Network Requirements

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

Designing for ISAAC

The ISAAC® Platform incorporates innovations and tooling from the IT industry into Audiovisual control systems. Based on battle-tested hardware and software users can leverage common IT equipment and approaches to greatly increase connectivity and integration of Audio-Visual systems into shared infrastructure. This inclusion of concepts from outside the traditional Audio-Visual space and increased reliance on networking may require additional focus to be placed on the network design for systems looking to incorporate ISAAC®.

Overview

Requirements and recommendations based on configurations:

Required for all ISAAC®deployments

- Multiple physical network connections to each ISAAC® hardware item
- Routing (IP Layer 3) to any network segments that must communicate with ISAAC®

Required for ISAAC®Nemesis deployments (recommended for Prelude)

- 1 or more for any additional VMs

Recommended for ISAAC®deployments

Each system will require IP addresses for:

- Dedicated VLAN for system management functions
- Separated VLANs for system segregation
- Centralized firewall for auditing and access control
- VPN access to ISAAC® network for remote access

Details

VLAN Segregation

All layers of the ISAAC® system have separate network interfaces for management features and traffic from normal operation. IT environments will often isolate these management features into a restricted IP address space and separate VLAN to better control access to critical operations. When ISAAC® is deployed in an environment where there is a separate management network, it is suggested that the ISAAC® management interfaces be assigned to it.

As a fully virtualized ecosystem, defining and connecting VLANs to Virtual Machines in an ISAAC® system is essentially "free"(1). Designers are free to borrow from IT and plan for more granular control and layout of their networks. Increased granularity allows for higher levels of access control and auditing, as well as easing the integration or convergence of AV and IT infrastructure, tooling, experience, and their respective costs and requirements.

Routing and Firewalling

Isolating and containing network connections into granular networks provides no benefits if those connections have no way to communicate to each other. Including a router in network designs not only allows that communication but also provides a known control point to implement access control, firewalling, and logging/auditing. All ISAAC® network connections support being routed, and firewall rules can be used to control access to certain ISAAC® features (2).

Outside Services

For optimal operation ISAAC® can utilize standard IT infrastructure services. All ISAAC® equipment can use the Network Time Protocol (NTP) to synchronize internal clocks and Domain Name System (DNS) to assign human-readable designations to IP addresses. On ISAAC® Prelude systems both are optional; on ISAAC® Nemesis systems NTP is required, and DNS is highly suggested.

Remote Access

ISAAC® relies on leveraging existing infrastructure for remote access. Systems requiring remote access will ideally implement VPN connections allowing remote users to connect the network. Using a VPN allows administrators and designers to leverage auditing and firewalls to manage, track, and secure all access to their networks. This also allows for remote access of any other equipment on the network, not just dedicated access to individual endpoints.

ISAAC® does not natively expose a VPN server; but VPN can be configured within ISAAC® virtual machine for small installations. Bigger installations or designs that are planning to highly leverage VPN connections are suggested to manage those connections on a dedicated device (often a central router).

Most modern IT networks are designed with VPN access in mind, so systems converging AV and IT systems can often benefit from using that existing infrastructure.

UPS Monitoring

ISAAC® integrates a monitoring system able to connect to a network connected UPS via SNMP and trigger actions based

on its status. ISAAC® can be configured to automatically safely shutdown based on customizable trigger conditions.

The monitoring requirements and IT-focused design of ISAAC® hardware leads to some system actions needing more time to execute than traditional audio visual equipment. Safely Shutting down ISAAC® servers requires first shutting down any VMs that may be running on it and then pre-setting configuration to be used on the next boot. Due to these extended requirements designs with ISAAC® should allow for a minimum of 15 minutes of UPS runtime in the event of a shutdown.

Similarly, booting an ISAAC® system from a cold start requires more time than may initially be expected. All ISAAC® hardware contains multiple sensors and embedded equipment to enable enhanced reliability and online maintenance. After the hardware is initialized the virtualization layer must start and begin booting individual VMs. The time to boot will depend on the number of VMs and the order they boot in but will require a minimum of 10 minutes before system services come online.

With those requirements in mind incorporating a network-connected UPS into ISAAC® designs is highly recommended. UPSs should be sized to allow for at least 20 minutes of runtime to allow for a safe system shutdown. For installations where temporary power losses are likely designing for extra UPS runtime can greatly mitigate the risk of a 30 minute outage for shutdown and power on due to short power interruptions.

(1) Adding/assigning network interfaces is a run-time configuration change, compared to physical cabling changes or outage causing resetting of traditional, dedicated AV hardware.
(2) See the companion document Connecting to ISAAC® for details on ports and connections.
(3) Some VMs or modules may require NTP for scheduling consistency.