Value Your Content

thinklogical®

Trust Our Proven Ingenuity

Recommended Best Practices for the Design of Secure Multi-Domain KVM and Video Routing Systems

A Whitepaper from
the Thinklogical Design Center

Table of Contents

About the Thinklogical Design Center

The Thinklogical Design Center (TLDC) is an invaluable resource available to our customers and partners. Led by two industry pioneers and co-founders of Thinklogical, David Cheever and Peter Henderson, the center has worked with customers and partners to provide thousands of conceptual system designs for requirements that range from the straightforward to the extremely innovative and complex.

Backed by a staff of tenured, industry-specific application and development engineers, the center helps customers and partners discern their needs and requirements, and then develop the appropriate system design. Often, features and functions are utilized in the design that the customer or partner had not previously considered. Sometimes, features or functions are customized or even created during the design discussion, utilizing Thinklogical's rapid development capability.

Typically, an initial TLDC consultation is a phone call lasting an hour or less. Initial system designs are usually completed within 24 hours. All TLDC services and consultations are complimentary.

To contact the TLDC, please call 800-291-3211, or email tldc@thinklogical.com

Executive Summary

In most cases, an organization's KVM and Video Routing systems are considered mission or business critical. These systems are typically deployed in areas that are core to the mission or business operation. They usually provide highly sensitive or very important content to users who are driving key organizational processes and making mission critical decisions. This is true whether the content is military intelligence, post-production video and audio, energy production control data, or video and audio from a live event, to name just a few examples. For these reasons, the security characteristics of KVM and Video Routing systems are of paramount concern.

This whitepaper reviews the industry's current understanding of the security threat, and then explores best practices for designing KVM or Video Routing systems to ensure the security of the content, as well as the operation of the system itself.

Five key design criteria are recommended:

1. The system architecture should physically secure and separate the target of the attack (content or system operation) from the threat: people.
2. The technologies used in the system should eliminate the ability to attack from a distance; that is, sniff or eavesdrop on the system.
3. The system should allow the administrator to closely manage and control access in accordance with the organization's security policies.
4. The system should automatically and continuously monitor for and identify breaches.
5. The system should be resilient; that is, it should be designed to not only withstand an attack, but also recover quickly following one.

The Threat

For more than a decade, surveys to determine IT executive's priorities have identified securing an organization's content and systems as the top concern. This is true for both commercial and government/military organizations. In response, innovative new technologies have been introduced to address the security concerns.

A key driver of innovation in security technology is the ever-increasing understanding of the threat itself. For instance, there is now a broad awareness that the threat can come from employees and contractors as well as external entities. This was, of course, the case with the recent US military and diplomatic exposure through Wikileaks. While studies draw various conclusions as to which group represents the greatest threat, it is clear from all findings that both groups are cause for concern.

Industry understanding has also moved beyond the simpler notion that all threats to the security of content and systems are malicious. It is now clear that loss of data, corruption of data, or user actions that may cause the system to fail can be entirely accidental mishaps by an otherwise well-meaning employee or contractor, yet still carry the same deleterious effect as the malicious action.

In addition, the various intents of a malicious attack have come into clearer view. Illicit or illegal acquisition of data has always been understood as a purpose for an attack. But equally important and increasingly frequent is the intentional disruption of mission/business critical systems with the intent of crippling the effective operations of businesses and government organizations.

Finally, an important aspect of any attack is whether the attacker is physically present, or limited to remote access.

Perhaps the security threat is best summarized with two simple observations: First, the focus of an attack is either to steal content, disrupt the operation of the system or both. Second, the attacker is always a person who has gained some immediate or remote access to the system.

These statements may seem oversimplified, but as we shall see in our discussion below, together they form the underlying principles in the development of a secure design. A robust system design first seeks to physically separate the threat from the target of the threat; that is, the people from the content. Second, a robust system design will provide the tools necessary to closely manage and control the interaction of authorized users with the system.

> *"The focus of an attack is either to steal content, disrupt the operation of the system, or both... The attacker is always a person who has gained some immediate or remote access to the system."*

> *"A robust system design first seeks to physically separate the threat from the target of the threat; that is, the people from the content."*

Introduction to KVM and Video Routing Systems

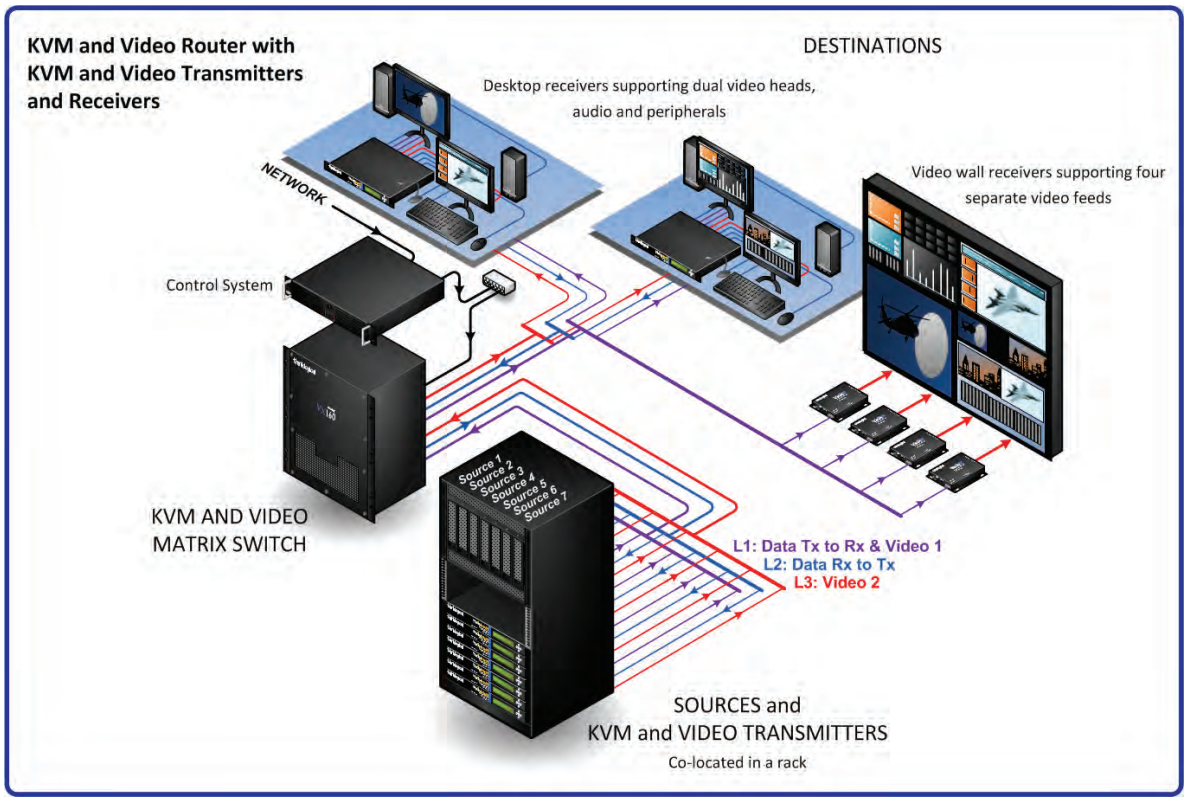
At a high level, a KVM or Video Routing system is the system, comprised of transmitters, receivers and routers (matrix switches), required to switch users between multiple sources and multiple destinations, using one set of user interface peripherals, such as a keyboard, video displays and a mouse.

Some common application environments for KVM or Video Routing systems include command and control centers, post-production editing suites, scientific modeling and simulation centers, or content analysis and distribution operations.

The difference between a KVM system and a local area network (LAN) is that the user, with one set of peripherals, requires access to several sources (servers, computers, databases, etc.), and they desire to switch between those sources and several destinations, which might include the display in front of them, a video wall, a DVD burner, etc. A LAN connects one user's computer to other users' computers or servers; a KVM system connects one user's peripheral devices to multiple computers, servers, displays, etc. that are "user-independant".

When multiple users need to access multiple sources and be able to connect to multiple destinations, a router (matrix switch) must be included in the system. Since video content is by far the largest constraint in the design of this router, the router is often called a Video Router (video content, compared to data and audio, utilizes most of the bandwidth).

Simple KVM and Video Routing System Example



Recommended Best Practices for Secure KVM and Video Routing Systems

Approaches to countering a security threat can be broadly grouped into five categories:

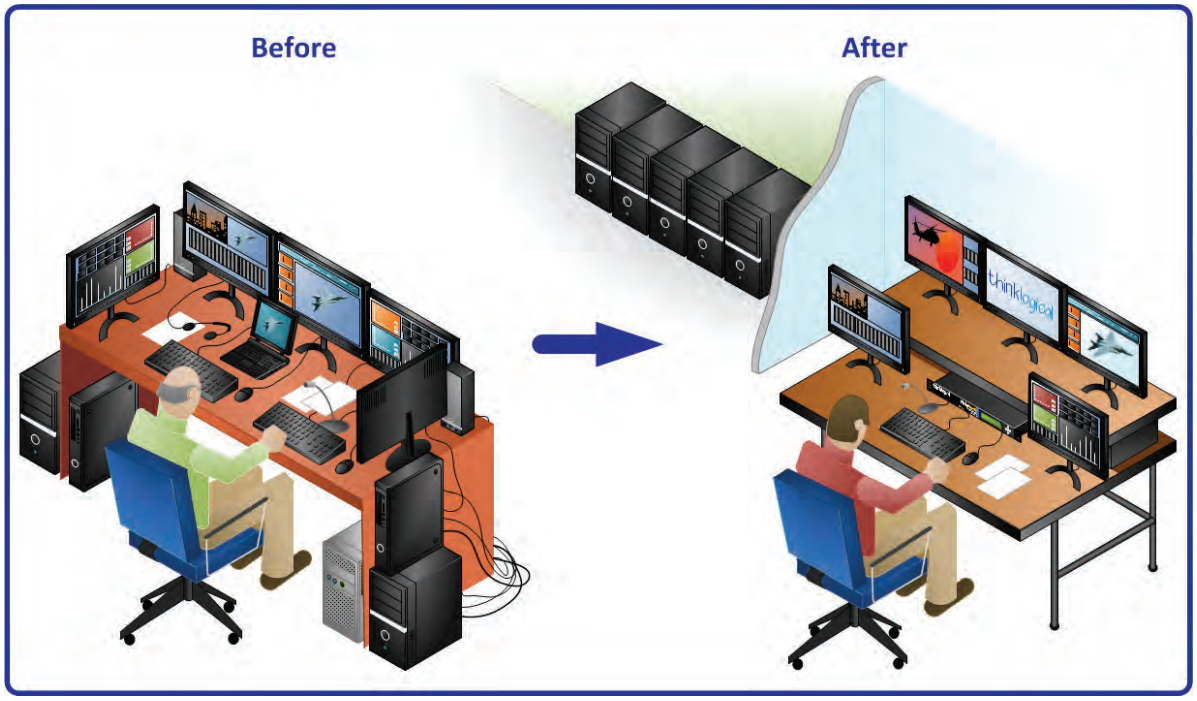
1. The system architecture should physically secure and separate the target of the attack (content or system operation) from the threat: people.
2. The technologies used in the system should eliminate the ability to attack from a distance; that is, sniff or eavesdrop on the system.
3. The system should allow the administrator to closely manage and control access in accordance with the organization's security policies.
4. The system should automatically and continuously monitor for and identify breaches.
5. The system should be resilient; that is, it should be designed to not only withstand an attack, but recover quickly following one.

Physical Separation

The objective of physical separation is to prevent the threat (people) from physically accessing the content or the system.

A common approach is to prevent unauthorized users from entering the physical location of the system, by restricting access through card readers, biometric readers, etc. This is a well-understood, sound and common practice for mitigating the potential threat from unauthorized users and external attackers.

But today's technologies allow for mitigation of internal attacks as well, through the physical separation of the threat (people) and the system: a robust KVM extension system provides high performance and secure access to the content for authorized users, without providing direct physical access to the hardware that hosts the content. With these systems, the source hardware can be located in a separate room, on a different floor, in a different building or even in a different town, effectively separating the threat (people) from the target of an attack (the content).



Separating users from computers can significantly reduce the threat that content and their attached networks will be perpetrated.

Eavesdropping

Fiber Optics are inherently and dramatically less vulnerable to eavesdropping attacks.

An important aspect of preventing the theft of content is the prevention of "eavesdropping." In this scenario, a perpetrator would gain access to the system using advanced technologies to intercept content through electrical, magnetic or acoustic emanations from the system. These are commonly termed "compromising emanations". With the right eavesdropping equipment, the perpetrator may be able to intercept these emanations from hundreds of meters away.

The most common system component identified as a culprit in the release of emanations is the wiring or cabling. In particular, copper cabling (twisted pair, coaxial, etc.) is a frequent target, as it produces significant emanations. Minimizing copper connections is a best practice.

System designers concerned about security avert this threat by using optical fiber whenever possible. Optical fiber does not produce compromising emanations. A perpetrator must physically "tap" into an optical fiber to steal content. Obviously this requires complete physical access. And often, the system can alert the system manager when a fiber has been tapped. In net, fiber optic systems are inherently and dramatically less vulnerable to eavesdropping attacks.

Management & Control

Limit user access to content and the system by limiting the number and functionality of peripheral ports.

Even with the source hardware separated from the users, authorized users will still be interacting with the system. This interaction provides another opportunity for security breaches. Therefore, a robust KVM system design will provide for close management and control of authorized user interaction with the system.

A first practical step to managing authorized users, is to limit their ability to copy content or inject malware using devices such as flash drives or other portable or concealable media. A good example of this approach is the management and restriction of USB ports whenever possible. In a secure KVM system, these ports will be limited in their functionality to the connection of Human Interface Devices (HID), or peripherals such as keyboard, mouse, controllers, etc. The ability to copy or inject content through a USB port will be functionally disabled.

Peripherals that use USB 2.0 present a particular problem. In these cases, it is not possible to limit the functionality of the port. Therefore, it is recommended that USB 2.0 ports only be used when there is no alternative.

Partitioning allows for isolation of resources within a router. Essentially, partitioning creates several isolated routers within a router.

A second focus is to ensure that authorized users only gain access to those parts of the system they are authorized to access. Sophisticated management techniques, most often deployed through software and firmware, are required to ensure the highest levels of compliance and lowest levels of intentional or unintentional violations of access rules.

For instance, KVM systems are often designed to access multiple sources across multiple networks with different security classification levels. A good example is the frequent requirement to operate "Red" and "Black" networks in a single military intelligence system (A Red network contains classified information in plain text, whereas a Black network contains classified information in an encrypted format, and/or non-classified information.) It is critical that a breach does not occur between these two networks, even though they may exist as part of the same KVM infrastructure.

Typically, there are two design approaches to manage issues like these: partitioning and restriction. Partitioning refers to the ability to dedicate resources within the system to isolated groups, with no chance of unintentional crossover, within a router, switch or system of routers and switches. Essentially, partitioning creates several routers within a router.

Restriction limits access to sources on a user-by-user, source-by-source basis.

Restriction addresses the idea of limiting access on a user-by-user, source-by-source basis. A strong KVM system design will allow the system manager to determine which users gain access to which sources, and perhaps more importantly, which users are denied access to which sources.

A strong technological approach to partitioning and restriction will minimize unintentional and intentional breach of the structure.

Security Monitoring

A secure KVM system design must include the ability to continuously monitor the system. The system should be capable of identifying breaches and attempted breaches, keeping records of breaches and attempted breaches, and providing information to help determine the nature of the breach and how it might be prevented in the future.

Resiliency

The final component of a secure KVM system design is resiliency, or the ability to recover should a breach occur. Clearly, mission critical systems must provide for redundancy at the component level, through functionality such as redundant power supplies and hot-swappable components. But a secure KVM system should also provide for automatic failover at the system level. If an intentional disruption of the system occurs, it should have the ability to immediately and automatically re-establish operation in a parallel system.

Secure KVM and Video Routing Systems from Thinklogical

At Thinklogical, secure KVM and video routing and extension is one of our top priorities for innovation and development. As such, we have been very successful in introducing systems that meet the most rigorous security and information assurance standards. We have provided hundreds of systems to users in the most secure markets in the world, such as the US Military and Intelligence Community, several European Ministries of Defense and NATO.

These customers, many of whom have the most demanding security requirements in their industries, have chosen Thinklogical for several reasons:

- Thinklogical systems can be designed to achieve, over significant distances if necessary, separation of the threat (people) from the target of the threat (the content)
- Thinklogical systems are fiber optic based, significantly reducing the opportunity for eavesdropping
- Thinklogical provides a robust and flexible suite of advanced security features and functions that allow for close management of user interaction in multi-domain environments to prevent attacks, and the resiliency necessary to withstand an attack
- Thinklogical provides the functionality required to allow for continuous monitoring of the system
- Thinklogical offers the highest performance in the industry, with 6.25 Gbps of bandwidth per thread, in a scalable, protocol-agnostic, completely non-blocking switching matrix. As a result, Thinklogical equipment transports every resolution of computer or broadcast video available today, with no compression, lost frames or artifacts.

And perhaps most importantly, because of these differentiators, Thinklogical has achieved the unique status of being accredited to The Common Criteria, Evaluation Assurance Level 4 and TEMPEST standards. We believe we are the only fiber optic based KVM and Video routing systems to have achieved these accreditations.

Design Concept	Thinklogical Approach & Benefits
Physical Separation	• Separate the threat (people) from the target of the attack • Sources (servers, computers) can be separated from destinations (keyboard, mouse, video wall, etc) by as much as 1,000 meters using multimode fiber or 40 kilometers when using single mode fiber • Realize additional benefits such as space management, flexibility and reduced noise and heat in the user area
Fiber Optics	• All Thinklogical products are designed specifically for use with fiber optics, making them inherently and dramatically less vulnerable to eavesdropping attacks • Realize additional benefits such as additional safety, longer distances and less conduit space
Partitioning	• Create as many partitions as there are ports in the router • Thinklogical's partitioning is achieved in firmware, not software. A perpetrator would need to gain physical access to the router to launch an attack that included violating the partitions – and even then, the router would need to be rebooted for the changes to take effect. • *Please see Charts 1 and 2 for more detail.*
Restriction	• Restrict on a port by port basis • Thinklogical's restriction is achieved in firmware, not software. A perpetrator would need to gain physical access to the router to launch an attack that included violating the restriction scheme – and even then, the router would need to be rebooted for the changes to take effect. • *Please see Chart 3 for more detail.*
Monitoring	• Use Thinklogical's industry standard "traps" and "alarms" to create robust monitoring systems
Resiliency	• Configure a parallel redundant system with two, synchronized Thinklogical routers running in parallel (mirroring with identical signals). Thinklogical's unique "switchover capability" allows the system to automatically choose a stream to "lock onto" and then automatically failover to the parallel stream if necessary. • Complete redundant, hot-swappable components such as power supplies and input/output cards.

Accreditation

Perhaps the most significant testimony to the security benefits of Thinklogical systems is our achievement of accreditation according the The Common Criteria and our approval under TEMPEST standards. Thinklogical routers are the only fiber optic KVM and Video routers in the world that have achieved both of these accreditations. This has led to their deployment in secure facilities throughout the world.

The Common Criteria is a framework available to customers with high security requirements, to specify those requirements so that testing laboratories can create evaluation criteria and testing procedures for vendors who want to achieve accreditation against the customer's requirements. EAL, or Evaluation Assurance Level is the level to which the product or system was tested and successfully passed. EAL 4 is the highest level that can be achieved based on the technical merits of the system.

Thinklogical's KVM and Video routers are the only fiber optic KVM and Video routers in the world to have been tested and accredited to The Common Criteria. In Thinklogical's case, our routers were tested to The Common Criteria and accredited to Evaluation Assurance Level 4. This is a truly unique achievement in the industry – one that is relevant to any customer with security as a key requirement for their KVM or Video routing system.

In addition, Thinklogical's KVM and Video routers have been accredited to TEMPEST SDIP 27, Level B.

TEMPEST is a framework that organizations use to judge the appropriateness of a product or system for use within a high security application, with specific focus on compromising emanations (electric, magnetic or audio). There are three levels of TEMPEST testing (A, B and C), defined by the distance a perpetrator would need to achieve to intercept signals from the system. Level A assumes the perpetrator has immediate access to the equipment. Level B assumes a distance of 20m and Level C, 100m.

Thinklogical KVM and Video routers have been approved to Level B, meaning that a perpetrator cannot 'eavesdrop' content through compromising emanations at a distance of 20 meters or more.

Chart 1: A Simple Partitioning Schema for a Thinklogical VX 80 KVM and Video Router

In this diagram ports 1 through 20 (Partition 1) are dedicated to "Black Network 1," ports 21 to 40 (Partition 2) to "Black Network 2" and so on. As such, sources using ports 1 through 20 can only communicate with destinations using ports 1 through 20 and vice versa. A source or destination in Black Network 1 cannot communicate, intentionally or unintentionally, with any port in Black Network 2 or either of the Red Networks.

Since Thinklogical implements partitioning in firmware, a perpetrator would need to gain physical access to the router to launch an attack that includes violating this structure.

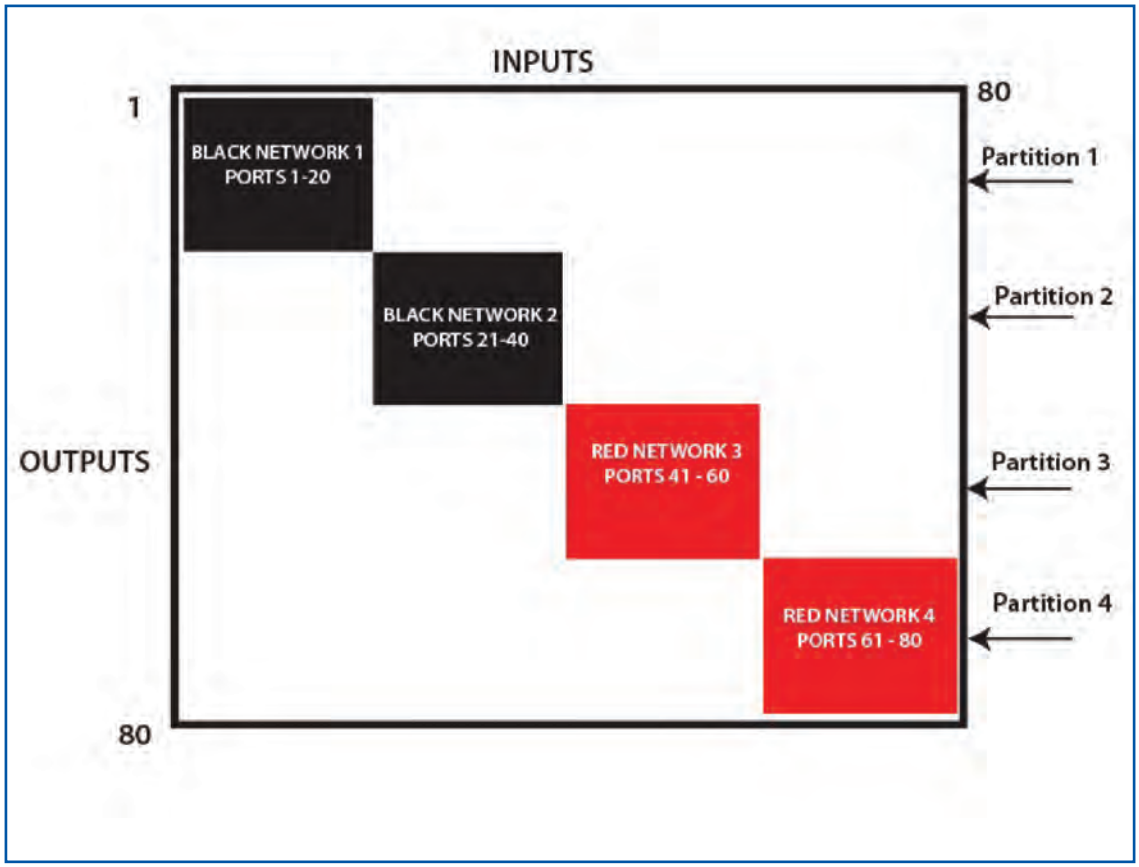


Chart 2: An Overlapping Partitioning Schema

In this scenario, the partitioning structure is implemented to allow for overlapping partitions. Ports 1 through 4 in Partition 2 are completely isolated. But ports 5 through 10 are accessible in both Partition 2 and Partition 3.

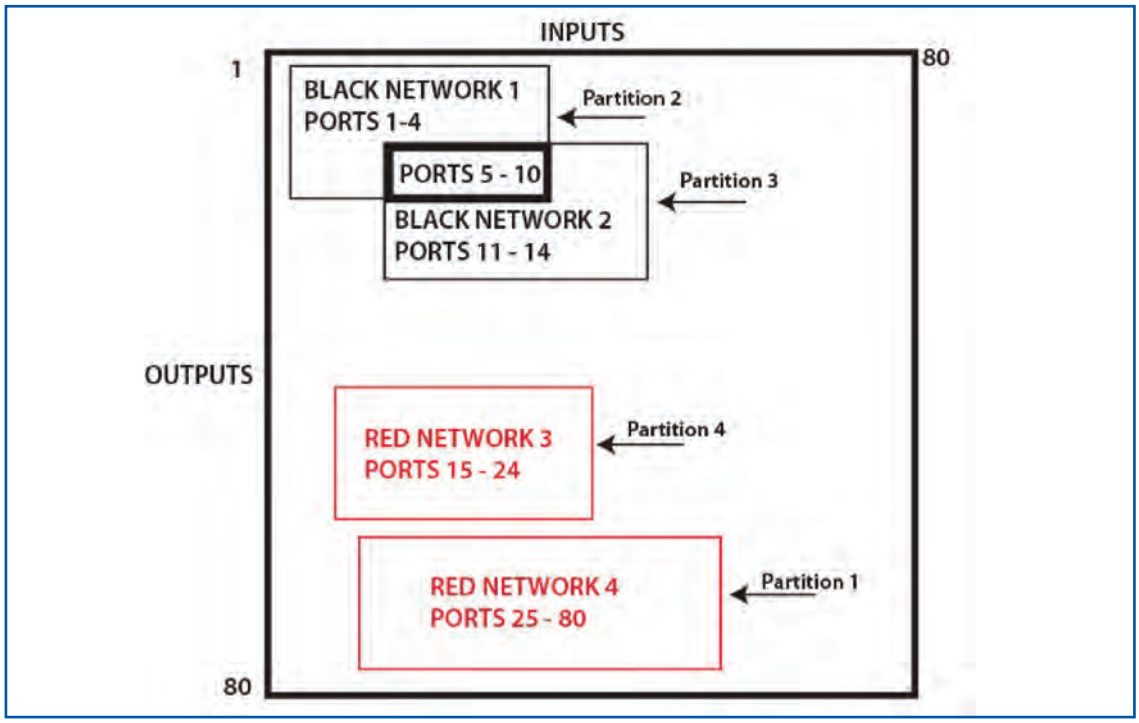
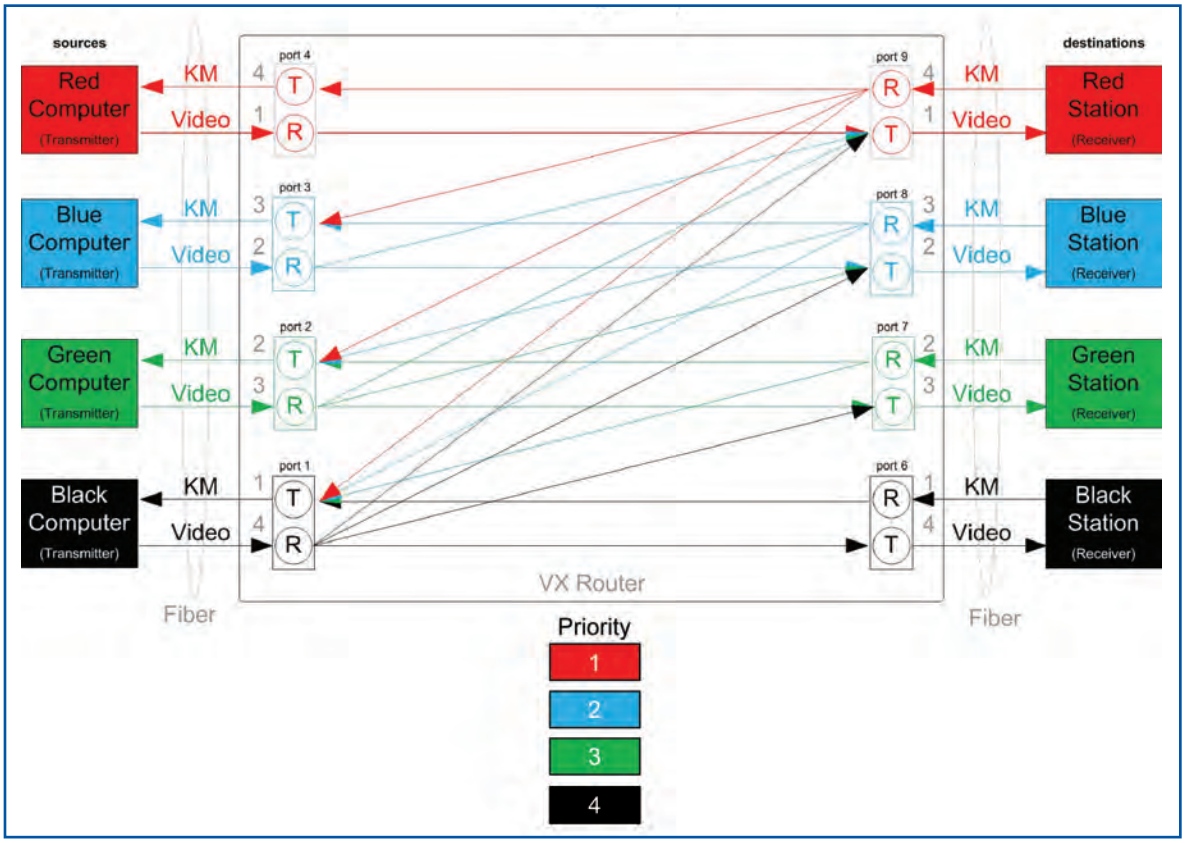


Chart 3: Restricted Switching Priority Scheme

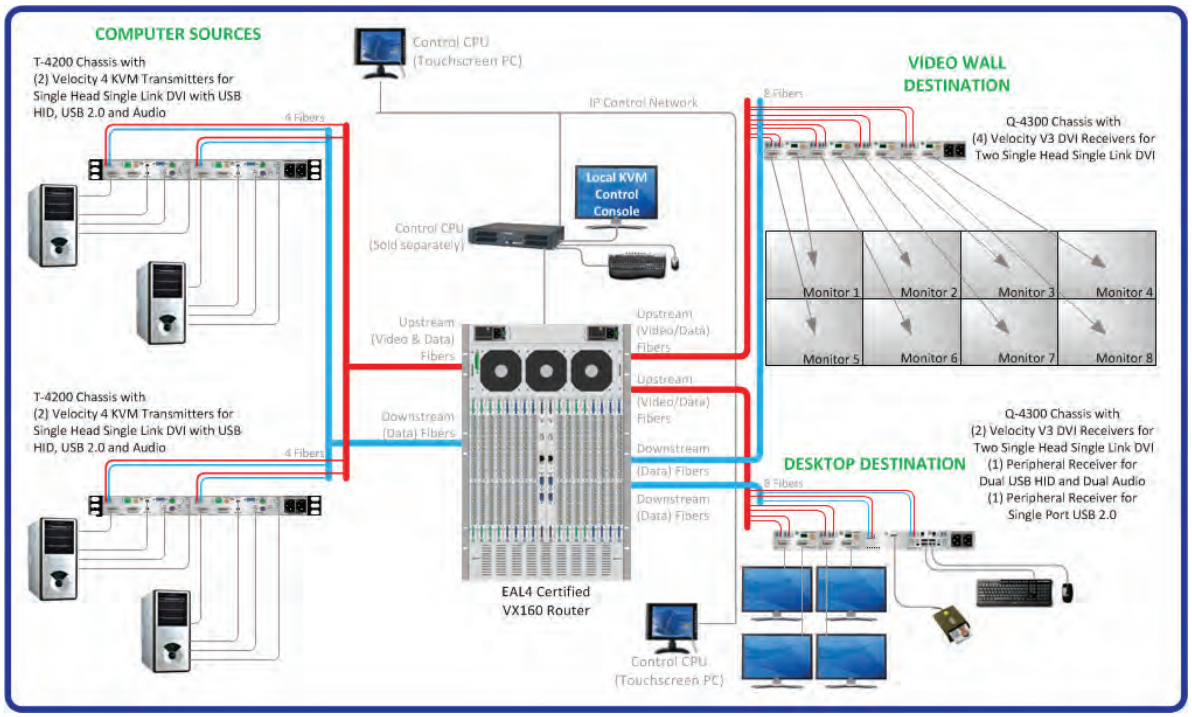


An Example Restricted Switching Schema

Thinklogical routers can be restricted on a port-by port basis. A priority level is assigned to each port. Ports can communicate with other ports, but only if the other port's priority level is equal to or less than theirs. For instance, in this diagram, Port 4 Receiver has a priority level of 1. Therefore, it can only communicate to Transmitters with priority level 1, which is the Transmitter on Port 9. Alternately, the Port 1 Receiver has a priority level of 4. Therefore, it can communicate to Transmitters with priority levels of 4 and below, which include the Transmitters on Ports 9, 8, 7 and 6.

Since Thinklogical implements restricted switching in firmware, a perpetrator would need to gain physical access to the router to launch an attack that includes violating the structure.

Thinklogical has provided hundreds of systems to users in the most secure markets in the world, such as the US Military and Intelligence Community, several European militaries and NATO.



Summary

The need for secure KVM and Video Routing systems is higher now than it has ever been. At the same time, technology advances are enabling innovative system design options that significantly improve the security of the KVM or Video system. Thinklogical is the world leader in providing these innovations. Robust technological approaches to partitioning, restriction, monitoring and resiliency, delivered in a fiber optic based architecture have caused customers with the need for highly secure systems to choose Thinklogical. Perhaps most importantly, Thinklogical's leadership is substantiated by their unique accreditation to Evaluation Assurance Level 4 under The Common Criteria and TEMPEST, Level B. This has resulted in deployment of Thinklogical systems in hundreds of secure facilities worldwide.

For more information or a complimentary consultation on your secure system needs, please contact the Thinklogical Design Center at 1-800-291-3211 or TLDC@thinklogical.com.

www.thinklogical.com

100 Washington Street
Milford, CT 06460 USA

Thinklogical Design Center
1-800-291-3211
TLDC@thinklogical.com