Technical Brief

Hiperwall Network Information

This document will cover Hiperwall network information that would be important when designing a Hiperwall system. Specifically, we will cover:

1. Network switch, VLAN, routing, and firewall requirements
2. Bandwidth requirements
3. Multicast considerations (IGMP)
4. Network security

1. Network Switch, VLAN, Routing and Firewall Requirements

Hiperwall requires a managed network switch that supports the following:

1. Non-blocking operation of all ports. This means that all ports run at full wire speed, with no packet loss.
2. IGMP Snooping
3. IGMP Querier
4. IGMP Immediate-Leave (or Fast-Leave)

For more information regarding IGMP Querier, and why it needs to be enabled on the local switch, please see the Hiperwall Technology Brief - Hiperwall IGMP (Multicast) Flow.

The Hiperwall network at a minimum should be on its own VLAN. While it is technically possible to run it on the same VLAN/subnet as the rest of the End Users network, it is not recommended, and careful consideration should be given to bandwidth requirements. Any flood control settings on the switch must be turned off.

If the Hiperwall system is implemented across multiple switches, then the inter-switch links must have a minimum bandwidth of 10Gbps across them. It is preferred to use stacking technology connections if possible. Stacking links provide upwards of 80Gbps bandwidth across the switch stack.

A network router is not required within the Hiperwall network. However, if you plan on bringing in content from outside the Hiperwall VLAN (such as workstation PC's, or IP cameras), or if you are going to control the Hiperwall system from outside your Hiperwall network, a router is required. Because we recommend the Hiperwall system be on its own VLAN, a router would be required if you want any network resources (such as shared drives, printers, etc) available to the Hiperwall system.

If you are using a router and are bringing content or control in from outside the Hiperwall VLAN, your firewall will need to allow that traffic through. The Hiperwall installers will open the Windows Defender Firewall to allow our applications to work. If you are using a hardware firewall on the other hand, you will need to forward (or allow) TCP port 14999 for Sender based products (which currently include HiperSource Sender, HiperSource Browser, and HiperCast) and TCP port 15001 for HiperOperator (remote control) to the IP address of the HiperController(s). One last port if needed is port 8000, if you are using HiperInterface (the Hiperwall API). Please note that NONE of these ports need to be opened into the Hiperwall VLAN unless you are using Hiperwall software from outside of your VLANTraffic originating on the Hiperwall network do not require this.

2. Bandwidth Requirements

1. Inside the Hiperwall VLAN
2. Outside the Hiperwall network

The Hiperwall network has strict network bandwidth requirements for internal connections. All Ethernet connections between Hiperwall computers on the Hiperwall VLAN to the network switch must be linking at 1Gbps and full duplex.

Some Hiperwall components are capable of network connections from outside the local Hiperwall network. These connections are called proxied connections since they rely on the Controller to relay (proxy) the captured content to the videowall. Proxy connections are initiated from outside the Hiperwall network and made to the Controller through ports 14999 (for the Sender, Browser, and HiperCast) and 15001 (for HiperOperator). Port forwarding is required on the outside facing router for these connections to succeed.

Hiperwall applications such as the HiperSource Sender, HiperSource Browser, and HiperOperator are routable and generally use relatively little bandwidth (depending on actual use case). A network connection of 100Mbps is generally enough for these individual applications' network connections.

If there are many incoming HiperOperator, Sender, or Browser connections and/or there is enough concurrent Sender or Browser objects with high enough capture framerate then 100Mbps may not be enough bandwidth at the network connection to the Hiperwall to sustain desired framerate.

The Sender and Browser have self-regulating internal mechanisms that automatically adjust framerate to minimize dropped frames, which has a direct relationship to available bandwidth. If greater framerate is desired, more bandwidth on the network connection to the Hiperwall may be needed.

Consider the following scenarios:

Sender A is in a remote office, proxied to the Controller. It is capturing a live, updating spreadsheet which is displayed at full screen on a connected 1920x1080 display. Its framerate throttle is adjusted to capture at about 10fps. Bandwidth usage fluctuates mildly but peaks at 13Mbps.

Sender B is in another remote office, also proxied to the same Controller as Sender A. It is capturing a live updating intranet webpage which is also displayed full screen on a 1920x1080 display. The Sender's throttle framerate setting is set to maximum and is capturing around 8fps using between 90 and 120Mbps.

Sender C is of a remote employee who is sharing his work on his laptop to the audience viewing the same videowall as Senders A and B. His content is mostly charts and graphs, but one of the pages in his slideshow links to a YouTube video. The Sender on his laptop is set to maximum framerate capture. The capture window is set to full desktop of his laptop's 1920x1080 display. The Network Utilization numbers from his laptop shows about 13Mbps achieving about 10fps (similar to Sender A) while showing the charts and graphs but drops to about 5fps for the slide playing back the windowed YouTube video, using between 115 up to 180Mbps.

If all the senders were displayed at the same time the Hiperwall Controller would need 300 Mbps of bandwidth, in order to prevent throttling during peak usage.

HiperCast is another application that can run from outside the local Hiperwall network. It receives connections from multiple Sender and Browser sources and makes proxy connections to multiple different Hiperwall systems. Because HiperCast is an aggregator of connections, its network bandwidth requirements will depend on how many simultaneous connections are made through it. An approximate figure can be made by getting the sum of the individual network usage numbers of each Sender or Browser sources that connect with the HiperCast server. This sum represents the total incoming bandwidth usage. Multiply this sum with the number of destination Hiperwall sites configured in HiperCast. This value represents the maximum outgoing bandwidth usage. The sum of incoming and maximum outbound network utilization will be the HiperCast's total network bandwidth requirement.

Let's use the same Senders A, B, and C in the above scenario, but this time, they are pointing their content to the HiperCast server. Also, the HiperCast server is configured to share and relay the Sender content to three different Hiperwall systems.

We know from earlier that the aggregate utilization of the three Senders peaks at about 313Mbps. This represents the peak incoming bandwidth for the HiperCast server. Multiplying this by three (for delivering the content to the three Hiperwall sites) will use up to (313Mbps x 3 destinations) 939Mbps. In this scenario, having a Gigabit network connection for the HiperCast Server is recommended.

This knowledge base article lists a few strategies that can be used to limit the amount of bandwidth the HiperCast service consumes across the WAN link.

3. Multicast Considerations (IGMP)

Hiperwall uses IP Multicast for efficiently sending signaling and streaming traffic. All multicast on the Hiperwall VLAN will not be routable to other VLANs due to the use of the IGMP querier configuration on the local Hiperwall switch. In addition, all Hiperwall multicast traffic is sent with a TTL (Time To Live) of 1. Meaning, even if the traffic gets routed (possibly due to a misconfigured network) it will be dropped after the first hop.

If there are external multicast video feeds that needs to be displayed on the Hiperwall, those feeds will need to be received on a dual homed device or displayed on a device not on the Hiperwall VLAN and captured to a Hiperwall capture source. For example, you may have IPTV broadcasting multicast on a VLAN. On the Hiperwall IP Streams PC, you would need 2 NICs, 1 connected to the Hiperwall VLAN, and one connected to the IPTV VLAN. The IP Streams software will handle the connections from there.

IGMP is used to manage local VLAN multicast traffic and PIM is used to manage multicast traffic between VLANs. For multicast to function, a multicast router (MRouter) must also exist on the network. Having IGMP Querier enabled on the local switch allows the switch to become the MRouter. If PIM is enabled on the Hiperwall VLAN, the router may override the IGMP Querier setting on the local switch and elect itself to be the MRouter, forcing all traffic to pass through it. This will be much slower than if it goes through the switch's IGMP Querier. Due to this speed difference Hiperwall requires PIM to be disabled on the up-steam device port.

4. Network security

Network security can be broken down into 2 main categories:

1. Network switch/router configuration
2. Hiperwall topology

When it comes to network switch or router configuration, as a general rule, you can follow your company guidelines. It is possible that a setting on the switch can cause an issue with the Hiperwall system, however, if IGMP is working per Hiperwall guidelines (see the Network Switch section above), then most settings on the switch will not affect the Hiperwall performance. One exception to this rule is any type of flood control settings on the Hiperwall VLAN. Hiperwall is a high bandwidth application and can trigger port shutdowns if this setting is enabled.

Hiperwall topology can be broken down into 3 separate groups. Each with their pro's and con's.

3. Fully routable
4. Dual NIC
5. Network Island

Fully routable means that the Hiperwall VLAN is fully accessible from the outside. This means that ALL VLANs can communicate with the Hiperwall VLAN. The benefit to this topology is convenience. No port forwarding is needed, all network assets are available to the Hiperwall VLAN, remote control is easily accomplished, etc.

One small tweak you can make to the Fully routable configuration is to only allow certain Hiperwall nodes access to the rest of the network. This is easily configured by using static IP addresses on the nodes you want locked down (no network access), and leaving off the default gateway. This will block internet access, as well as any other network access that is not on the Hiperwall VLAN, but will allow all Hiperwall nodes to communicate freely.

A typical scenario is to have the Controller some Sources have access to the outside world, but HiperView PCs be blocked. This also will prevent any unwanted Windows updates, which can potentially break a perfectly working system.

A Dual NIC setup means that the Hiperwall Controller PC(s), and possibly others, have 2 or more NICs in the PC. One network connection will go to the Hiperwall VLAN, and the other(s) will go to the corporate network. This setup allows you to keep the Hiperwall VLAN isolated from all other VLANs, and control which Hiperwall PCs will have access to other VLANs. This setup potentially is more secure than fully routable.

A Network Island topology means there is no IP communication between Hiperwall PCs and the rest of the network. This is the most isolated setup with all sources coming via video cables to capture cards or h.264 encoders. The downside to this isolation is some of the more advanced features of Hiperwall will not be available. These include controlling the wall from a workstation or sending a remote screen to the wall.

Sharp NEC Display Solutions Europe GmbH, Landshuter Allee 12-14, 80637 Munich
phone: +49 89 99699-0 | e-mail: infomail.sndse@sharp.eu | www.sharpnecdisplays.eu

© 2024 All rights reserved. All product specifications and pricing subject to change without notice.