Vertiv™ Avocent® HMX 5000, 6000 and 8000 Series High Performance KVM Extenders

Network Recommendations Technical Note

APRIL 2, 2021

Recommended Network Criteria

When setting up Vertiv™ Avocent® HMX 5000, 6000 and 8000 series high performance KVM extender systems, the network infrastructure is critical. The following recommendations ensure your network performs at optimal levels.

Ethernet Switch General Requirements

For optimal performance, the Ethernet switches within your network should meet the following requirements. For each network setting listed below, configuration commands for Cisco switches are also provided for your reference.

NOTE: For your convenience, commands are listed in a group that can be easily copied into a text file. Creating a master text file that includes all of the commands allows you to minimize the use of the enable, configure terminal, end, write mem and copy running-config startup-config commands.

- Switches must be a gigabit, “non-blocking” switch (has a switching bandwidth supporting full speed, full duplex on all ports simultaneously, including inter-switch link ports)
- An IP address/subnet mask must be configured on the switch for the VLAN.
- Switches must have IP addresses and default gateways assigned.

  To manually assign IP information to multiple switched virtual interfaces (SVIs), begin in privileged EXEC mode and enter the following commands.

```
enable
configure terminal
interface vlan 1
ip address<ip-address subnet mask>
exit
ip default-gateway<ip-address>
end
show interfaces vlan
show ip redirects
write mem (or copy running-config startup-config)
```

- All switch ports hosting Vertiv™ Avocent® HMX extender system equipment must have Spanning Tree Portfast configured.

  To enable Spanning Tree Portfast to reduce blockage time, enter the following commands.

```
enable
configure terminal
interface range Gi1/0/1-24 (Use -48 if using a 48-port switch)
spanning-tree portfast
end
show spanning-tree interface<interface-id>portfast
write mem (or copy running-config startup-config)
```

- If the switch has a separate Bridge Multicast Filtering setting, it must be enabled.

- If using fiber switches, these switches must provide multicast support. For setting details, check the recommendations from the manufacturer of your preferred switch.
- For more multicast information, see the *Unicast and Multicast Communications* section of this technical note.

- Switches must support IGMP Snooping enabled at the switch and VLAN levels to support Share mode:
  - The default IGMP version used by the Vertiv™ Avocent® HMX Advanced Manager is version 2.
    NOTE: To use IGMP version 3, the network switch must also be set to support this version at the switch level and the VLAN. The Avocent® HMX Advanced Manager must also be set to IGMP version 3 by selecting *Dashboard- Settings- Network* in the user interface.
  - Depending on the IOS naming convention, IGMP should be set for either immediate or fast leave.

    To enable IGMP Snooping at the switch level, begin in privileged EXEC mode and enter the following commands.

    ```
    enable
    configure terminal
    ip igmp snooping
    end
    write mem (or copy running-config startup-config)
    ```

  - If you have not designated a VLAN, then the default VLAN (typically VLAN 1) must have IGMP Snooping enabled.

    To enable IGMP Snooping at the VLAN level, begin in privileged EXEC mode and enter the following commands.

    ```
    enable
    configure terminal
    ip igmp snooping vlan
    end
    write mem (or copy running-config startup-config)
    ```

  - If the switch requires the IGMP Querier service to support IGMP Snooping, then the IGMP Querier service must be available on one switch (or a router) in the switch configuration.
    NOTE: In a multi-switch environment, the IGMP Querier service only has to be enabled on one switch.
    - Cisco switches require either an mrouter on the network or an IGMP Querier service running, even with a single, standalone switch. However, most managed Cisco switches ship with the IGMP Querier service available and the mrouter is seldom used.

    To enable IGMP Querier, enter the following commands.

    ```
    enable
    configure terminal
    ip igmp snooping querier
    end
    show ip igmp snooping vlan
    write mem (or copy running-config startup-config)
    ```

  - To see if IGMP Snooping is properly set up, use Wireshark (available free at Wireshark.org) or another network sniffing application (network sniffer) to plug into any port on your switch or VLAN.
    NOTE: Do not mirror ports; pick an empty network port on the VLAN and plug in there.
    - Begin an unfiltered sniffer trace and verify that only occasional IGMP administration packets are being seen on the network port. IGMP administration communication packets will have 224.0.0 as the first three octets of their address.
    - See the *Unicast and Multicast Communications* section of this technical note for more information on using Wireshark/network sniffers.
- Switches must have Jumbo frames enabled if using Vertiv™ Avocent® HMX 6000 series transmitters and receivers with target computers running at 2K or higher video resolutions (resolutions greater than 1920 x 1200), or if you have any dual-link capable monitors connected to any receivers.

To enable Jumbo frames, set the size to the maximum (9000) and enter the following commands.

```
enable
configure terminal
system mtu 9000 (some switches require “system mtu jumbo 9000”)
end
write mem (or copy running-config startup-config)
reload
```

- Switch ports must be set to Access mode.

  To enable Access mode, enter the following commands.

```
enable
configure terminal
interface range Gi1/0/1-24 (Use -48 if using a 48-port switch)
switchport mode access
end
write mem (or copy running-config startup-config)
```

Single and Multi-Network Configuration Requirements

For single network/VLAN configurations, ensure the following requirements are met:

- Subnet Operations must be set to “off” during initial configuration of the Vertiv™ Avocent® HMX Advanced Manager; the Advanced Manager DHCP server is automatically enabled.
- Confirm there are no other DHCP servers available on the Vertiv™ Avocent® HMX extender primary network. Any DHCP servers/IP Helpers/DHCP Relays that are reachable from the network supporting extender units will conflict with the auto-discovery and automatic address assignment by the HMX Advanced Manager (including Windows servers with Active Directory-integrated DHCP and DNS services that should be on a production network/VLAN and not on the HMX extender system network/VLAN).

For multi-network configurations where the Vertiv™ Avocent® HMX extender system is used in a multi-subnet/VLAN environment, ensure the following requirements are met:

- Subnet Operations must be set to “on” during initial configuration of the Vertiv™ Avocent® HMX Advanced Manager; the Advanced Manager DHCP server is automatically disabled.
- Any DHCP servers/IP Helpers/DHCP Relays must be configured to deliver Vertiv™ Avocent® HMX extender system-specific configuration data to its transmitters, receivers and backup Managers. For additional information on the DHCP requirements in this type of configuration, contact your Vertiv Technical Support representative.
- If using multiple switches, determine which transmitters and user stations connect to each other most often and organize them on the same switch. When connected this way, their traffic is across the backplane of the same switch rather than across a low bandwidth inter-switch link or medium bandwidth stacking module.
  - If you have more than one switch and this configuration is not practical, then ensure you have a high speed 10 Gbps inter-switch link or multiple 10 Gbps inter-switch links with aggregation configured between switches.
    NOTE: When estimating inter-switch bandwidth requirements, use 800 Mbps for each dual-head video connection supported across the link, and use 350 Mbps for each single-head video connection. These are average bandwidth consumption estimates for an application running full-screen, full-motion video at 1920 x 1200 video resolution.

Unicast and Multicast Communications

By default, when only one receiver is connected to a transmitter, the session uses unicast communications. However, once a second receiver connects to the same transmitter, transmitter to receiver audio and video communications switch to multicast communication streams. Separate audio and video multicast IP group addresses are created for each transmitter, and they are set on the multicast IP base address set by the Vertiv™ Avocent® HMX Advanced Manager during initial configuration (the default is 237.1.1.1).

When that second receiver connects to the same transmitter for the first time, the transmitter's audio and video multicast group IP addresses are set to the next two available sequential multicast addresses. To use Wireshark or another network sniffer to confirm that switches are properly set up to handle multicast packets, ensure you have an instance where two receivers are connected to the same transmitter (sharing). There should be no multicast packets from transmitters seen in a Wireshark/network sniffer packet trace on your management computer.

For example, the following is a sample of source and destination IP addresses.
NOTE: The multicast group destination IP address used below should never be seen in a Wireshark/network sniffer trace of a switch hosting a Vertiv™ Avocent® HMX extender system.

- In this sample, all Vertiv™ Avocent® HMX extender units are configured for operation on the 192.168.13.0 network:
  - The transmitter source IP address is 192.168.13.20.
  - The transmitter audio multicast group destination IP address is 237.1.1.37.
  - The transmitter video multicast group destination IP address is 237.1.1.36.

In multi-switch environments, repeat the sniffing process on one port for each individual switch to ensure proper multicast support configuration and operation. For example, multicast support may be set up correctly on one or two switches properly, but not all of the switches.
NOTE: When the switch is properly set up, ensure you copy each switch's running config to the startup config.