IP addressing

This White Paper is only applicable for Prelude and Nemesis series. For Foundation series, please refer to the Quick Start Guide.

The ISAAC® Platform is built from the ground up to enable users and administrators the flexibility to use and manage their systems without worrying about physical access.

ISAAC® is logically separated into 3 operational levels: the physical hardware, a virtualization solution, and the virtual machines that run the system's workload. Each level has at least one point where it is connected to a network for access and management.

What‟s on the network?

Unlike most traditional audiovisual equipment or appliances, the virtualization features of the ISAAC® Platform allow some of these components to dynamically move and balance across physical connections and hardware. Where that more traditional approach requires a one-to-one mapping of physical connections (ethernet patch points) to logical connections (IP addresses) the ISAAC® system is more flexible to changing demands in the virtualized components.

Level 1 - Hardware

All ISAAC® hardware is configured, managed, and monitored over the network.

Servers

ISAAC® servers have a discrete baseboard management controller (BMC) that can interact with and monitor the main system regardless of its current running state. This controller has a dedicated physical connection on all current ISAAC® servers. From the BMC's webpage you can power the server on and off, access the built-in network KVM for troubleshooting, and change hardware configuration.

Nemesis Shared Storage

The shared storage appliance that ships as part of an ISAAC® Nemesis system has redundant chassis controller modules. They each have a dedicated physical network connection and serve web interface to manage the storage pool and view warnings or logged data.

Level 2 - Virtualization

Between the physical hardware and virtual machines running on an ISAAC® server there is a thin Hypervisor layer. A Hypervisor is a very minimal operating system, like GNU/Linux or Windows, but is purpose-built to run and manage virtual machines. Each server runs a Hypervisor which has a logical network interface serving management web pages and a control API. In an ISAAC® system direct access to this level is rare, usually reserved for troubleshooting and VMWare configuration. Most control and management of the system will be done through the ISAAC Workspace, which in turn interacts with the virtualization layer on the user's behalf.

This is the first level at which logical connections may start to differ from physical connections. Every ISAAC® server has multiple general-purpose network ports that can be configured to conform with the greater network. The most common configuration is as a pool (1), where all ports are configured identically with any VLANs (2) that may be required and any logical connections are dynamically assigned to some combination of physical connections.

In a Nemesis system there is an additional pair of physical interfaces and one logical interface per server. These are dedicated links for Fault Tolerance features and do not interact with the outside network, the two hosts are directly connected to each other. These are assigned by default as shipped and don’t need addresses assigned. They therefore don’t appear in the IP requirement address list below.

Level 3 ‘ Virtual Machines

All the real work and user interaction with an ISAAC® system is done in Virtual Machines (VM). These are the self-contained operating systems and applications used to control and manage your environment. All ISAAC® systems will have at least a VM that hosts the ISAAC® Workspace itself and may be configured with additional VMs for specific tasks (show or lighting control, programming tools, etc.). Nemesis systems will also have a VM dedicated to running a cluster management appliance that interacts with the virtualization level and ISAAC® Workspace APIs to provide redundancy and control features.

As fully virtual parts of the system, the logical connections for these VMs will dynamically assign and migrate to the subset of physical ports available depending on which hardware they are running on and balancing decisions made by the virtualization system. AV system designs using the ISAAC® Platform cannot assume that any VM will

exclusively use any single host or physical network connection as that would prevent the redundancy and failure tolerance the platform is designed for (3).

Configuration Prerequisites

When a Nemesis ISAAC® system is configured, the Cluster Management VM generates and manages certificates that are tied to its IP address. Changing IP addresses or switching from DHCP to static IPs after the fact for either the Cluster Management VM or the hosts compromises these certificates and requires the Cluster Management VM to be re-installed to regenerate these certificates properly.

Therefore, it is required to know what the desired IP address is upon configuration of a Nemesis ISAAC ® system. If no specific requirements are provided before shipment, all components will be configured to use DHCP.

In the event of the default DHCP configuration or the provided static IPs are incorrect, the Cluster Management VM will have to be re-installed after shipment. Clustering based features of the system (High Availability, Fault Tolerance, and seamless migrations between hosts) will not be functional until that is done. Reinstallation of the VM may incur additional cost and scheduling constraints for the involvement of ISAAC Support resources, which most likely will generate delays in the final availability of the ISAAC® system.

Summary

In general, to provide the remote management and robustness required of an ISAAC® system each will present multiple logical and physical network connections. Logical connections may be distributed across physical connections to maximize availability and will dynamically shift to balance workloads.

When designing an ISAAC® system into a network, keep the following addressing requirements in mind:

Prelude Systems (3+ IPs)

- 1 for hardware BMC (4)
- 1 for virtualization hypervisor (4)
- 1 for ISAAC® VM (Workspace)

Depending on specific configuration and usage:

- 1 or more for any additional VMs

Nemesis Systems (5) (8+ IPs)

Each system will require IP addresses for:

- 2 for hardware BMC (1 per server) (4)
- 2 for virtualization hypervisor (1 per server) (4)
- 2 for storage appliance controllers (4)
- 1 for ISAAC® VM (Workspace)
- 1 for Cluster Management VM (4)

Depending on specific configuration and usage:

- 1 or more for any additional VMs

(1) The hypervisor balances across connections based on MAC address. Switch connections do not need to be configured for LACP/LAG bonding.
(2) ISAAC® supports a mixture of VLAN tagged and untagged traffic on these ports; configuring them as trunks with all traffic tagged is suggested.
(3) This does not require any special support by other networking equipment and will be compatible with all modern infrastructure.
(4) In an environment with a dedicated management network, we suggest designating these items as management.
(5) Nemesis 900 systems may have different requirements.