

Architectural Approaches to Multi-Network Visualization

Secure integration while maintaining strict network separation.

Prepared by: John Stark, VP Product Management, Activu Corporation

LAST EDIT	DOC VER	EDITOR	NOTES
4/27/2023	V1	Jstark	Initial Release

Introduction

Government, military, and civil organizations tasked with operating at the highest levels of secrecy and security use separate, strictly isolated networks to ensure that information transmitted and shared on those networks are available only to authorized users. Additionally, network isolation ensures that the information present on connected systems is not contaminated through unknown sources, allowing users to trust the information they are accessing.

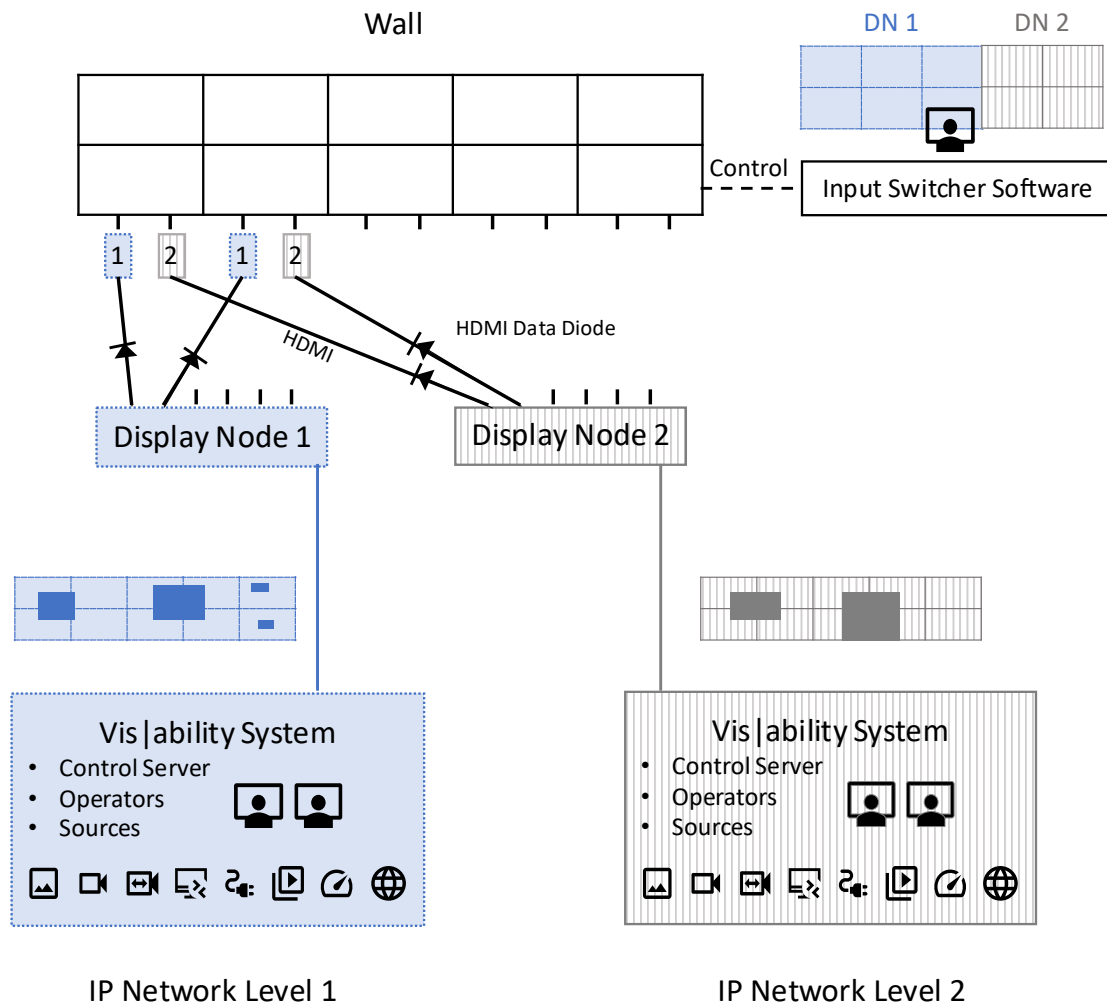
Secure networks are named according to their security level or operational application. For example: NIPR (Non-classified Internet Protocol Router – non-classified), SIPR (Secure Internet Protocol Router - secret/classified), JWICS (Joint World Wide Intelligence Communications System – secret/classified defense intelligence), NSAnet, among others. Networks that are unclassified and have more permissive access policies are considered “lower” networks, whereas networks that contain highly classified information, and are therefore strictly limit who has authority to access that network, are termed “higher” networks. Information, in general, can never move from a higher classification to a lower classification, but the opposite is not true – data in lower classifications can be “brought up” to higher classification networks under specific circumstances.

Network isolation, although necessary to maintain security and secrecy, presents significant challenges for command staff requiring an integrated view of information found across multiple networks, and organizations in general where access to content across networks is needed to gain and maintain situational awareness. The convenient, aggregated visualization of multiple levels of classified data is necessary to identify, assimilate, and integrate related information, and is critical to making fast, accurate decisions in response to time-critical events.

This white paper will discuss multiple approaches to providing that integrated view of multiple network content, while maintaining strict separation between the networks. Each approach has pros and cons that will be discussed, with emphasis on the ability to share information on a common video wall, but also to provide collaborative access within a command.

Architecture 1: Input Switching Direct to Display Wall

In this approach each network level has its own independent vis/ability system, allowing users within that network to take full advantage of the collaborative capabilities of the platform, including having exclusive video walls for intra-network display and collaboration, and the ability to communicate among users on that network using vis/ability.



To integrate multiple network content onto the same visual surface, inputs to a video wall are switched to show outputs of a Display Processor (in Activu vis/ability terms, a Display Node) on that network. Display Node outputs are either connected to the video wall via a hardware data diode, or are run through a short fiber transceiver pair, for isolation purposes. Each network level is connected to a consistent input on all displays in the video wall, for example, input 1 is for non-classified information, and input 2 is for classified information.

The video wall outputs can be allocated to show all of one network, or subdivided among networks that are connected to the Video Wall displays. Control of which networks are visible is accomplished through a vis/ability application called the "Input Switcher", which is deployed onto an isolated control network and only communicates with the Video Wall displays.

To users on each network this Video Wall is treated like any wall in a single network environment, however, the visible portion of the wall is controlled by Source Switcher and is designed to be operated at the highest network level to view information from multiple connected networks.

Cons:

- A common single video wall cannot be operated normally when more than one network level is displayed on the video wall.
- The total number of network levels is limited to the number of supported inputs on the display devices that comprise the video wall.
- It is possible to not recognize which network is present on the video wall.
- Inputs are only available on the Display Node, limiting the ability to support more collaborative or distributed workflows.
- To support more network levels than the total number of inputs per display device, it would be required to use a matrix switch with the total number of inputs be at least the number of network levels multiplied by the number of display devices in the video wall, and the number of outputs on the switch to be the total number of display devices in the video wall. For larger video walls, or for many network levels, the matrix switch can become very expensive. Alternatively, multiple smaller switches can be used for system scale, at the cost of complexity.

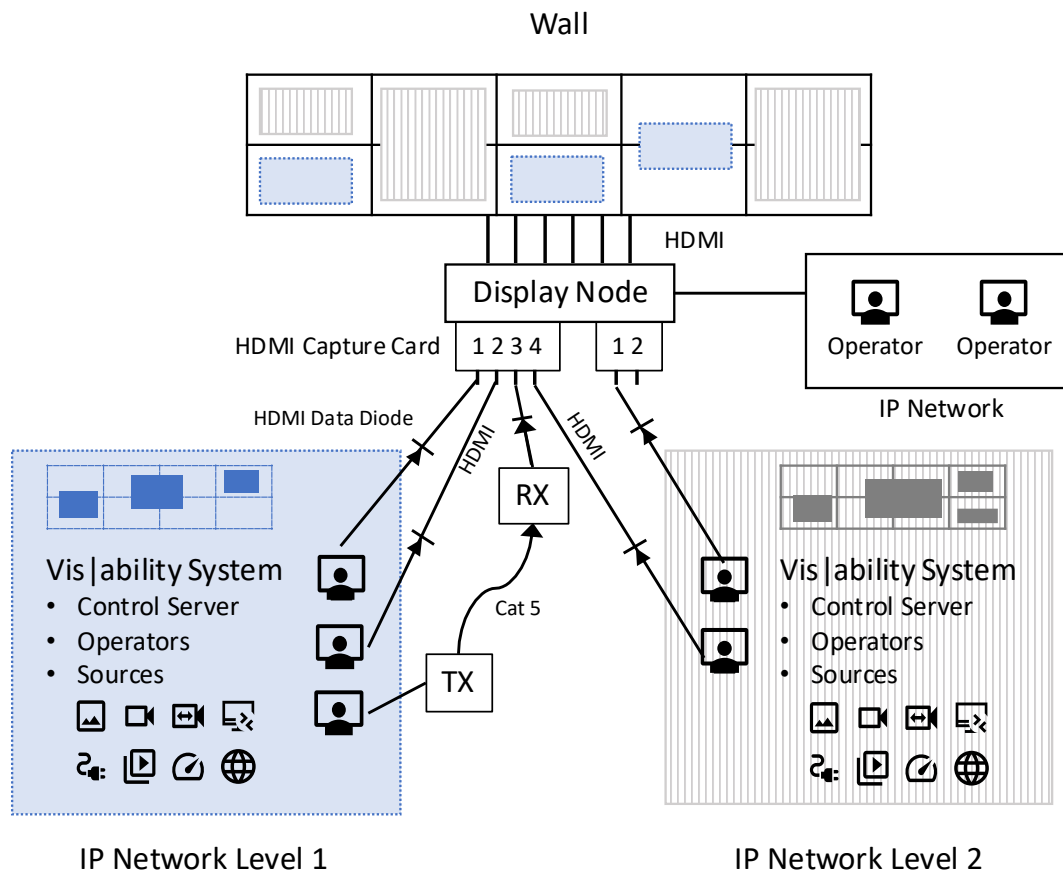
Pros:

- Each vis/ability system has complete functionality, with the ability to manage and present content from various sources of information: network capture, IP cameras, web (intranet), media and images, as well as local applications.
- Collaboration can occur among users within a network level.

Architecture 2: Baseband Input Direct to Display Node

Similar to Architecture 1, this design varies in that it takes direct baseband input into a common Display Node and displays them as windows on a video wall. This allows content from each network level to be mixed in a windowed environment with commensurate functionality. Windowed content on the Display Nodes can be labeled and coded with appropriate border colors, providing consistent identification of the source network.

Network isolation is maintained through data diodes or unidirectional optical transmission.



Video wall management is achieved through a separate control network, although the control network could also be present on a secured network and bring content to the video wall. Video wall management is typically done on the highest security level network.

Cons:

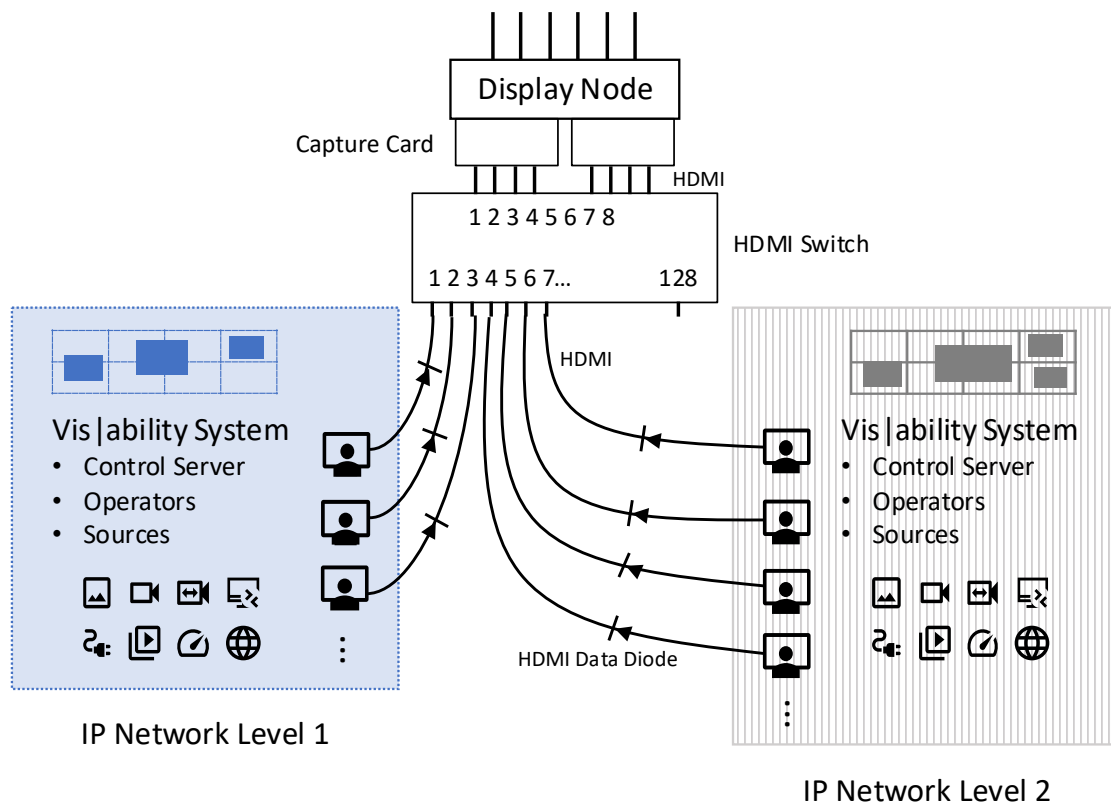
- Limited number of inputs based on Display Node configuration.
- Limited number of supported network levels based on Display Node configuration.
- Inputs from other networks are limited to desktop capture.
- Inputs are only available on the Display Node, limiting the ability to support more collaborative or distributed workflows.
- Potentially difficulty validating the applicability of the hardware used in the Display Node without specific support from the manufacturer (e.g. Volatility Statement, Immunities Testing).

Pros:

- High performance of captured inputs.
- Flexible display of content on the video wall.
- Compact and simple design.
- Cost effective.

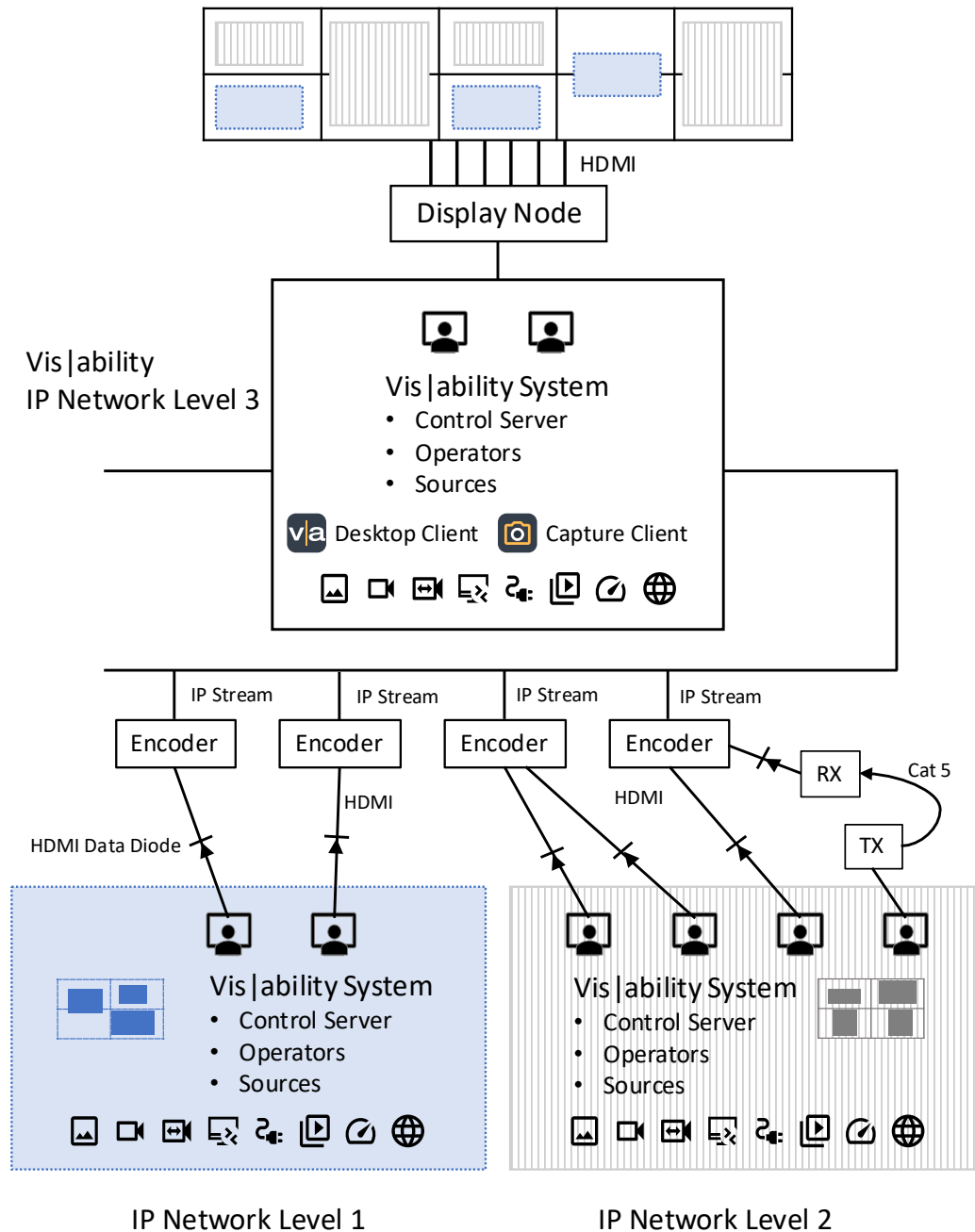
A variation of this design architecture could include an upstream matrix switch, using data diodes to isolate the network, or a matrix switch that is certified to handle secure content. This could expand the scale of inputs and allow for more than one Display Node. However, secure matrix switches of this nature are costly and provide fixed configurations that are difficult to expand over time. This approach

also comes at the cost of flexibility; specialized AV technicians and control system designers will be required to alter the system.



Architecture 3: IP Encode to Higher Networks

This architecture, rather than direct lower network content rendered on computers directly into video walls or Display Nodes (then onto video walls), uses baseband capture and IP encode devices (video encoders) to take network isolated content and deliver it as encoded streams onto a higher network classification.



Modern encoders and Display Nodes can support SRT and other secure streaming technologies, avoiding unauthorized access on the network. Additionally, current encoders can support high resolution content.

This architecture, using video streaming technology, allows for flexible use of content: displayed as scalable windows on one or more video walls, on authorized desktops, and within collaborative tools that support IP video streams. Additionally, this approach makes it simpler to scale the deployment – adding or removing encoders as needed. Adding or removing access to network levels is also simple to do, not requiring the provisioning of esoteric equipment such as secure matrix switches.

IP streams can be labeled and coded with appropriate border colors, providing consistent identification of source network simple. Metadata in the stream definition can further enhance the ability to identify the origin of content.

<diagram>

Cons:

- Requires many devices to encode content into IP streams.
- Cost scales quickly with many inputs or network levels to support.
- Potential security risk with distributed capture and encode creating many points of contact with secure networks.
- Content can potentially be accessed anywhere on the target network, if the network is misconfigured.
- Streams displayed on end points (Desktop computers, Video walls) can exhibit significant latency.
- Lossless compression requires high network bandwidth provisioning (10+ Mb/s).

Pros:

- Content is available anywhere on the target network.
- Scale is simple to accomplish, input count can be virtually unlimited.
- Content from multiple networks can be viewed on one or more video walls, in freely scalable windows.
- Users on the target network can collaborate without tying up video wall resources.

Conclusion

Secure networks pose significant operational challenges when there is a need to assimilate information from multiple security levels into a common operating picture. To support these applications, there are several approaches to provide the operational and visualization flexibility, while maintaining security and strict network isolation policies found in many government and military environments.

Primarily AV approaches have the benefit of, generally, simplicity and price efficiency, but at the cost of scalability. IT centric solutions (Architecture 3: IP Encode to Higher Networks) come with superior deployment flexibility with cost scaling as the deployment grows, but at the price of technical complexity and perceived risks with streamed content on a secured/classified network.

Activu vis|ability can operate on the highest-level classified networks, as well as on lower and unclassified networks, providing the ability for lower network operators to provide content to higher classification networks, as needed. Within any specific network level, all operators connected to vis|ability can take advantage of collaborative functionality, if granted access – including video walls dedicated to that network level.

Activu vis|ability can support any and all of these approaches to multi-level network visualization.