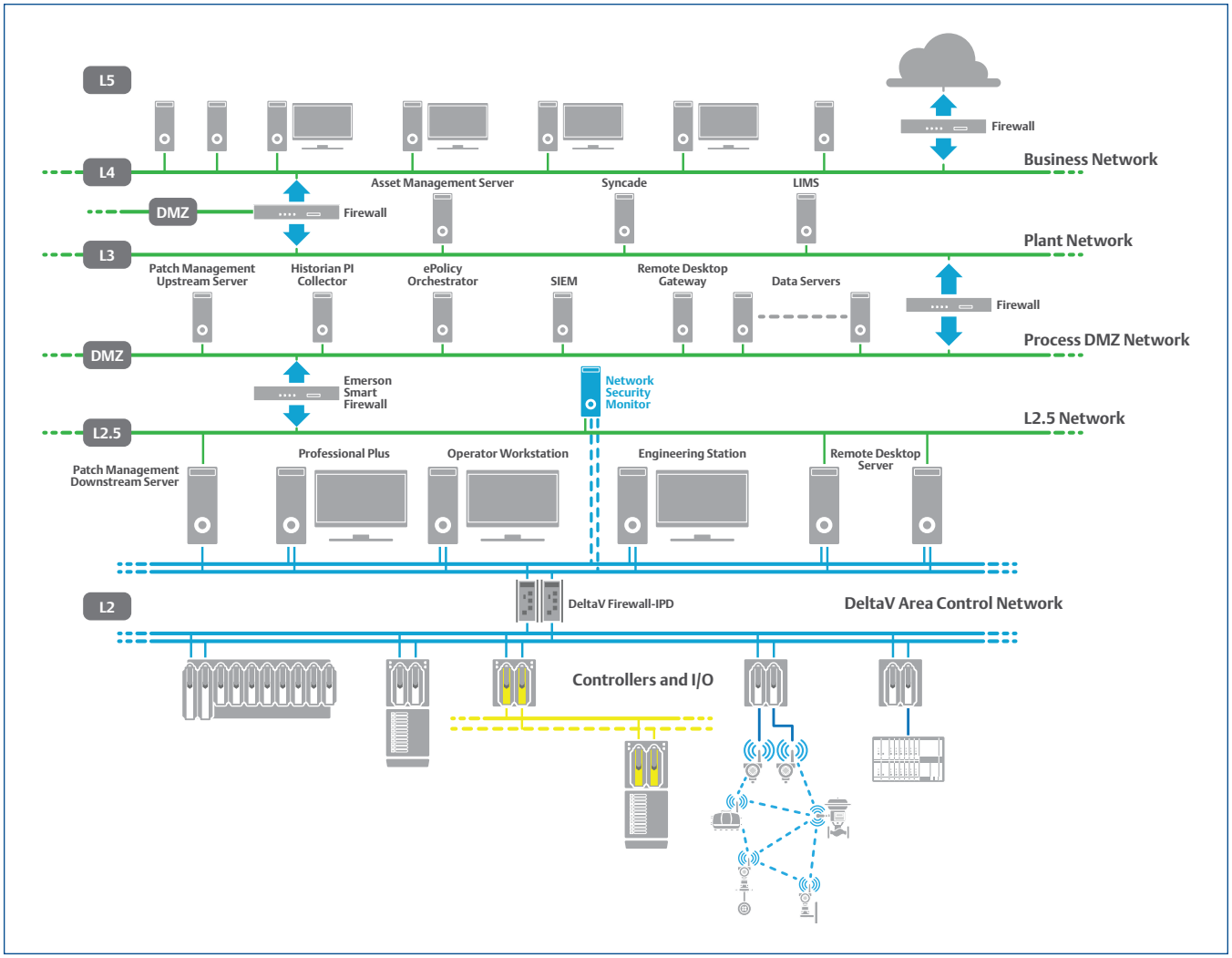
DeltaV™ Smart Switches Port Mirroring

This white paper provides information about the supported port mirroring feature for DeltaV Smart Switches.



DELTAV™

EMERSON™

Table of Contents

Introduction

A critical part of cybersecurity is monitoring, and many features, applications, and solutions are available to help you gather system data in many different ways. Workstations, servers, and network equipment can all log information that could collectively help identify a possible attack or misuse of certain system functions, which are usually forwarded to a Syslog Server and/or Security Information and Events Management (SIEM) console. However, network data comprises more than just events and alerts flagged by endpoints in a system.

Communications are encapsulated within the Ethernet data traffic and the DeltaV Area Control Network (ACN) is based on DeltaV Smart Switches, where end-to-end communications are not always broadcast. Therefore, only specific recipients have access to the packets sent by a given sender (unicast message). This white paper describes how the DeltaV ACN packets, whether broadcast, multicast, or unicast packets, can be mirrored – specifically directed – to the Network Security Monitor (NSM) for DeltaV Systems from any DeltaV Smart Switch on a port-by-port basis – you decide which ports to monitor (mirror) from an easy to use DeltaV configuration menu.

Network Security Monitor for DeltaV Systems

The NSM for DeltaV Systems is a solution based on the Intel Security Application Data Monitoring (ADM). NSM is comprised of an appliance that is connected to Ethernet ports of switches that are configured to forward mirrored data in one direction (outgoing only) to be displayed by a SIEM console – the SIEM for DeltaV Systems, which is based on the Intel Security SIEM solution. The combined environment allows DeltaV ACN data to be monitored to help identify possible issues (e.g. misuse) and cyber-threats.

The main goal with a SIEM and NSM solution is to determine the baseline for DeltaV system communications within a given site, and periodically compare it with the most current status. Any discrepancies should be evaluated and a remediation plan implemented. These are examples of such discrepancies:

- Unknown IP addresses communicating at the DeltaV ACN
- IP addresses mismatch between DeltaV ACN primary and secondary networks
- Out-of-the-ordinary data rates between specific embedded nodes
- Control communications between embedded nodes installed behind different firewalls

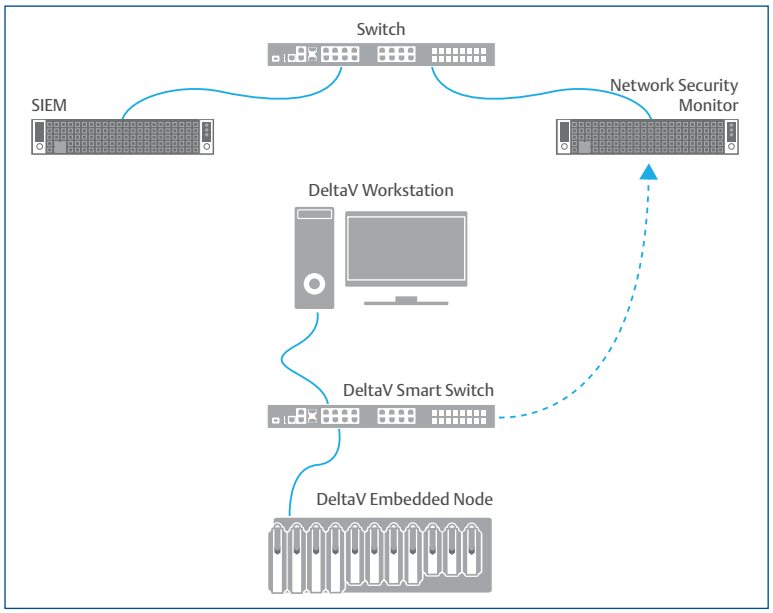


Figure 1 – Simplified network layout showing DeltaV Smart Switch connected to the NSM and SIEM.

Figure 1 illustrates a simple example where traffic shared between a DeltaV workstation and a DeltaV embedded node is also mirrored to a pre-configured DeltaV Smart Switch port, which is connected to the NSM appliance and finally displayed on the SIEM console.

Network Design and Specific Components

A key component for the NSM solution is a feature called 'port mirroring' that has been implemented on all DeltaV Smart Switches. This feature allows all DeltaV ACN traffic to be 'mirrored' from the configured ports (mirrored ports) to a probe port and directed to the NSM appliance.

Mirrored data are managed internally by each of the configured DeltaV Smart Switches and once enabled, the port mirroring feature does not interfere with the DeltaV communications.

Once configured, the probe port shall not be connected to any DeltaV workstations, servers, or embedded nodes. The probe port provides unidirectional data flow of mirrored packets and therefore would interfere with DeltaV communications if endpoints were connected to it. Disconnected probe ports on DeltaV Smart Switches can be easily identified as their probe port LED flashes to indicate the ports have been configured as probe ports (once connected the LEDs will flash normally indicating connectivity).

The port mirroring feature has been recently implemented and the DeltaV Smart Switches must be running v8.0.13 or higher in order to support this feature. Port mirroring is disabled by default, so it must be first enabled and properly configured to allow mirrored traffic to be directed to the probe port. DeltaV Smart Switches have a built-in wizard to simplify the port mirroring configuration, which prompts the user to enter the mirrored ports (individually or on a port range basis) and the probe port. This wizard is accessible through the switch's command line interface (CLI) through the serial port or remotely using telnet (Telnet is only available if the DeltaV Smart Switch is commissioned and if firewalls are not blocking connections to port 23). Figure 2 shows how the wizard to configure port mirroring works.

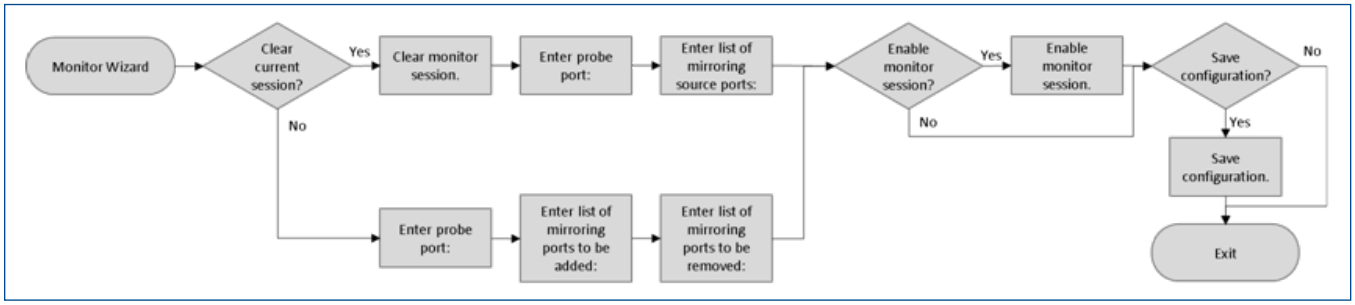


Figure 2 – Port mirroring configuration wizard flow chart

DeltaV Smart Switches can be configured to mirror data that is directed to the probe port in raw format, without any special handling or sampling available. If the maximum bandwidth of the probe port is reached, then mirrored data in excess will be dropped by the DeltaV Smart Switch. Normal communication packets between the DeltaV devices are not dropped.

The RM100-Family have switches with two gigabit uplink ports, and up to three groups of eight 100Mbps ports each. Each group of eight ports is managed by a dedicated switching processor and therefore all three processors are connected to each other through a gigabit inter-CPU bus. A combination of maxed-out ports where at least 10 ports of the 16 (two of the eight-port modules) all simultaneously running at 100Mbps each can eventually lead to mirrored packets being dropped by the switch. This limitation shall be taken into consideration when designing port mirroring for DeltaV systems. Figure 3 helps illustrate this bottleneck that is only applicable to the 24-port switches within the RM100-Family. However, it would be extremely rare, or in fact an indication of a network problem, to have ten ports on any switch all running simultaneously at 100Mbps in any DeltaV system on one switch.

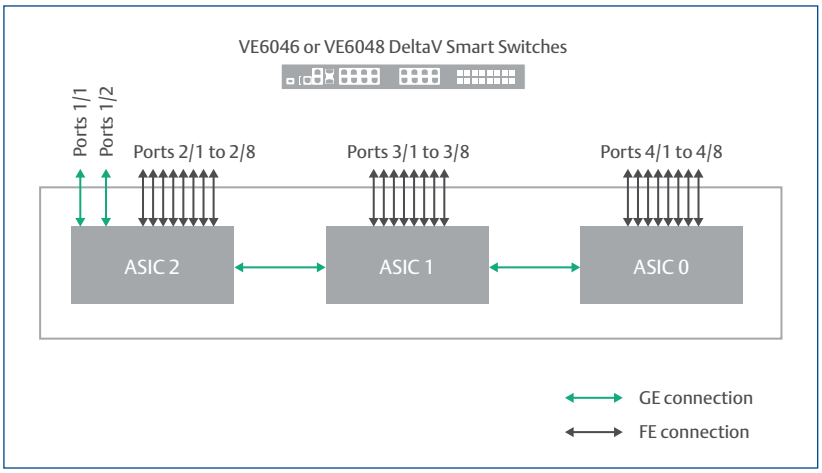


Figure 3 – Inter-processors communication diagram.

RM104 and RM1040 DeltaV Smart Switches are ideal for data concentration since all ports on these switches are gigabit capable and there is no bottleneck between inter-module processing communications that would affect mirrored data dropping in this case.

Security wise, probe ports provide unidirectional data flow only (from switch to the NSM) and therefore this port cannot be used for other communications. Depending on your risk assessment, per-port data-diode, or even a dedicated firewall could still be deployed.

The probe port does not receive any traffic and transmits only monitored traffic; therefore, it cannot be used for regular DeltaV connectivity. The port mirroring feature does not mirror all of the received traffic and this variation depends on the underlying switch processing capabilities of each of the DeltaV Smart Switches. Below you can find a table that better describes the exceptions to port mirroring on DeltaV Smart Switches:

Ingress Traffic Type	DeltaV Smart Switches (FP20s, MD20/30s, RM100s)	DeltaV Smart Switches (RM104 and RM1040)
Packets dropped by ingress storm control	Not mirrored	Not mirrored
Packets with CRC errors	Not mirrored	Not mirrored
Undersized frames	Not mirrored	Not mirrored
Oversized frames	Not mirrored	Not mirrored
Packets received for an unknown VLAN	Mirrored	Not mirrored
Packets received on a locked port with an unknown source MAC address	Mirrored	Not mirrored
Packets received on a disabled port	Not mirrored	Not mirrored
Local discards (source and destination MAC addresses are learned on the same port)	Mirrored	Not mirrored

Table 1 – Ingress mirroring overview.

Central Switch for Data Redirection

Up to this point, we are considering that each DeltaV Smart Switch will be configured to mirror local traffic– the first layer of switches that directly connect to the DeltaV end nodes and connect to each other through uplink ports between them, and then forward their individual traffic to the NSM through the configured probe port. DeltaV systems may be deployed with many DeltaV Smart Switches daisy-chained together or in a star topology, and therefore the NSM would be required to have multiple network connections available – one connection is required for each switch that has a probe port.

Daisy-chained switches should NOT have their uplink ports mirrored due to the duplication of traffic – so EACH switch needs to have its own probe port regardless of the network topology. The NSM is supplied with only four available network cards, but there can be many more probe ports from switches, and it may not be convenient or cost effective to add more NSM security appliances just to extend the number of ports for individual switch probe ports connectivity.

With that said, some of the DeltaV Smart Switches (RM104 and RM1040 only) have a special menu option within the port mirroring configuration tree that allows them to be converted to a **Central Switch**. When converted, these central switches will redirect ingress data (that comes from other Smart Switch probe ports only), to the configured probe port on the Central Switch. Probe ports (from the first level end node switches) would normally be directly connected to the NSM appliance's NIC cards (up to four switches with probe ports to the four NIC cards of the NSM appliance), or in some cases be connected to an adjacent central switch to extend the number of switches connected to same NSM network port. Figure 4 illustrates these two supported use cases when the DeltaV Smart Switches are configured as central switches.

Note that without consideration of a bandwidth limitation of the NSM appliance itself, when the Central Switches are daisy-chained as in Figure 4, the combined traffic between the central switches cannot exceed 1Gbps – this is because each port on the central switches are 1Gbps maximum. However, with consideration of the limitations of the NSM appliance itself, the combined traffic of all switches in the network cannot exceed 500Mbps due to the capacity of the NSM appliance (a higher-end ADM appliance is available that supports up to 1Gbps total capacity).

In summary, if the 500Mbps capacity of a NSM is reached, another NSM appliance can be added and networked with another switch to connect to the SIEM appliance, or a higher end NSM appliance can be used. If the capacity of a probe port on an individual switch is ever exceeded (very rare), the load can be distributed across switches with cable changes to balance the loading. Emerson can help validate the network loading and NSM loading upon request.

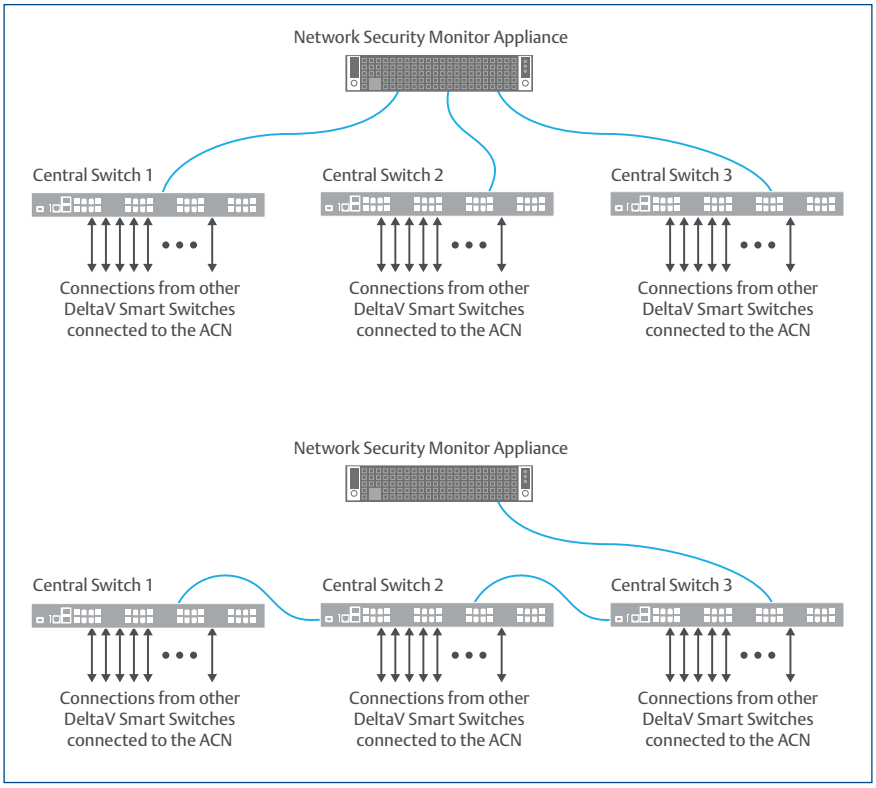


Figure 4 – Central switch use cases.

DeltaV Smart Switches configured to be Central Switches shall not be used as conventional DeltaV Smart Switches and instead be only used to simplify the port mirroring network connections. The DeltaV Smart Switches can always be set to their default configuration state in case a central switch is to be re-utilized within the DeltaV ACN for DeltaV data traffic switching purposes. When configured to be a central switch, the DeltaV Smart Switches are no longer managed by the DeltaV Network Device Command Center.

On the current implementation of port mirroring for DeltaV Smart Switches, the central switches can only be configured with a single probe port, hence load sharing would need to be managed by multiple central switches, or by adding multiple NSM appliances, whichever is more suitable for the given mirroring application.

Example Network Architecture

The following example network architecture (Figure 5) details how the connections work between DeltaV Smart Switches, the Central Switch, and the NSM. In this specific example, DeltaV ACN traffic from both sides of the Firewall-IPDs are mirrored to the Central Switch, which then concentrates everything on a single network connection to the NSM.

This example is not including mirroring of the L2.5 network (which is not represented in the diagram), nor the connection between the NSM and the SIEM. The SIEM may be installed at the same network level as the NSM, but the recommendation is to connect it to the DMZ network right after the Emerson Smart Firewall (perimeter delimiter).

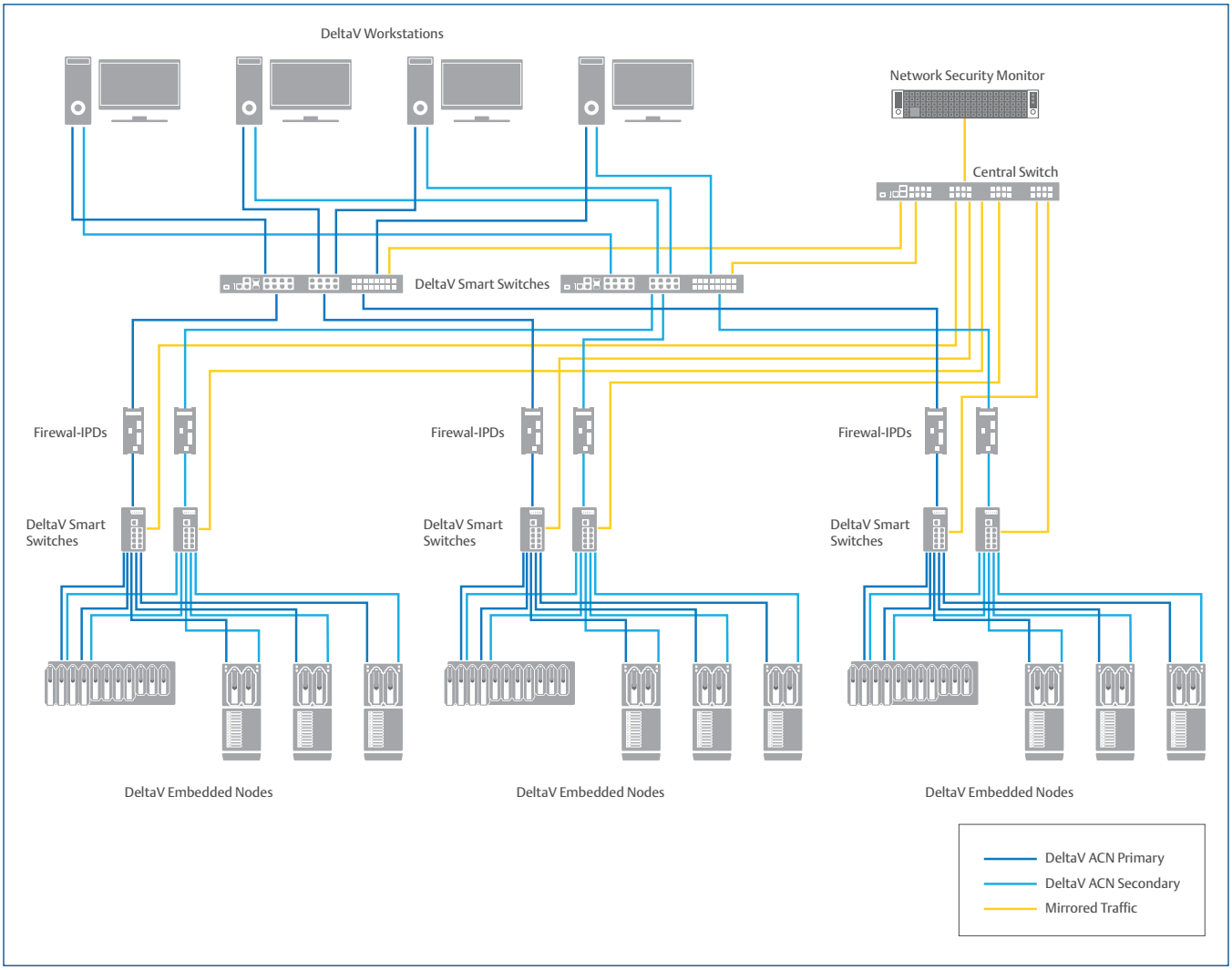


Figure 5 – Example architecture illustrating port mirroring.

Compatibility Table

Table 2 highlights the DeltaV Smart Switches and the support for port mirroring. Please refer to the DeltaV Smart Switches product data sheet for additional information about each of the switch families, and make sure to follow the details below prior to implementing port mirroring on a DeltaV ACN.

DeltaV Smart Switch family	Reference VE number	Firmware version	DeltaV version	Port mirroring functionality
FP20-Series	VE6041	8.0.13	v11.3.1 and higher	Port mirroring only
MD20-Series	VE6042	8.0.13		Port mirroring only
MD30-Series	VE6043	8.0.13		Port mirroring only
RM100-Series	VE6046 / VE6047 / VE6048	8.0.13		Port mirroring only
RM104	VE6053	8.0.13		Port mirroring and Central Switch
RM1040	VE6054	8.0.13		Port mirroring and Central Switch

Table 2 – DeltaV Smart Switches and port mirroring compatibility.

Bandwidth Allocation and Final Considerations

If a fully mirrored switch where all ports are simultaneously running at 100Mbps (200Mbps full duplex), this would generate a total combined bit rate of 2.4Gbps, much more than a 100Mbps probe port could handle, or even a 1Gbps probe port.

In very few situations and totally dependent on a specific use case (e.g. Batch Operations), DeltaV systems would have 100Mbps communication load on any given individual switch port, and it would be extremely rare that there would be 10 devices on a single switch simultaneously communicating at 100Mbps, which then would oversubscribe a 1Gbps probe port. Typically, a DeltaV switch port runs at only a few Mbps, never close to 100Mbps in addition to doing this simultaneously with other ports at this much of a network load.

DeltaV Smart Switches that do not contain any gigabit uplink ports (i.e., the FP20-Series switches and MD20-Series switches), have only 100Mbps ports available as a probe port, therefore, if one port is used for the probe port, there are seven ports left that could be mirrored on an FP20 switch.

In order not to exceed 100Mbps for the probe port on the FP20 switch, the average for each of the seven ports could not exceed 14Mbps simultaneously (7 ports x 14Mbps = 98Mbps). DeltaV end devices do not typically communicate at more than a few megabits per second each. Additionally, there is not a duplication of traffic between end devices and uplink traffic since port mirroring does not include uplink ports monitoring.

The entire port mirroring function is based on monitoring only receiving (Rx) traffic of the end nodes, and therefore uplink traffic and transmitting (Tx) traffic is not duplicated – keeping traffic going to the probe port minimal and efficient.

While Emerson has made every effort to measure/confirm worse case bandwidth usage on various large DeltaV systems, in regards to validating any possible oversubscription of a probe port so that specific cases could be flagged, there is always a chance that due to the infinite number of possible network topologies, a probe port could occasionally be oversubscribed. In these cases, bandwidth measurements using a network sniffer could be taken at the probe port of each switch, and through cabling changes, and a balancing of bandwidth between switches could be achieved and lowered on the extreme cases. Typically, this is not a concern for most DeltaV systems.

Please contact your local Emerson sales office for additional information about Performance Services to implement port mirroring on your existing DeltaV Smart Switches, and to design a solution based on NSM and SIEM.

DeltaV Smart Switches Port Mirroring

October 2016

The port mirroring feature for DeltaV Smart Switches and the NSM for DeltaV systems are expected to provide information that support the defense-in-depth strategy and represent an additional layer of protection to your DeltaV system. These products and features represent only one portion of an overall DeltaV security solution. Using port mirroring and/or Network Security Monitor for DeltaV systems does not guarantee that your DeltaV system is secure from cyber-attacks, intrusion attempts, or other undesired actions. Users are solely and completely responsible for their control system security, practices, and processes, and for the proper configuration and use of the port mirroring feature or the Network Security Monitor for DeltaV systems.

Emerson Process Management
North America, Latin America:
+1 800 833 8314 or
+1 512 832 3774

Asia Pacific:
65 6777 8211

Europe, Middle East:
+41 41 768 6111

www.emerson.com/deltav

DELTAV™

EMERSON™