# Best practices when deploying VMware vSphere 5.0 connected to HP Networking Switches

## Table of contents

- Executive summary: 2
- Overview: 2
  - VMware ESXi 5: 2
  - HP Networking: 3
- Link aggregation: 3
  - Link Aggregation Control Protocol (LACP): 3
  - Port Trunk/Bridge Aggregations: 4
  - Meshing: 4
  - Distributed Trunking: 4
  - Intelligent Resilient Framework (IRF): 4
- Networking in VMware ESXi 5: 5
  - Load balancing: 5
  - Failover configuration: 6
- Intelligent Resilient Framework (IRF) and VMware: 7
- Deployment best practices: 7
  - Dual switch configuration: 7
  - Dual switch configuration using Intelligent Resilient Framework (IRF): 9
- Best practices for configuring HP Networking switches for use with VMware ESXi 5 hosts: 10
  - Configuring the ESXi vSwitch: 10
  - Configuring the HP Networking switches: 15
- Appendix A: Glossary of terms: 20
- For more information: 21
Executive summary

This white paper provides information on how to utilize best practices to properly configure VMware vSphere 5.0 virtual switches directly connected to HP Networking switches. By leveraging HP Networking with VMware vSphere, HP delivers the foundation for the data center of the future, today, by providing a unified, virtualization-optimized infrastructure. HP Networking solutions enable the following:

- Breakthrough cost reductions by converging and consolidating server, storage, and network connectivity onto a common fabric with a flatter topology and fewer switches than the competition.
- Predictable performance and low latency for bandwidth-intensive server-to-server communications.
- Improved business agility, faster time to service, and higher resource utilization by dynamically scaling capacity and provisioning connections to meet virtualized application demands by leveraging technologies such as HP Intelligent Resilient Framework (IRF)
  - VMware’s vMotion can complete 40% faster using IRF than standard technologies such as rapid Spanning Tree Protocol (STP)\(^1\)
  - IRF virtually doubles network bandwidth compared with STP and Virtual Router Redundancy Protocol (VRRP), with much higher throughput rates regardless of frame size
  - IRF converged around failed links, line cards, and systems vastly faster than existing redundancy mechanisms such as STP
  - STP can take up to 30 seconds or more to recover after a line card failure; IRF can recover from the same event in as little as 2.5 milliseconds
- Removal of costly, time-consuming, and error-prone change management processes by
  - Utilizing IRF to allow multiple devices to be managed using a single configuration file from a single, easy-to-manage virtual switch operating across network layers
  - Utilizing HP’s Intelligent Management Center (IMC) to manage, monitor, and control access to either a few or thousands of switches in multiple locations from a single pane of glass
- Modular, scalable, industry standards-based platforms and multi-site, multi-vendor management tools to connect and manage thousands of physical and virtual resources

This document also includes explanations of different types of link aggregation protocols that HP leverages in its networking products to help meet the network resiliency needs of your network and business applications.

Target audience: Network and/or System administrators configuring the network of their rack mounted servers using VMware ESXi 5 hosts and HP Networking switches.

This white paper describes testing performed in August 2012.

Overview

VMware ESXi 5

With the release of vSphere 5.0, VMware has once again set new industry standards with its improvements to existing features such as increased I/O performance and 32-way virtual SMP, and with brand new services such as Profile-Driven Storage, Storage Distributed Resource Scheduler (SDRS), and vSphere Auto Deploy. New VM virtual hardware provides additional graphic and USB 3.0 support. Most importantly, with support for up to 32 CPUs and 1TB of RAM per VM, your virtual machines can now grow four times larger than in any previous release to run even the largest applications.

This is the first release of vSphere to rely entirely on the thinner ESXi 5.0 hypervisor architecture as its host platform. The ESX hypervisor used in vSphere 4.1 is no longer included in vSphere; however, the vSphere 5.0 management platform (vCenter Server 5.0) still supports ESX/ESXi 4.x and ESX/ESXi 3.5 hosts.

Use Profile-Driven Storage to identify the right storage resource to use for any given VM based on its service level. With SDRS you can aggregate storage into pools, greatly simplifying scale management and ensuring optimum VM load balancing while avoiding storage bottlenecks. With Auto Deploy, the new deployment model for vSphere hosts running

the ESXi hypervisor, you can now install new vSphere hosts in minutes and update them more efficiently than ever before.


For complete documentation on VMware vSphere 5.0, go to: [http://pubs.vmware.com/vsphere-50/index.jsp](http://pubs.vmware.com/vsphere-50/index.jsp)

**HP Networking**

HP is changing the rules of networking with a full portfolio of high-performance, standards-based products, solutions, and services. These offerings are secure, energy-efficient, cost-saving, and developed specifically to simplify the complexities of networking for all customers, from the largest enterprise to the smallest emerging business.

By investing in HP’s best-in-class networking technology, customers can build high-performance, secure, and efficiently managed network environments that are flexible, interoperable, and highly cost-effective. When integrated as part of the HP Converged Infrastructure and supported by HP and partner service capabilities, HP Networking solutions deliver application and business services across the extended enterprise to meet critical business demand.

**The HP FlexNetwork architecture**

The HP FlexNetwork architecture is a key component of the HP Converged Infrastructure. Enterprises can align their networks with their changing business needs by segmenting their networks into four interrelated modular building blocks that comprise the HP FlexNetwork architecture: HP FlexFabric, HP FlexCampus, HP FlexBranch, and HP FlexManagement. FlexFabric converges and secures the data center network with compute and storage. FlexCampus converges wired and wireless networks to deliver media-enhanced, secure, and identity-based access. FlexBranch converges network functionality and services to simplify the branch office. FlexManagement converges network management and orchestration.

The HP FlexNetwork architecture is designed to allow IT professionals to manage these different network segments through a single pane-of-glass management application, the HP IMC. Because the FlexNetwork architecture is based on open standards, enterprises are free to choose the best-in-class solution for their businesses. Even with the shift to the network cloud, the HP FlexNetwork architecture is ideal for supporting this evolution. Enterprises deploying private clouds must implement flatter, simpler data center networks to support the bandwidth-intensive, delay-sensitive server-to-server virtual machine traffic flows, and workload mobility that are associated with cloud computing. They must also be able to administer and secure virtual resources, and orchestrate on-demand services. The HP FlexNetwork architecture helps enterprises to securely deploy and centrally orchestrate video, cloud, and mobility-enhanced architectures that scale from the data center to the network edge.

**Link aggregation**

Link aggregation is the general term to describe various methods of combining (aggregating) multiple network connections in parallel to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links fails. There are several forms of link aggregation used by HP products that we will highlight here.

**Link Aggregation Control Protocol (LACP)**

Link Aggregation Control Protocol (LACP) is an open industry IEEE standard (IEEE 802.3ad) that provides a method to control the bundling of several physical ports together to form a single logical channel. A LACP enabled port will send Link Aggregation Control Protocol Data Unit (LACPDU) frames across its link in order to detect a device on the other end of the link that also has LACP enabled. Once the other end receives the packet, it will also send frames along the same links enabling the two units to detect multiple links between themselves and then combine them into a single logical link. LACP can be configured in one of two modes: active or passive. In active mode it will always send frames along the configured links. In passive mode however, it acts as "speak when spoken to", and therefore can be used as a way of controlling accidental loops (as long as the other device is in active mode).

LACP is most commonly used to connect a user device (a server, workstation), with multiple links to a switch in order to form a single logical channel. To form a single logical channel on the server requires the configuration of NIC teaming, also known as bonding. For a Microsoft® Windows® host, which does not support NIC teaming natively, HP provides a teaming tool for HP branded NICs which can be downloaded from HP on the Support and Drivers page.
Port Trunk/Bridge Aggregations

Port trunking (ProCurve OS) and Bridge Aggregation (Comware OS) allow you to assign multiple similar links, the number depends on the type and model of the switch, to one logical link that functions as a single, higher-speed link providing dramatically increased bandwidth to other switches and routing switches. This capability applies to connections between backbone devices as well as to connections in other network areas where traffic bottlenecks exist. A trunk/bridge aggregation configuration is most commonly used when aggregating ports between network switches/routers as well as other network devices, such as ESX/ESXi, that do not speak the 802.3ad LACP protocol.

Meshing

Switch meshing technology, available as part of the ProCurve OS, allows multiple switches to be redundantly linked together to form a meshing domain. Switch meshing eliminates network loops by detecting redundant links and identifying the best path for traffic. When the meshing domain is established, the switches in that domain use the meshing protocol to gather information about the available paths and to determine the best path between switches. To select the best path, the meshed switches use the following criteria:

- Outbound queue depth, or the current outbound load factor, for any given outbound port in a possible path
- Port speed, based on factors such as 10 Mbps, 100 Mbps, 1000 Mbps (or 1 Gbps), 10 Gbps, full-duplex, or half-duplex
- Inbound queue depth for any destination switch in a possible path
- Increased packet drops, indicating an overloaded port or switch

For more information on Switch Meshing, you can view the white paper at hp.com/rnd/pdfs/Switch_Meshing_Paper_Tech_Brief.pdf

Distributed Trunking

Distributed Trunking (DT) is a link aggregation technique, where two or more links across two switches are aggregated together to form a trunk. The IEEE standard—802.3ad—limits the links that can be aggregated within a single switch/device. To overcome this limitation, HP developed a new proprietary protocol called Distributed Trunking Interconnect Protocol (DTIP) to support link aggregation for the links spanning across the switches. DT provides node-level L2 resiliency in an L2 network, when one of the switches fails. The downstream device (for example, a server or a switch) perceives the aggregated links as coming from a single upstream device. This makes interoperability possible with third party devices that support IEEE 802.3ad.

Users can configure Distributed Trunking using one of the following:

- Manual Trunks (without LACP)
- LACP trunks

Distributed Trunking is available on HP Networking 8200, 6600, 6200, 5400, and 3500 series switches today. All Distributed Trunking switches that are aggregated together to form a trunk must run the same software version.

For more information on Distributed Trunking, you can view the white paper at http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA3-4841ENW

Intelligent Resilient Framework (IRF)

IRF technology extends network control over multiple active switches. Management of a group of IRF enabled switches is consolidated around a single management IP address, which vastly simplifies network configuration and operations. You are allowed to combine as many as nine HP 58x0 series switches to create an ultra-resilient virtual switching fabric comprising hundreds or even thousands of 1-GbE or 10-GbE switch ports.
One IRF member operates as the primary system switch, maintaining the control plane and updating forwarding and routing tables for the other devices. If the primary switch fails, IRF instantly selects a new primary, preventing service interruption and helping to deliver network, application, and business continuity for business-critical applications.

Within the IRF domain, network control protocols operate as a cohesive whole to streamline processing, improve performance, and simplify network operation. Routing protocols calculate routes based on the single logical domain rather than the multiple switches it represents. Moreover, edge or aggregation switches that are dual homed to IRF-enabled core or data center switches “see” the associated switches as a single entity, thus enabling true active/active architecture, eliminating the need for slow convergence and active/passive technologies such as spanning tree protocol (STP). Operators have fewer layers to worry about, as well as fewer devices, interfaces, links, and protocols to configure and manage.


Networking in VMware ESXi 5

This guide is not intended to highlight the best practices for performance for guests. For that information, you can view a white paper published by VMware called “Performance Best Practices for VMware vSphere 5.0” which can be downloaded from vmware.com/pdf/Perf_Best_Practices_vSphere5.0.pdf. This document should be reviewed for optimizing your VMware guests networking based on the hardware you are using.

With VMware ESXi 5, it is possible to connect a single virtual or distributed switch to multiple physical Ethernet adapters. A virtual or distributed switch can share the load of traffic between physical and virtual networks among some or all of its members and provide passive failover in the event of a hardware failure or a network outage. The rest of this section describes what policies can be set at the port group level for your virtual and distributed switches.

---

**Note**

All physical switch ports in the same team must be in the same Layer 2 broadcast domain.

---

**Load balancing**

Load balancing allows you to spread network traffic from virtual machines on a virtual switch across two or more physical Ethernet adapters, giving higher throughput than a single physical adapter could provide. When you set NIC teaming policies, you have the following options for load balancing:

**Route based on the originating virtual switch port ID**

Route based on the originating virtual switch port ID functions by choosing an uplink based on the virtual port where the traffic entered the virtual switch. This is the default configuration and the one most commonly deployed since this does not require physical switch configuration in terms of link aggregation.

When using this setting, traffic from a given virtual Ethernet adapter is consistently sent to the same physical adapter unless there is a failover to another adapter in the NIC team. Replies are received on the same physical adapter as the physical switch learns the port association.

A given virtual machine cannot use more than one physical Ethernet adapter at any given time unless it has multiple virtual adapters and this setting provides an even distribution of virtual Ethernet adapters to the number of physical adapters. A downside to this method is that a VM’s virtual adapter is paired with a busy physical Ethernet adapter, even if there is another completely idle Ethernet adapter that is a part of the virtual switch, the traffic will never use the idle Ethernet adapter, but will continue to use the overloaded Ethernet adapter.

**Route based on source MAC hash**

Route based on source MAC hash, functions exactly like route based on the originating virtual switch port ID except it chooses an uplink based on a hash of the source Ethernet MAC address. This method is known to cause a bit more load on the host as well as not guarantee that virtual machines using multiple virtual adapters to the same virtual or distributed switch will use separate ports.
Route based on IP hash

Route based on IP hash, functions by choosing an uplink based on a hash of the source and destination IP addresses of each packet. (For non-IP packets, whatever is at those offsets is used to compute the hash.) What this means is that in contrast to route based on the originating virtual switch port ID and route based on source MAC hash, traffic from a VM is not limited to the use of one physical Ethernet adapter on the port group, but can leverage all Ethernet adapters for both inbound and outbound communications as per the 802.3ad link-aggregation standard. This allows for greater network resources for VMs, since they can now leverage the bandwidth of two or more Ethernet adapters on a host, and the evenness of traffic distribution depends on the number of TCP/IP sessions to unique destinations, not the number of VMs to Ethernet adapters in the port group.

All adapters in the NIC team must be attached to the same physical switch or an appropriate set of IRF or DT switches and configured to use 802.3ad link-aggregation standard in static mode, not LACP. All adapters must be active. For ease of management it is recommended that all port groups within a virtual switch inherit the settings on the virtual switch.

Although this method is the only one that distributes traffic evenly, it does come at a small cost to the VMware ESXi host. Each packet that exits the virtual switch must be inspected by the VMkernel in order to make routing decisions. Therefore, this inspection process uses CPU time to calculate which physical NIC it will use.

Failover configuration

When configuring a port group and load balancing, it is also necessary to configure the proper network failover detection method to use for failover detection when an Ethernet adapter in your port group is lost.

Link Status only

Link Status only relies solely on the link status provided by the network adapter. This detects failures, such as cable pulls and physical switch power failures, but it cannot detect configuration errors, such as a physical switch port being blocked by spanning tree, misconfigured VLANs, or upstream link failures on the other side of a physical switch.

Beacon Probing

Beacon Probing addresses many of the issues that were highlighted with the Link Status method. Beacon Probing sends out and listens for beacon probes, Ethernet broadcast frames sent by physical adapters to detect upstream network connection failures, on all physical Ethernet adapters in the team. It uses this information, in addition to link status, to determine link failure. Beacon probing can be useful to detect failures in the switch connected to the ESX Server hosts, where the failure does not cause a link-down event for the host. A good example of a failure that could be detected is where upstream connectivity is lost to an upstream switch that a switch from an ESXi host is connected to. With Beacon Probing, this can be detected, and that Ethernet adapter will be deactivated in the port group. Beacon Probing is not supported when using Route based on IP hash and requires a minimum of 3 Ethernet adapters in your virtual switch.

Failback

By default, NIC teaming applies a fail-back policy. That is, if a physical Ethernet adapter that had failed comes back online, the adapter is returned to active duty immediately, displacing the standby adapter, if configured, that took over its slot. If the primary physical adapter is experiencing intermittent failures, this setting can lead to frequent changes to the adapter in use and affect network connectivity to the VMs using that adapter.

You can prevent the automatic fail-back by setting Failback in the vSwitch to No. With this setting, a failed adapter is left inactive even after recovery until another currently active adapter fails, or the Administrator puts it back into operation.

Using the Failover Order policy setting, it is possible to specify how to distribute the workload for the physical Ethernet adapters on the host. It is best practice on scenarios where IRF or DT cannot be leveraged that a second group of adapters are connected to a separate switch in order to tolerate a switch failover.

Using the Notify Switches option enables your VMware ESXi hosts to communicate with the physical switch in the event of a failover. If enabled, in the event of an Ethernet adapter failure, a notification is sent out over the network to update the lookup tables on physical switches. In almost all cases, this is desirable for the lowest latency when a failover occurs.
Intelligent Resilient Framework (IRF) and VMware

HP tasked Network Test to assess the performance of Intelligent Resilient Framework (IRF), using VMware as part of the workload for testing. Network Test and HP engineers constructed a large-scale test bed to compare vMotion performance using IRF and Rapid Spanning Tree Protocol (RSTP). With both mechanisms, the goal was to measure the time needed for vMotion migration of 128 virtual machines, each with 8 GB of RAM, running Microsoft SQL Server on Windows Server 2008.

On multiple large-scale test beds, IRF clearly outperformed existing redundancy mechanisms such as the Spanning Tree Protocol (STP) and the Virtual Routing Redundancy Protocol (VRRP).

Among the key findings of these tests:

- Using VMware’s vMotion facility, average virtual machine migration time took around 43 seconds on a network running IRF, compared with around 70 seconds with rapid STP.
- IRF virtually doubled network bandwidth compared with STP and VRRP, with much higher throughput rates regardless of frame size.
- IRF converged around failed links, line cards, and systems vastly faster than existing redundancy mechanisms such as STP.
- In the most extreme failover case, STP took 31 seconds to recover after a line card failure; IRF recovered from the same event in 2.5 milliseconds.
- IRF converges around failed network components far faster than HP’s 50-millisecond claim.

This document can be viewed at the following URL: [http://www3.networktest.com/hpirf/hpirf1.pdf](http://www3.networktest.com/hpirf/hpirf1.pdf)

Deployment best practices

There are a many options when configuring VMware ESXi vSwitches connected to HP switches. Below we will highlight two scenarios, one using a non-IRF configuration and one using an Intelligent Resilient Framework (IRF) or Distributed Trunk configuration where active/active connections are used for the ESXi vSwitch.

Dual switch configuration

In the configuration in Figure 1, of the 4 connections available, two connections go to one switch, two go to the other switch. It is recommended, even if only using 2 connections, to use two separate network cards in order to add another layer of resiliency in the case of a card failure.

Figure 1. Standard network diagram
Route based load balancing on the originating virtual switch port ID functions is used in this scenario which means that no link aggregation configuration is needed on the two switches. Although all four ports are used, traffic to and from a given virtual Ethernet adapter is consistently sent to the same physical adapter. This means that if there is contention on the associate physical adapter, even if there is another physical adapter with little or no utilization, traffic from the virtual Ethernet adapter on the VM will continue to send/receive traffic from the physical adapter under contention.

You cannot create a link aggregation across two separate switches without technologies such as Intelligent Resilient Framework (IRF) or Distributed Trunking (DT), which will be talked about more in scenario two. You also cannot create two link aggregation groups (Figure 2), one going to one switch one going to the other. VMware does not support multiple trunks on the same vSwitch and your ESXi host and guest may encounter MAC address flopping, where a system uses two MAC addresses one after the other which will cause serious issues on your network.

**Figure 2.** Example of an incorrect and unsupported configuration

Additionally, it is not recommended to create a scenario such as Figure 3. Although it will work, it is not practical since your network traffic is not guaranteed to go over the 802.3ad link.

**Figure 3.** Example of an incorrect and unsupported configuration
Dual switch configuration using Intelligent Resilient Framework (IRF)

The best and recommended configuration for performance and resiliency is to leverage HP’s Intelligent Resilient Framework (IRF) in its data center switches powered by Comware (Figure 4). This will not only tolerate a switch failure, but also allow a virtual Ethernet adapter in a VM to leverage the bandwidth from all four physical Ethernet adapters in a vSwitch. With the use of IRF, you can create a link aggregation across two separate switches since IRF enables the two switches to act as one.

Figure 4. Example diagram using Intelligent Resilient Fabric (IRF)
Best practices for configuring HP Networking switches for use with VMware ESXi 5 hosts

Configuring the ESXi vSwitch

1. Launch the vSphere Client and connect to your vCenter Server instance or your ESXi host.
2. Select your ESXi 5 host, and go to the Configuration tab. Select Networking under the Hardware section of the Configuration window (Figure 5).
3. Select Properties on the first vSwitch connected to the HP Network Switch you will be configuring (Figure 5).

Figure 5. VMware vSphere Client vSwitch Configuration Window
4. In the vSwitch Properties window, select the **Network Adapters** tab. From this window, you can see the current network adapters in your vSwitch. If you need to add a network adapter, select the **Add...** button (Figure 6).

**Figure 6. VMware vSphere vSwitch Properties Window**
5. Select the additional network adapter(s) from the list that you would like to have in the vSwitch (Figure 7). Then select the **Next** button.

*Figure 7. Add Adapter Wizard*
6. Ensure that the network adapter(s) you added are in **Active Adapters** (Figure 8) and then select **Next**. If it is not in the **Active Adapters** section, use the **Move Up** button on the right side to move it into that group.

**Figure 8.** Add Adapter Wizard – All adapters in Active Adapters

7. Select the **Finish** button on the **Adapter Summary** screen.
8. Select the **Ports** tab, and then select **vSwitch** (Figure 9) from the Properties window and select the **Edit...** button.

**Figure 9. vSwitch Properties Window**
9. Select the NIC Teaming tab in the vSwitch Properties window and set **Load Balancing** to **Route based on IP hash** (Figure 10). Also, ensure that **Network Failover Detection** is set to **Link status only**. Then select the OK button.

Figure 10. vSwitch Properties Window – Configuring NIC Teaming Properties

10. If your other configurations are not set up to inherit their properties from the vSwitch configuration, which is the default, repeat steps 8 and 9 for each configuration. You can easily see if you are not inheriting the properties by selecting the configuration and looking at the **Failover and Load Balancing** section. If **Load Balancing** is not set to **Route based on IP hash** and/or **Network Failover Detection** is not set to **Link status only**, then you need to edit the configuration appropriately.

11. Select “Close” on the “vSwitch Properties” window. Repeat for each of your vSwitches that you are configuring in Active/Active mode going to an HP Networking switch.

**Configuring the HP Networking switches**

Once you have completed configuring your vSwitch(s), next you need to configure the HP Networking switch that the system connects to. Configuring a switch running the Comware or the ProCurve operating system is highlighted in the following section. The end goal is to configure the port mode to trunk on the HP Switch to accomplish static link aggregation with ESX/ESXi. Trunk mode of HP switch ports is the only supported aggregation method compatible with ESX/ESXi NIC teaming mode IP hash.
Note
Port Numbers will be formatted differently depending on the model and how the switch is configured. For example, a switch configured to use Intelligent Resilient Framework (IRF) will also include a chassis number as part of the port number.

Comware
In this example, we will be making a two port link aggregation group in an IRF configuration. You can see that this is a two switch IRF configuration by observing the port number scheme of chassis/slot/port. A scheme of 1/0/8 means chassis 1, or switch 1, slot 0 port 8. A scheme of 2/0/8 means chassis 2, or switch 2, slot 0 port 8.

Link aggregation groups can be larger and the number of ports depends on the model of the switch. For example, an HP 12500 series switch can have a 12 port link aggregation group.

1. Log into the network device via the console and enter system-view. The following steps can also be accomplished using the Web UI available on most switches, but that will not be covered in this guide.
   <Comware-Switch>system-view

2. Create the Bridge Aggregation interface to contain the uplinks from your server. In this example we will be creating the interface of Bridge Aggregation 11. Your numbering may vary depending on the current configuration on the switch you are using.
   [Comware-Switch] interface Bridge-Aggregation 11

3. Give your new interface a description in order to help you identify it easier:
   [Comware-Switch-Bridge-Aggregation11] description ESXi-Server-1-vSwitch0

4. Return to the main menu:
   [Comware-Switch-Bridge-Aggregation11] quit

5. Enter the first interface that you will be aggregating:
   [Comware-Switch] interface Ten-GigabitEthernet 1/0/8

6. Enable the interface. If it is already enabled, it will tell you that the interface is not shutdown.
   [Comware-Switch-Ten-GigabitEthernet 1/0/8] undo shutdown

7. Put the port in the link aggregation group:
   [Comware-Switch-Ten-GigabitEthernet1/0/8] port link-aggregation group 11

8. Return back to the main menu and repeat steps 5-7 for all your interfaces going into the link aggregation group.

9. Return to the Bridge Aggregation for the final configuration:
   [Comware-Switch] interface Bridge-Aggregation 11

Note
If you get an error similar to "Error: Failed to configure on interface..." during any of the following steps, you will need to run the following command on the interface that has the error and then re-run step 5-7.

[Comware-Switch] interface Ten-GigabitEthernet 1/0/8

[Comware-Switch-Ten-GigabitEthernet1/0/8] default
This command will restore the default settings. Continue? [Y/N]: Y

If the default command is not available:
[Comware-Switch-Ten-GigabitEthernet1/0/8] port link-type access
10. Change the port type to a trunk:
   ```
   [Comware-Switch-Bridge-Aggregation11] port link-type trunk
   ```

11. Enable the interface:
   ```
   [Comware-Switch-Bridge-Aggregation11] undo shutdown
   ```

12. Set the Port Default VLAN ID (PVID) of the connection. The PVID is the VLAN ID the switch will assign to all untagged frames (packets) received on each port. Another term for this would be your untagged or native VLAN. By default, it is set to 1, but you will want to change it if your network is using another VLAN ID for your untagged traffic.
   ```
   [Comware-Switch-Bridge-Aggregation11] port trunk pvid vlan 1
   ```

13. If you configured your vSwitch to pass multiple VLAN tags, you can configure your bridge aggregation link at this time by running the following command. Repeat for all the VLANs you need to pass through that connection.
   ```
   [Comware-Switch-Bridge-Aggregation11] port trunk permit vlan 85
   ```
   Please wait... Done.
   Configuring Ten-GigabitEthernet1/0/8... Done.
   Configuring Ten-GigabitEthernet2/0/9... Done.

14. If you set your PVID to something other than the default 1, you will want to remove that VLAN 1 and repeat step 12 for your PVID VLAN. If you do not want to use your PVID VLAN through your virtual switch, omit entering the second command below.
   ```
   [Comware-Switch-Bridge-Aggregation11] undo port trunk permit vlan 1
   ```
   Please wait... Done.
   Configuring Ten-GigabitEthernet1/0/8... Done.
   Configuring Ten-GigabitEthernet2/0/9... Done.

15. Now display your new Bridge Aggregation interface to ensure things are set up correctly. You will want to make sure your PVID is correct, and that you are both passing and permitting the VLAN you defined. In this example, we are not passing the untagged traffic (PVID 1) and only packets tagged with VLAN ID 85 and 134. You will also want to make sure your interfaces are up, and you are running at the correct speed, two 10Gbps links would give you 20Gbps of aggregated performance.
   ```
   [Comware-Switch] display interface Bridge-Aggregation 11
   Bridge-Aggregation11 current state: UP
   IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-e207-f2e0
   Description: ESXi-Server-1-vSwitch0
   20Gbps-speed mode, full-duplex mode
   Link speed type is autonegotiation, link duplex type is autonegotiation
   PVID: 1
   Port link-type: trunk
   VLAN passing: 85, 134
   VLAN permitted: 85, 134
   Trunk port encapsulation: IEEE 802.1q
   ... Output truncated...
   ```

16. Now check to make sure the trunk was formed correctly. If both connections have something other than “S” for the status, here are a couple of troubleshooting steps. If none of these work, then delete and recreate the bridge aggregation and reset all the ports back to default. Ensure that
   a. You configured the interfaces correctly.
   b. You enabled (undo shutdown) the port on the switch.
c. The VLANs being passed/permitted match that of the group.
d. The port is connected to the switch on the interface you specified and is connected and enabled on the server:

   [Comware-Switch] display link-aggregation verbose Bridge-Aggregation 11

   Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
   Port Status: S -- Selected, U -- Unselected
   Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
          D -- Synchronization, E -- Collecting, F -- Distributing,
          G -- Defaulted, H -- Expired

   Aggregation Interface: Bridge-Aggregation11
   Aggregation Mode: Static
   Loadsharing Type: Shar

   Port             Status    Oper-Key
                    -----------------------------------------------
   XGE1/0/8         S         2
   XGE1/0/9         S         2

17. Save the configuration. Repeat these steps for each vSwitch you have configured. Once completed, exit the switch, and you are done.

**ProCurve**

In this example, we will be making a two port link aggregation group. Unlike the IRF configuration above where everything was done from a single switch and no special setup was needed on the IRF connection, if your setup is leveraging Distributed Trunking, additional steps will be needed to run the other switch in the DT configuration. It is also required that you use **dt-trunk** and not **dt-lacp** in the configuration.

Link aggregation groups can be larger and the number of ports depends on the model of the switch. For example, an HP 8200 series switch can have an 8 port link aggregation group.

1. Log into the network device via the console, enter the CLI interface if at the menu view, and enter configuration mode. The following steps may also be accomplished using the Web UI available on most switches, but that will not be covered in this guide.

   ProCurve-Switch# configure terminal

2. Create the link aggregation (trunk):
   a. Not using Distributed Trunking:

      ProCurve-Switch(config)# trunk 9,10 trk11 trunk

   b. Using Distributed Trunking:

      ProCurve-Switch(config)# trunk 9,10 trk11 dt-trunk

**Note**

If you are adding more than two ports, and they are contiguous, you can say ports 9-12, then you can use a dash to define that. An example is below.

ProCurve-Switch(config)# trunk 9-12 trk11 trunk
3. Ensure the Trunk was created:
   ProCurve-Switch(config)# `show trunks`

   Load Balancing
<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Type</th>
<th>Group</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td></td>
<td>SFP+SR</td>
<td>Trk11</td>
<td>Trunk</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td>SFP+SR</td>
<td>Trk11</td>
<td>Trunk</td>
</tr>
</tbody>
</table>

4. Enable the ports you put in the trunk group:
   ProCurve-Switch(config)# `interface 9 enable`
   ProCurve-Switch(config)# `interface 10 enable`

5. If you configured your vSwitch to pass multiple VLAN tags, you can configure your trunk connection at this point by running the following command. Repeat for all the VLANs you need to pass through that connection.
   ProCurve-Switch(vlan-85)# `tagged trk11`
   ProCurve-Switch(vlan-85)# `quit`
   ProCurve-Switch(config)# `show vlan 85`

   Status and Counters - VLAN Information - VLAN 85
   VLAN ID : 85
   Name : ESXi VLAN 1
   Status : Port-based
   Voice : No
   Jumbo : Yes

<table>
<thead>
<tr>
<th>Port Information</th>
<th>Mode</th>
<th>Unknown</th>
<th>VLAN</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>Untagged</td>
<td>Learn</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Untagged</td>
<td>Learn</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Untagged</td>
<td>Learn</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Untagged</td>
<td>Learn</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>Trk1</td>
<td>Tagged</td>
<td>Learn</td>
<td>Up</td>
<td></td>
</tr>
<tr>
<td>Trk11</td>
<td>Tagged</td>
<td>Learn</td>
<td>Up</td>
<td></td>
</tr>
</tbody>
</table>

6. Set the Port Default VLAN ID (PVID) of the connection. The PVID is the VLAN ID the switch will assign to all untagged frames (packets) received on each port. In the ProCurve OS, this would be the untagged VLAN. By default, it is set and added to VLAN 1, but you will want to change it if your network is using another VLAN ID for your untagged traffic. If you do not want to pass your untagged network through your virtual switch, omit adding the port to the untagged network in this example (VLAN 2).
   ProCurve-Switch(config)# `vlan 1`
   ProCurve-Switch(vlan-1)# `no untagged trk11`
   ProCurve-Switch(vlan-1)# `quit`
   ProCurve-Switch(config)# `vlan 2`
   ProCurve-Switch(vlan-2)# `untagged trk11`
   ProCurve-Switch(vlan-2)# `quit`

7. Save the configuration:
   ProCurve-Switch(vlan-2)# `write me`
8. You now need to repeat the same steps on your other switch if you are using Distributed Trunking.
9. Repeat these steps for each vSwitch you have configured. Once completed, exit the switch, and you are done.

**Appendix A: Glossary of terms**

**Table 1. Glossary**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge Aggregation</td>
<td>Comware OS terminology for Port Aggregation.</td>
</tr>
<tr>
<td>Distributed Trunking (DT)</td>
<td>A link aggregation technique, where two or more links across two switches are aggregated together to form a trunk.</td>
</tr>
<tr>
<td>IEEE 802.3ad</td>
<td>An industry standard protocol that allows multiple links/ports to run in parallel, providing a virtual single link/port. The protocol provides greater bandwidth, load balancing, and redundancy.</td>
</tr>
<tr>
<td>Intelligent Resilient Framework (IRF)</td>
<td>Technology in certain HP Networking switches that enables the ability to connect similar devices together to create a virtualized distributed device. This virtualization technology realizes the cooperation, unified management, and non-stop maintenance of multiple devices.</td>
</tr>
<tr>
<td>LACP</td>
<td>Link Aggregation Control Protocol (see IEEE 802.3ad)</td>
</tr>
<tr>
<td>Port Aggregation</td>
<td>Combining ports to provide one or more of the following benefits: greater bandwidth, load balancing, and redundancy.</td>
</tr>
<tr>
<td>Port Bonding</td>
<td>A term typically used in the UNIX®/Linux world that is synonymous to NIC teaming in the Windows world.</td>
</tr>
<tr>
<td>Port Trunking</td>
<td>ProCurve OS terminology for Port Aggregation.</td>
</tr>
<tr>
<td>Spanning Tree Protocol (STP)</td>
<td>Spanning Tree Protocol (STP) is standardized as IEEE 802.1D and ensures a loop-free topology for any bridged Ethernet local area network by preventing bridge loops and the broadcast traffic that results from them.</td>
</tr>
<tr>
<td>Trunking</td>
<td>Combining ports to provide one or more of the following benefits: greater bandwidth, load balancing, and redundancy.</td>
</tr>
<tr>
<td>Virtual Switch</td>
<td>Virtual switches allow virtual machines on the same ESX/ESXi host to communicate with each other using the same protocols that would be used over physical switches, as well as systems outside of the ESX/ESXi host when configured with one or more physical adapters on the host, without the need for additional networking hardware.</td>
</tr>
<tr>
<td>vSphere Distributed Switch</td>
<td>vSphere’s Distributed Switch spans many vSphere hosts and aggregates networking to a centralized cluster level. The Distributed Switch abstracts configuration of individual virtual switches and enables centralized provisioning, administration and monitoring through VMware vCenter Server.</td>
</tr>
</tbody>
</table>
**For more information**

For more information on HP Networking products, visit [hp.com/go/networking](http://hp.com/go/networking)

For more information on HP and VMware, visit [hp.com/go/vmware](http://hp.com/go/vmware)

For more information on VMware vSphere 5, visit [vmware.com/products/datacenter-virtualization/vsphere/index.html](http://vmware.com/products/datacenter-virtualization/vsphere/index.html)


To help us improve our documents, please provide feedback at [hp.com/solutions/feedback](http://hp.com/solutions/feedback).

---

**Get connected**

[hp.com/go/getconnected](http://hp.com/go/getconnected)

Current HP driver, support, and security alerts delivered directly to your desktop

---

© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation. UNIX is a registered trademark of The Open Group.

4AA4-4192ENW, Created October 2012