APPLICATION NOTE

APCON
Solutions for Networks

TITAN EnterPoint™ Software:

Manage Network Monitoring from a Single, Centralized Point

INTRODUCTION

As today's Fortune 500 production networks grow in size and scope, so does the demand for achieving total network visibility. One hundred percent visibility is essential to realizing the rigorous "five-nines" uptime standard, and failing to monitor all points on the network can lead to costly outages or increase the time to resolution – resulting in significant revenue losses as well as customer dissatisfaction.

In response, enterprises are investing in farms of monitoring and analysis tools such as protocol analyzers, sniffers, probes, archiving systems and intrusion detection systems. To most enterprises, these tools are not an option. Rather, they are a requirement to maintaining a healthy network and meeting security and compliance regulations. However, ranging in cost from $25,000 to over $150,000 each, they also represent a significant capital investment.

While it is cost prohibitive to put these devices at every network monitoring point, it is equally unwise to have them sit idle until needed. The ideal solution is to deploy devices in a way that allows them to be shared to maximize coverage and device utilization – where they can be roved instantly and electronically to a required point on the network at a moment's notice. With the adoption of matrix switching technology, efficient device sharing is now becoming more common. However, effectively managing this infrastructure from a single, centralized point has remained a challenge.

The natural answer for this dilemma is to have a company already dedicated to network connectivity deliver a trustworthy and tested solution. And now one company has. APCON's intuitive, web-accessible EnterPoint software offers IT departments a single, centralized point of control from which to administer an efficient and comprehensive network monitoring program.

> **"EnterPoint provides a comprehensive, web-based package with all the functionality needed for Fortune 500 network monitoring programs – at a cost that acknowledges the financial constraints every enterprise is dealing with today."**
>
> **— Richard Rauch**
> **President & CEO**
> **APCON, Inc.**

DEVICE CONNECTIVITY WITH MATRIX SWITCHING

The matrix switch has become a key ingredient for today's efficient monitoring device tool farms. These switches scale from 32 to 288 ports each, and support any combination of 1Mb to 10Gb rates – both copper and fiber – while also supporting media conversion, distance extension and signal regeneration seamlessly all at the same time. Premium switches also support various protocols including, but not limited to, T1/E1/J1, DS3/E3/STS-1, SONET OC-3/12/48, SDH STM-1/4/16, 10GigE, Fibre Channel 1/2/4/8/10 Gig, FDDI, 10/100/1000 Ethernet, SDI/HDI video, and more. Also available are solutions that scale into thousands of ports and are manageable through easy-to-use GUI software.

To understand the full impact a matrix switching solution can have, consider the enterprise customer that has between two and 20 purpose-built data centers located around the globe. Each of these locations likely requires monitoring services that include deep packet inspection, traffic analysis, network break-fix, equipment upgrades and more. Matrix switch technology makes it possible to reduce monitoring equipment investments by an average of 50 percent per data center while still guaranteeing that customers can achieve 100 percent network visibility.

In one example, a client has invested in five analysis tools per data center and has five locations worldwide. At an average cost of $50,000 per tool, as well as a 15% yearly service contract on each, the total cost per location is $250,000 in equipment and $37,500 in annual support fees. Multiplying that by five equates to $1,250,000 in tools and $187,000 in annual support fees. *(fig. 1a)*

With the use of matrix switch technology, the tools could be reduced to two per location for a total cost of $500,000 – resulting in a savings of $750,000 on tools and $112,000 in on-going annual support services. These savings quickly offset the cost of the matrix switches as well as the on-going annual support costs. *(fig. 1b)*

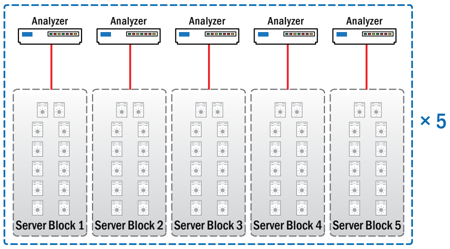


Figure 1a
$1,250,000 Equipment costs
$187,000 Maintenance costs

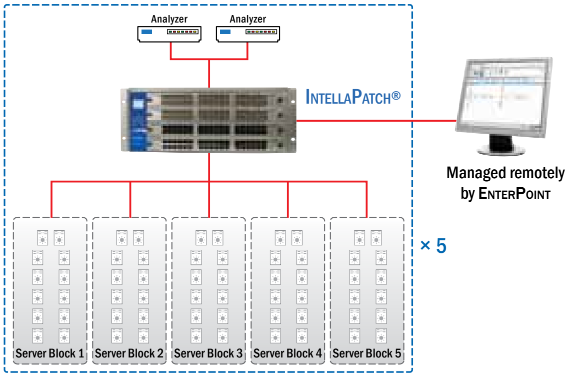


Figure 1b
$500,000 Equipment costs
$75,000 Maintenance costs

NETWORK MONITORING MADE EFFICIENT

While matrix switch technology has emerged as a new standard for sharing monitoring devices in large enterprise networks, a centralized solution for managing end-to-end connectivity through the switch matrix was absent – until TITAN EnterPoint. This intuitive application, developed by the pioneer of matrix switching technology, offers four key functionalities required for effective network monitoring programs:

- Scheduling and managing monitoring sessions,
- Setting and managing third-party device configurations,
- Managing device use department-wide,
- Reporting on device utilization, inventory and activity.

The first, most basic functionality is the need to connect a SPAN, Tap or mirror port to analysis or security devices for the purpose of diagnosing network issues. A matrix switch deployment makes this connectivity achievable regardless of device location, and now EnterPoint offers one simple screen from which to make it happen.

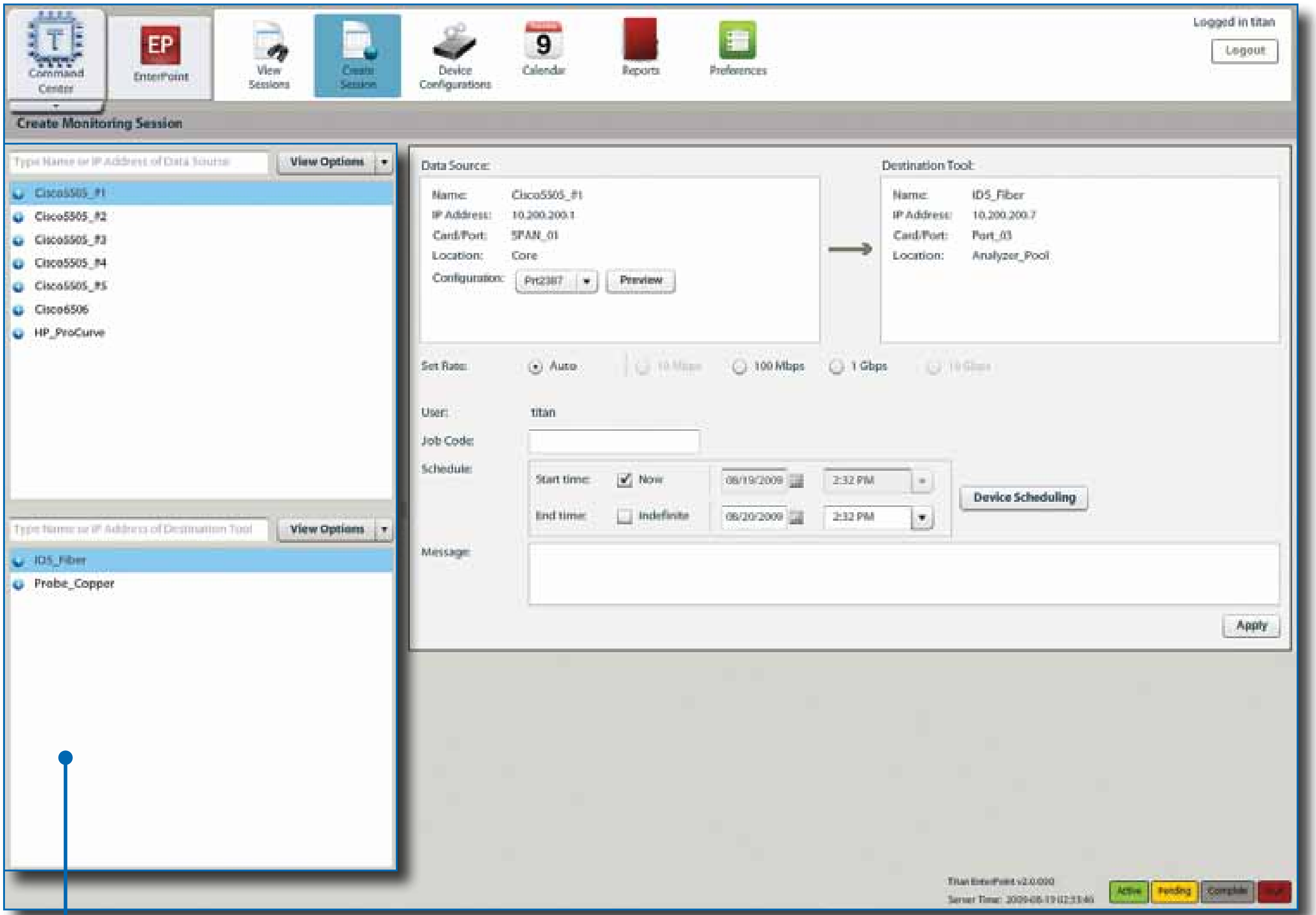
The Create Session screen displays a list of Data Sources, as well as a list of Destination Tools. *(fig. 2)* To make the process most efficient, EnterPoint only displays the names of sources and destinations that are available and to which the user has access. When beginning a monitoring session, the user selects a source and a destination, applies a source configuration if applicable, then chooses a rate, sets a schedule, adds a job code or message if desired, and clicks the Connect button. Six simple steps to setting a monitoring session.

From there, the user can click to the View Sessions screen where he is able to view all monitoring sessions scheduled or in progress. *(fig. 3)* This “dashboard” offers a snapshot that includes the source and destination of each monitoring session, as well as the device location, start time and scheduled end time, ID code, user name, link status and optional user message.

The View Sessions screen offers several viewing options, such as the ability view or hide many of the columns on the dashboard. There is also the ability to hide other users’ sessions and also any sessions that are set as reservations. Users can view additional connection detail on a specific monitoring session with a single mouse click, which expands the view to show the path through the matrix. *(fig. 4)* Detailed device information is also available by right-clicking a particular source or destination. Users can then disconnect a session when the issue is resolved with a simple mouse click.

CREATE SESSIONS

- Once a source is selected, the list of tools automatically narrows – showing only available devices
- Preview and apply saved configurations to sources at the time of connection
- Add an ID code for job ticketing purposes
- Create connections that run indefinitely or set a specific time frame – beginning now or later



Create Monitoring Session

Type Name or IP Address of Data Source

- Cisco5505_#1
- Cisco5505_#2
- Cisco5505_#3
- Cisco5505_#4
- Cisco5505_#5
- Cisco6506
- HP_ProCurve

Type Name or IP Address of Destination Tool

- IDS_Fiber
- Probe_Copper

Data Source:

Name: Cisco5505_#1
IP Address: 10.200.200.1
Card/Port: SPAN_01
Location: Core
Configuration: Prt2387

Destination Tool:

Name: IDS_Fiber
IP Address: 10.200.200.7
Card/Port: Port_03
Location: Analyzer_Pool

Set Rate: ● Auto ○ 10 Mbps ○ 100 Mbps ○ 1 Gbps ○ 10 Gbps

User: titan

Job Code:

Schedule:
Start time: ☑ Now 08/19/2009 2:32 PM
End time: □ Indefinite 08/20/2009 2:32 PM

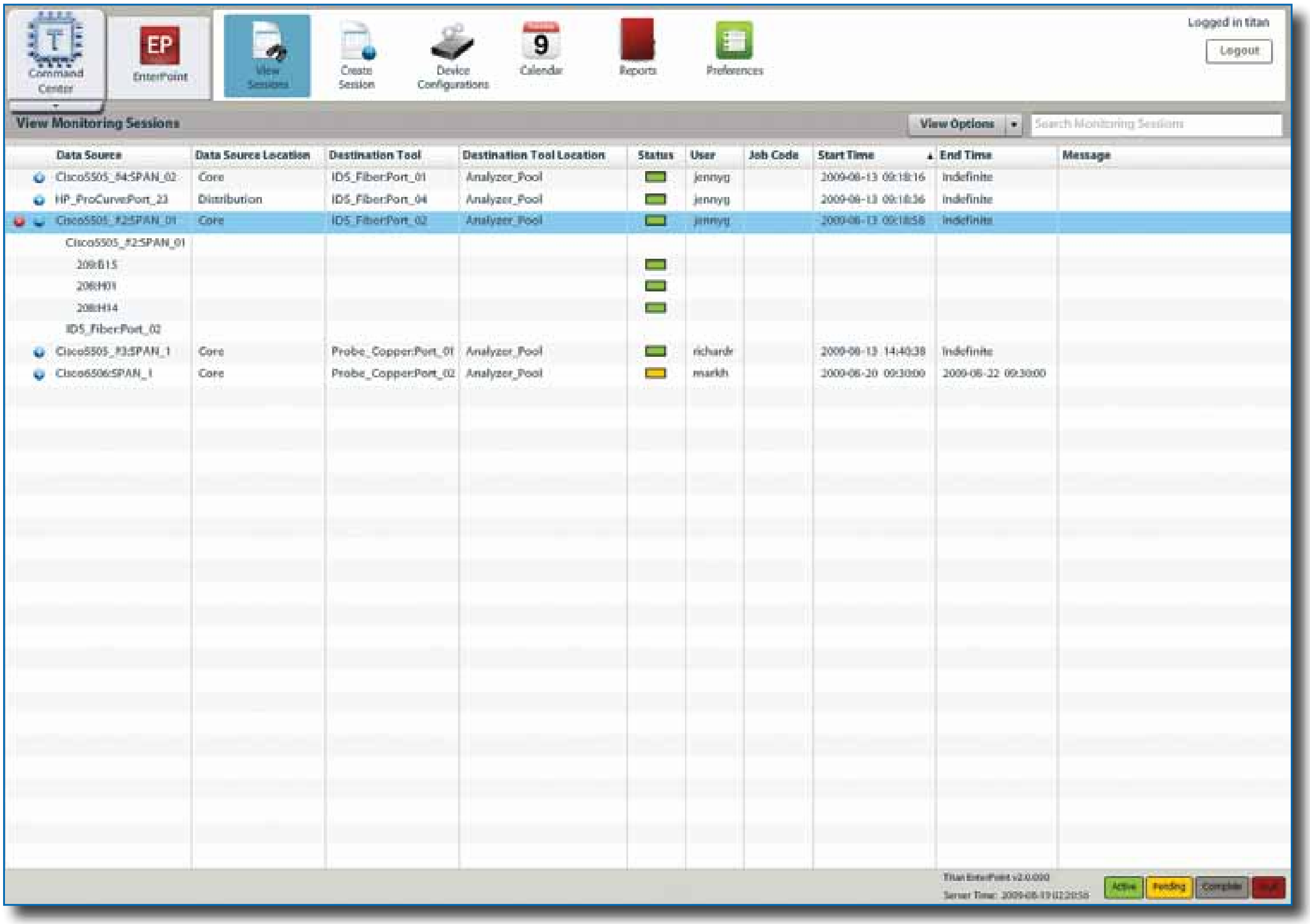
Message:

Titan EnterPoint v2.0.030
Server Time: 2009-08-19 02:33:46

Figure 2

VIEW SESSIONS

- Clicking the “plus” button reveals the path through the matrix
- A status light indicates that connections are live or pending, or in fault
- Disconnect finished monitoring sessions with a single click
- View options enable users to show or hide specific information

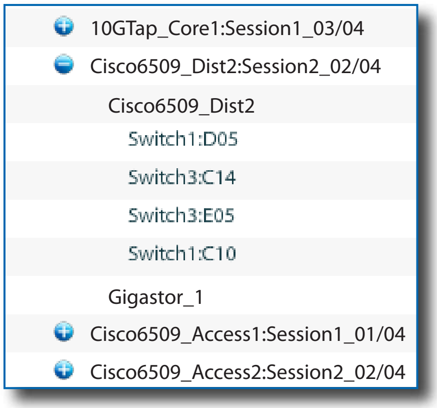


View Monitoring Sessions

Data Source	Data Source Location	Destination Tool	Destination Tool Location	Status	User	Job Code	Start Time	End Time	Message
Cisco5505_#4:SPAN_02	Core	IDS_FiberPort_01	Analyzer_Pool	🟩	jennyg		2009-08-13 09:18:16	Indefinite	
HP_ProCurvePort_23	Distribution	IDS_FiberPort_04	Analyzer_Pool	🟩	jennyg		2009-08-13 09:18:36	Indefinite	
Cisco5505_#2:SPAN_01	Core	IDS_FiberPort_02	Analyzer_Pool	🟩	jennyg		2009-08-13 09:18:58	Indefinite	
Cisco5505_#2:SPAN_01									
208:B15				🟩					
208:H01				🟩					
208:H14				🟩					
IDS_FiberPort_02									
Cisco5505_#3:SPAN_1	Core	Probe_CopperPort_01	Analyzer_Pool	🟩	richardr		2009-08-13 14:40:38	Indefinite	
Cisco6506:SPAN_1	Core	Probe_CopperPort_02	Analyzer_Pool	🟨	markh		2009-08-20 09:30:00	2009-08-22 09:30:00	

Titan EnterPoint v2.0.030
Server Time: 2009-08-19 10:20:58

Figure 3



⊕ 10GTap_Core1:Session1_03/04
⊖ Cisco6509_Dist2:Session2_02/04
Cisco6509_Dist2
Switch1:D05
Switch3:C14
Switch3:E05
Switch1:C10
Gigastor_1
⊕ Cisco6509_Access1:Session1_01/04
⊕ Cisco6509_Access2:Session2_02/04

Figure 4

CONFIGURE THIRD-PARTY DEVICES

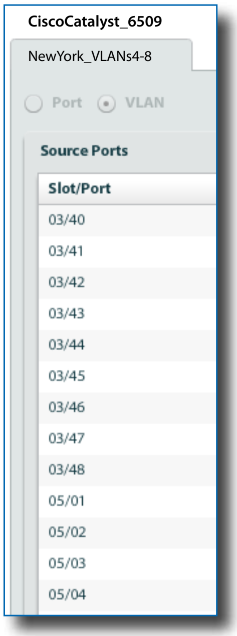
An essential feature of any network monitoring program is the ability to manipulate the flow of information coming from any SPAN or monitoring point. For a user with permission to edit Data Source configurations, EnterPoint makes it possible for him to build and store an unlimited number of configurations – applying the chosen configuration at the time the monitoring session begins.

For example, if the user has access to a Cisco Catalyst 6509 switch, he would be able to create a configuration called “NewYork_VLANs4-8” that funnels the desired VLAN or port-based traffic from the switch out the SPAN port. *(fig. 5)* When connecting the desired SPAN port on that Cisco switch to a Niksun monitoring applicance on the Create Session screen, he would be able to apply the saved “NewYork_VLANs4-8” configuration to the monitoring session when it goes live – whether that is immediately or at a time in the future. *(fig. 6)*

When a monitoring session is complete, a user can manually disconnect the session or EnterPoint disconnects it automatically at the end of the scheduled timeframe. Upon disconnection, EnterPoint resets any Data Source with a saved “default” back to the original configuration.

THIRD-PARTY DEVICE CONFIGURATION

- Build and store device-specific configurations
- Apply at the time a device is required for a monitoring session
- Automatically reset a device to its programmed default configuration once a monitoring session is complete



CiscoCatalyst_6509

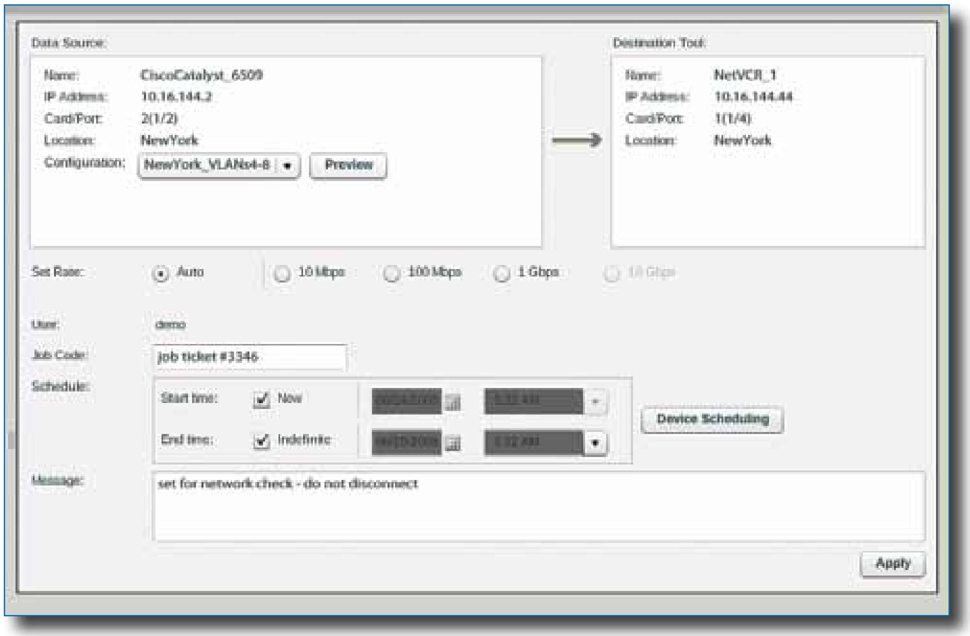
NewYork_VLANs4-8

○ Port ● VLAN

Source Ports

Slot/Port
03/40
03/41
03/42
03/43
03/44
03/45
03/46
03/47
03/48
05/01
05/02
05/03
05/04

Figure 5



Data Source:

Name: CiscoCatalyst_6509
IP Address: 10.16.144.2
Card/Port: 2(1/2)
Location: NewYork
Configuration: NewYork_VLANs4-8

Destination Tool:

Name: NetVCR_1
IP Address: 10.16.144.44
Card/Port: 1(1/4)
Location: NewYork

Set Rate: ● Auto ○ 10 Mbps ○ 100 Mbps ○ 1 Gbps ○ 10 Gbps

User: demo

Job Code: job ticket #3346

Schedule:
Start time: ☑ Now
End time: ☑ Indefinite

Message: set for network check - do not disconnect

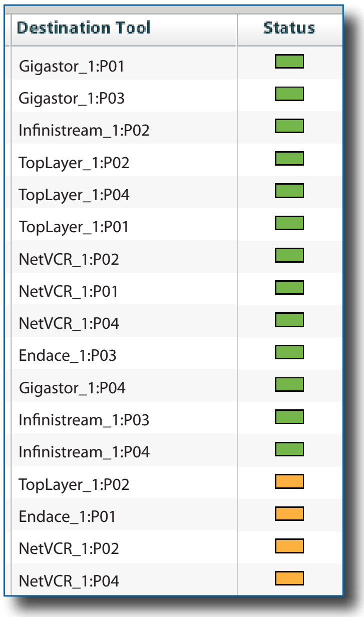
Figure 6

RESERVING DEVICES & RESOLVING SCHEDULE CONFLICTS

Knowing that many users will have immediate network issues to diagnose, EnterPoint can – by default – create monitoring sessions that begin immediately and remain up until the user manually disconnects them. In cases where a future connection is desired, EnterPoint offers the ability to create a reservation.

To book a reservation, the user begins with the same simple steps of choosing a Data Source and Destination Tool, and then applying a configuration to that source if desired. The user then inputs the future start time and desired end time with the aid of the calendar, and clicks the Connect button.

If the devices are already in use during the desired timeframe, EnterPoint will display a scheduling conflict resolution screen – showing the user which of the devices is already in use and allowing him to choose a different timeframe for his monitoring session. Users can ask EnterPoint to display the next available time or choose a different time/date themselves. Once the conflict is resolved, EnterPoint creates a reservation for that monitoring session. When the user returns to the View Sessions screen, he sees this connection is identified with a yellow status light to indicate that it is “pending.” *(fig. 7)*



Destination Tool	Status
Gigastor_1:P01	🟩
Gigastor_1:P03	🟩
Infinistream_1:P02	🟩
TopLayer_1:P02	🟩
TopLayer_1:P04	🟩
TopLayer_1:P01	🟩
NetVCR_1:P02	🟩
NetVCR_1:P01	🟩
NetVCR_1:P04	🟩
Endace_1:P03	🟩
Gigastor_1:P04	🟩
Infinistream_1:P03	🟩
Infinistream_1:P04	🟩
TopLayer_1:P02	🟨
Endace_1:P01	🟨
NetVCR_1:P02	🟨
NetVCR_1:P04	🟨

Figure 7

Going to the Calendar screen, the user can view the same information. Both active and pending monitoring sessions are displayed in Outlook-like style on a per device basis. Clicking on a monitoring session, a pane on the right side of the window displays the Data Source and Destination Tool, as well as the rate, user, ID code and message information specific to that monitoring session. Once a monitoring session is highlighted in either the Data Source or Destination Tool window, EnterPoint automatically scrolls to the corresponding device associated with that monitoring session. *(fig. 8)*

The Calendar screen offers several convenient viewing options, including daily, weekly and monthly views. Schedules can be viewed by device or specifically by port. Additionally, for users with permission, adjusting monitoring sessions is as simple as editing the information in the pane on the right side of the screen and saving the changes.

DEVICE CALENDAR

- ○ Create “reservations” for monitoring sessions to begin at a scheduled time
- ○ View device usage on an Outlook-style calendar
- ○ Review, adjust or disconnect monitoring sessions

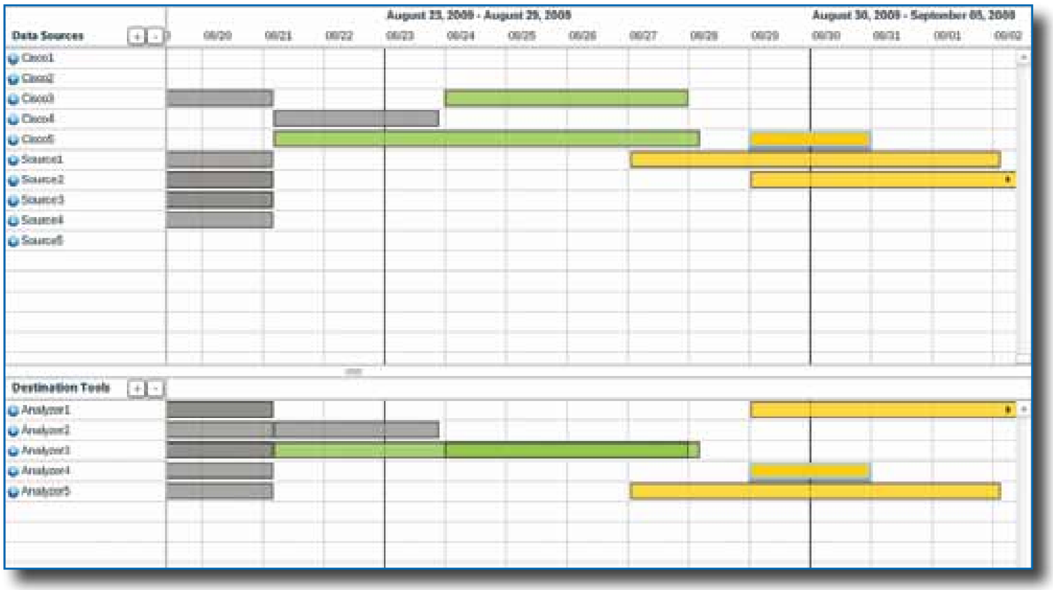


Figure 8

BUILT-IN REPORTS TRACK USAGE & INVENTORY

Many enterprises, large ones especially, have had no easy means of determining – at any point in time – how many monitoring devices they have, and where and how they are being used. This "blind spot" can lead to uninformed decisions with potentially significant financial ramifications.

EnterPoint introduces reporting capabilities that make it possible to review the use of every device in the EnterPoint inventory and understand where, when and by whom it is being utilized. With such information, network managers can review:

- The number and duration of all monitoring sessions from a particular timeframe,
- The utilization percentage of all or specific devices,
- The quantity and location all devices in inventory.

This is key to understanding whether there are too few tools of a particular kind, or if tools are available and can be better utilized elsewhere. The organization will benefit from better decision-making regarding purchases of additional tools – a critical advantage considering the cost of such devices. Further, it will know if analytical sessions are historically high for certain areas of any network, or whether potential performance issues are brewing, which can be remedied before a failure occurs. *(fig. 9)*

EnterPoint offers a high level of granularity with its reports. For example, the Device Utilization report enables the user to select one or more devices from a list, and then filter by such parameters as location, port type, user and percentage of use – allowing the user to get the specific level of reporting detail that is most useful.

After previewing the report, users have the option of saving the search as a custom report within EnterPoint. Users can also export the results for use with another analysis tool or for inclusion in other reports. Export formats include PDF, CSV, Excel, Word and PowerPoint.

REPORTS

- ○ Choose from an array of pre-built Activity and Resource reports, including usage by device and inventory reports
- ○ Create and save custom reports
- ○ Export reports in a variety of file formats, including PDF, XML, CSV

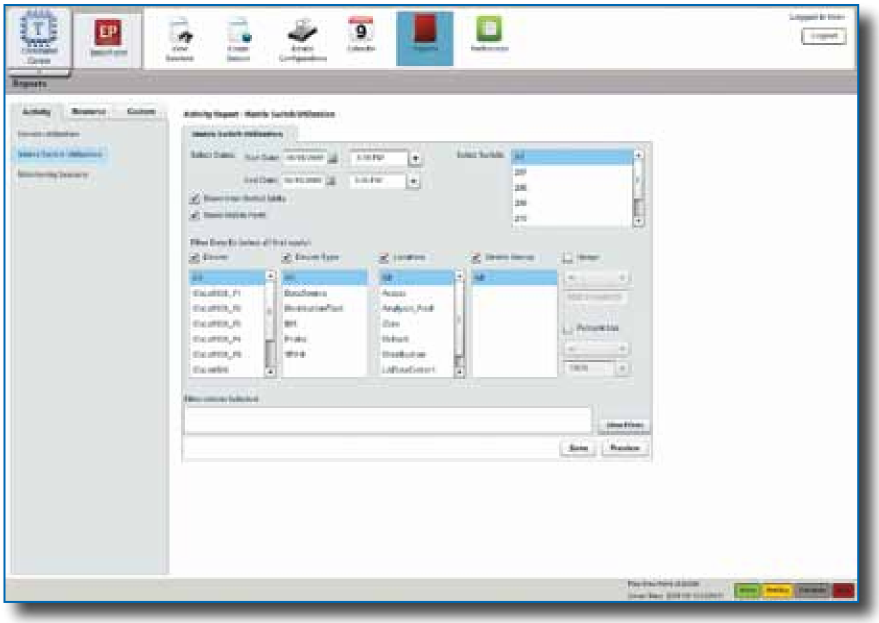


Figure 9

ENTERPRISE-CLASS SYSTEM FUNCTIONALITY

By design, EnterPoint has been developed as a web-based interface – assuring better availability to end-users in the enterprise and eliminating security concerns about installing third-party software. To access EnterPoint, a user simply opens his standard web browser and inputs the correct IP address. After logging in, the user arrives at the page last viewed during the previous visit – generally the View Sessions or Create Sessions screen.

Knowing that EnterPoint must integrate into an environment with a multitude of other tools and systems, APCON added several information fields to make the user experience more seamless:

- **Job ticket:** Nearly all enterprise networks use an electronic job ticketing system for tracking network issues, and EnterPoint includes a field referencing the job ticket or job code on the Create Session screen. That information also shows prominently on the View Sessions screen.
- **Location:** Many enterprise networks have devices in more than one physical location, and EnterPoint displays this information with the monitoring session detail.
- **Message:** To alert other system users to the purpose for individual monitoring sessions, EnterPoint includes an optional message field for users to fill out.

Another element distinguishing EnterPoint is the ease of set up and configuration. The program is designed to make set-up as swift and intuitive as possible – and the system can generally be set up in a matter of hours, not days. The Global Settings module steps the user through a series of screens that configure the matrix switches, source and destination devices, users and permissions, and server settings.

As an enterprise-class platform, EnterPoint boasts a robust set of security features designed for maintaining maximum system uptime. Those include:

- Support for centralized authentication mechanisms such as RADIUS and TACACS+.
- Comprehensive logging of all configuration change and security events
- User-settable security levels that allow an administrator to enable or deny access to specific features on a per user or per user-group basis. For example, an admin can restrict access for users to edit or delete monitoring sessions, edit device configurations and make edits to the device calendar, just to name a few.

> **"For the first time, management can see which network devices are being used at maximum capacity. This leads to fact-based decision making about whether additional capital investments are justified."**

In any enterprise today, network uptime is paramount, which is why IntellaPatch Series 3000 switches offer redundant controllers with automatic failover. The active controller manages the user interfaces to the switch while the standby unit monitors activity on the active device. Should the active controller fail, the standby unit will power it off and become the active device.

Synchronization is also essential to uninterrupted network operation. This is made possible when the active controller always holds the current configuration state of the switch-where the state includes information on patches and rates, presets, user management, and other global switch settings Whenever a configuration change is made to a switch, the changed configuration is copied to the standby controller. This enables it to manage all aspects of the switch in the event of a failure and subsequent fail-over from the active controller.

As an added measure of protection, IntellaPatch Series 3000 controllers also feature dual LAN ports. This provides network redundancy, meaning that each LAN port is assigned with an address from a separate segment of the network. If a fault is detected in either the LAN port or that LAN port's segment of the network, the secondary LAN port will automatically assume connection to the network.

Lastly, EnterPoint offers system scalability. That is, the ability to support a large number of simultaneous users in an environment that has large number of sources and tools, and an environment with a complex switch matrix. EnterPoint can scale to manage your environment and expand as the user base or equipment base grows.

CONCLUSION

EnterPoint addresses the need for an enterprise to have ready access to all of its analysis tools on a one-to-one basis. It speeds and simplifies device connections, provides a clear picture of monitoring sessions, allows sessions to be scheduled to accommodate tool usage and availability, and provides a comprehensive reporting capability that significantly enhances decision-making surrounding the enterprise's continuing investment in and deployment of high-cost monitoring tools.