional VIDs.
- For system S1, using the HMC create Virtual Ethernet adapters (V12 and V13) for partitions S11 and S12 with PVID 1 and no additional VIDs.

- For system S1, using the HMC assign a physical Ethernet adapter E11 to the Virtual I/O server and connect the adapter to the Ethernet switch port P1.
- Using the Virtual I/O server interface, set up a Shared Ethernet adapter ent2 with the physical adapter ent0 and virtual adapter ent1.
- Follow the above steps to configure system S4. Systems S2 and S3 are standalone servers with physical Ethernet adapters.
- Now boot up the LPARs so that the devices created above are recognized during the boot process.
- Now configure IP addresses for S11 (en0), S12 (en0), S2 (en0), S3 (en0), S41 (en0), S42 (en0) such that they all belong to the same IP subnet with the router connected to P5 of the Ethernet switch.
- The Shared Ethernet on Virtual I/O servers for S1 (en2) and S4 (en2) can also be configured with IP addresses on the same IP subnet. This is only required for network connectivity to the Virtual I/O servers.

3.3 General Network Setup

A Virtual I/O server with Shared Ethernet adapters can be used to set up a complex network in such a way that multiple networks can share a single physical Ethernet adapter. The picture below shows how a more general network can be setup using IO partition Shared Ethernet adapters. This setup shows two logical subnets with some systems on each subnet and some on both subnets. Systems on the same subnet are required to be on the same VLAN and therefore have the same VLAN IDs so that they can communicate without going through a router. The separation in the subnets is achieved by ensuring that the systems on the two subnets have different VLAN IDs.



High level description of the steps required to set up the above configuration:

- Set up the Ethernet switch ports as follows:
 - P1: Tagged Port (VID 1,2)
 - P2: Untagged Port (PVID 1)
 - P3: Untagged Port (VID 2)
 - P4: Tagged Port (VID 1,2)

P5: Untagged Port (PVID 1)

P6: Untagged Port (PVID 2)

- For system S1, create Virtual Ethernet adapters for the Virtual I/O server:

Create V11 for the Virtual I/O server with trunk setting and VID 1. Specify an unused PVID value (101) as it is required even though it is not used.

Create V12 for the Virtual I/O server with trunk setting and VID 2. Specify an unused PVID value (102) as it is required even though it is not used.

- For system S1, create Virtual Ethernet adapters for other partitions:

Create V13 and V14 for partitions S11 and S12 with PVID 2 and no additional VIDs.

Create V15 and V16 for partitions S13 and S14 with PVID 1 and no additional VIDs

- For system S1, assign a physical Ethernet adapter E11 to the Virtual I/O server and connect the adapter to the Ethernet switch port P1.
- Using the Virtual I/O server interface, set up a Shared Ethernet adapter ent3 with the physical adapter ent0 and virtual adapters ent1 and ent2.
- Systems S2 and S3 are standalone servers with physical Ethernet adapters.
- For system S4, create Virtual Ethernet adapters for the Virtual I/O server:

Create V41 for the Virtual I/O server with trunk setting and VID 1, 2. Specify an unused PVID value (101) as it is required even though it is not used.
- For system S4, create Virtual Ethernet adapters for other partitions:

Create V42 for partitions S41 with VID 1, 2. Specify an unused PVID value (101) as it is required even though it is not used.

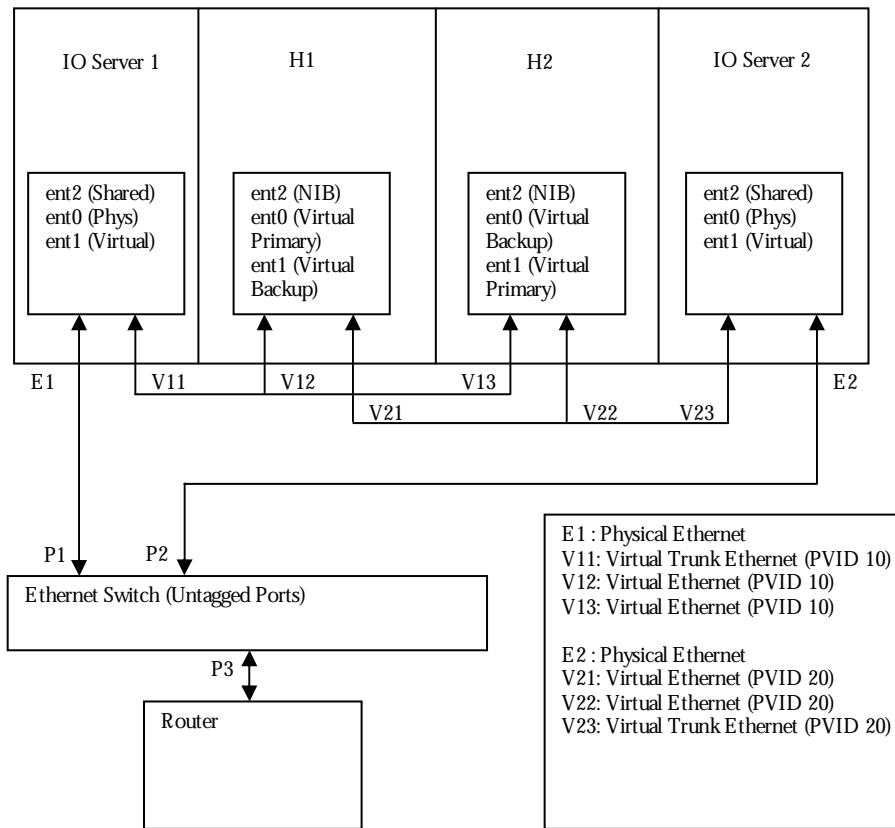
Create V43 for partitions S42 with VID 1, 2. Specify an unused PVID value (101) as it is required even though it is not used.
- For partitions S41 and S42, create VLAN devices ent1 with tag 1 and ent2 with tag 2.
- For system S4, assign a physical Ethernet adapter E41 to the Virtual I/O server and connect the adapter to the Ethernet switch port P4.
- Using the Virtual I/O server interface, set up a Shared Ethernet adapter ent2 with the physical adapter ent0 and virtual adapter ent1.
- Now configure IP addresses:

S13 (en0), S14 (en0), S2 (en0), S41 (en1), S42 (en1) belong to the same VLAN (VLAN 1) and are on the same IP subnet with the router connected to P5 of the Ethernet switch.

S11 (en0), S12 (en0), S3 (en0), S41 (en2), S42 (en2) belong to the same VLAN (VLAN 2) and are on the same IP subnet with the router connected to P6 of the Ethernet switch.

- The Shared Ethernet on Virtual I/O servers for S1 and S4 can also be configured with IP addresses on the same IP subnet. This is only required for network connectivity to the Virtual I/O servers.
- As tagged VLAN is being used, additional VLAN devices have to be defined over the Shared Ethernet adapters before configuring IP addresses.

3.4 High Availability



The picture above shows a highly-available network configuration using multiple Virtual I/O servers. This configuration uses virtual adapters created with only PVID and the physical Ethernet switch uses only untagged ports. The Virtual I/O server 1 has a Shared Ethernet adapter which provides external connectivity to the LPAR H1 and H2 through adapters V12 and V13 respectively. Virtual I/O server 2 has a Shared Ethernet adapter which provides

external connectivity to LPAR H1 and H2 through adapters V21 and V22 respectively. LPAR H1 has the virtual adapters V12 and V21 configured in network interface backup mode such that V12 is the primary and V21 is the backup with the IP address of the router as the address to query for ping heartbeats. This enables LPAR H1 to get its primary connectivity through Virtual I/O server 1 and backup connectivity through Virtual I/O server 2. LPAR H2 has a similar setup except that the virtual adapter V22 is the primary and V13 is the backup. This enables LPAR H2 to get its primary connectivity through Virtual I/O server 2 and backup connectivity through Virtual I/O server 1.

When the primary Virtual I/O server for an adapter fails, the network interface backup mechanism will detect the failure as the path to the gateway will be broken. The network interface backup setup will failover to the backup adapter and therefore get its connectivity via its backup Virtual I/O server.

3.5 Other considerations

Virtual networking uses more system resources to drive the similar network workloads to the physical network compared to a directly attached physical network adapter. Therefore if an LPAR is driving enough traffic to the physical network to consume a physical adapter, it is preferable to allocate physical resources to such a LPAR.

Virtual Ethernet allows fairly large MTU for inter-LPAR communication whereas communication through the Shared Ethernet is limited to much smaller MTU supported by the physical media. Larger MTU will give better performance for most applications and IP fragmentation will impact performance. The Shared Ethernet adapter handles a MTU mismatch by doing IP fragmentation or generating ICMP packets to aid PMTU discovery based on the PMTU discovery setting of the LPAR originating the packets. Therefore, the MTU for the Virtual Ethernet should be chosen such that packets can be sent outside using the Shared Ethernet without IP fragmentation. Furthermore, keeping the PMTU discovery enabled on AIX 5L will ensure that TCP packets are not fragmented in case the MTU of the Virtual Ethernet is higher than the physical network.

References

- IEEE Standard 802.1Q Virtual Bridged Local Area Networks
- IEEE Standard 802.3 AD Aggregation of Multiple Link Segments



© IBM Corporation 2004

IBM Corporation
Integrated Marketing Communications
Systems and Technology Group
Route 100
Somers, New York 10589

Produced in the United States of America
July 2004
All Rights Reserved

This document was developed for products and/or services offered in the United States. IBM may not offer the products, features, or services discussed in this document in other countries. The information may be subject to change without notice. Consult your local IBM business contact for information on the products, features and services available in your area.

All statements regarding IBM future directions and intent are subject to change or withdrawal without notice and represent goals and objectives only.

IBM, the IBM logo, the e-business logo, the AIX 5L logo, @server, AIX 5L, POWER5 are trademarks or registered trademarks of International Business Machines Corporation in the United States or other countries or both. A full list of U.S. trademarks owned by IBM may be found at <http://www.ibm.com/legal/copytrade.shtml>.

Other company, product, and service names may be trademarks or service marks of others.

IBM hardware products are manufactured from new parts, or new and used parts. Regardless, our warranty terms apply.

Copying or downloading the images contained in this document is expressly prohibited without the written consent of IBM.

This equipment is subject to FCC rules. It will comply with the appropriate FCC rules before final delivery to the buyer.

Information concerning non-IBM products was obtained from the suppliers of these products or other public sources. Questions on the capabilities of the non-IBM products should be addressed with the suppliers.

All performance information was determined in a controlled environment. Actual results may vary. Performance information is provided "AS IS" and no warranties or guarantees are expressed or implied by IBM.

The IBM home page on the Internet can be found at <http://www.ibm.com>.

The AIX 5L home page on the Internet can be found at: <http://www.ibm.com/servers/aix>.