MIIM

DELIVERING BEYOND

Enhancing Security through Advanced Physical Layer Management

Christophe HINET, RCDD

Advanced Solutions Director

MOLEX Premise Networks and its logos are trademarks of the MOLEX Corporation. Other manufacturer's trademarks, logos and products mentioned are acknowledged as their property. The information in this document is subject to change without notice and should not be construed as a commitment by MOLEX. MOLEX Premise Networks assumes no responsibility for any errors that may appear in this document.

Some conditions may apply for some of the MIIM functionalities to operate properly. Please contact your Molex sales representative.

molex®

one company › a world of innovation

© 2012 Molex Incorporated. All Rights Reserved.

I REALLY NEED TO TALK TO YOU ABOUT SECURITY ON LAYER 1 TODAY !

molex

one company › a world of innovation

© 2012 Molex Incorporated. All Rights Reserved.

I REALLY NEED TO TALK TO YOU ABOUT SECURITY ON LAYER 1 TODAY !

PAGE 32

OF YOUR

CONFERENCE BOOK…

Christophe HINET, RCDD

Advanced Solutions Director

TE Connectivity / AMP CONNECT

molex

one company › a world of innovation

© 2012 Molex Incorporated. All Rights Reserved.

I REALLY NEED TO TALK TO YOU ABOUT SECURITY ON LAYER 1 TODAY !

Christophe HINET, RCDD

Advanced Solutions Director

MOLEX

~~Christophe HINET, RCDD~~

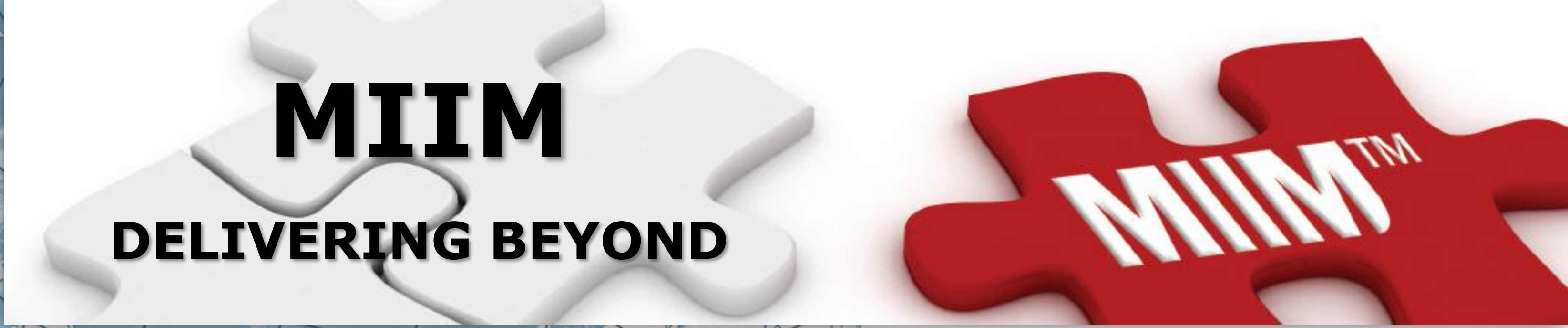
~~Advanced Solutions Director~~

~~TE Connectivity / AMP CONNECT~~

molex

one company › a world of innovation

© 2012 Molex Incorporated. All Rights Reserved.



MIIM

DELIVERING BEYOND

Enhancing Security through Advanced Physical Layer Management

Christophe HINET, RCDD

Advanced Solutions Director

MOLEX Premise Networks and its logos are trademarks of the MOLEX Corporation. Other manufacturer's trademarks, logos and products mentioned are acknowledged as their property. The information in this document is subject to change without notice and should not be construed as a commitment by MOLEX. MOLEX Premise Networks assumes no responsibility for any errors that may appear in this document.

Some conditions may apply for some of the MIIM functionalities to operate properly. Please contact your Molex sales representative.

molex®
one company › a world of innovation

© 2012 Molex Incorporated. All Rights Reserved.

Enhancing Security through APLM solutions

- **Traditional focus of security within the IT department :**
  - authentication of users
  - monitoring traffic usage
  - backing up of data – protection of “virtual” assets and “virtual” connectivity

- **Protection of physical assets is traditionally confined to the security department :**
  - Cabinet and Comms Room Security
  - ID badges
  - Security guards
  - Cameras

- **What’s missing : coordination with IT tools to track the physical connection of end devices in real time**
  - Protection from theft of equipment – and the data on them – through continuous monitoring of the physical connection of end-devices to the network
  - Protection from inadvertent security breaches by well-meaning employees

© 2012 Molex Incorporated. All Rights Reserved.

Enhancing Security through APLM solutions

- **The potential loss of secure data has repercussions on any business:**
- **Think…**
  - Confidential patient records
  - Secret government files
  - Credit card information or proprietary technology blueprints

- **Can this be considered as a drop in the Ocean ?**
- **No… This may have severe consequences**

- **Unfortunately, it is not unusual for such delays in the reporting of missing assets…**

© 2012 Molex Incorporated. All Rights Reserved.

Enhancing Security through APLM solutions

- **Wesley College, Australia:**
  - $120,000 in expensive laptops and other computer equipment stolen

- **San Jose Medical Group:**
  - 2 stolen computers, with the loss of patient databases with social security numbers and medical information - subject to legal action from clients

- **Home Office Minister's PC stolen from her office in Manchester UK:**
  - Containing restricted information on defence and housing markets

- **The Centre for Retail Research said the UK was one of the worst countries in Europe for stealing by employees, costing employers £1.5bn last year.**

© 2012 Molex Incorporated. All Rights Reserved.

Enhancing Security through APLM solutions

- According to a report from the Computer Security Institute/FBI Computer Crime and Security Survey, the theft of a single laptop results in an average loss of $89,000 – the value of the hardware is just a fraction of the total loss.

- A survey by Kensington in 2001 put the average number of laptops stolen from medium and large sized companies at 11.65 per year.

- Would it not be better to know where your assets are and be aware when they are moved?

© 2012 Molex Incorporated. All Rights Reserved.

A Story…

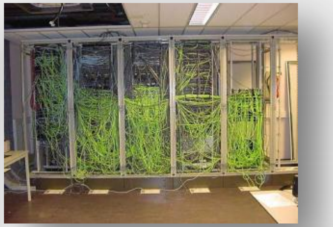
- The scenario: a college campus with 5 buildings, and a student whose lap top is infected with a Denial of Service virus
- Student goes on line, the switch recognizes the threat, and shuts down the channel. Crisis avoided, right?
- IT tries to locate the student by going to the TR to see which horizontal the particular switch port is connected to.   Then check records to see what room the outlet is located in, only to find no one there, because…
- In the mean time the student figures the network must be down, and goes to the next floor to connect from there.   When that doesn’t work, he moves on to another building on campus, and repeat….
- Roughly 5 hours later, the laptop and user were found and the problems were corrected. For the IT staff, this was 5 hours of pure chaos. And for the student, this was 5 hours of pure frustration.

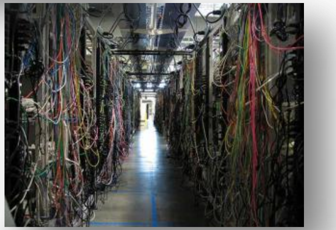
© 2012 Molex Incorporated. All Rights Reserved.

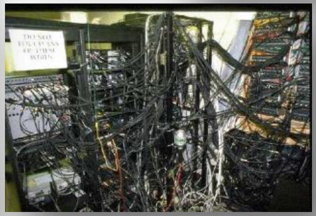
A Story…

TRADITIONAL

- OK… And I did not dare mentioning Data Centers…







© 2012 Molex Incorporated. All Rights Reserved.

Layer 1 : Security Issues & Challenges

- **Every day IT infrastructure managers face a variety of Layer 1 Challenges and Threats as they work to maintain the quality of the installed network. These can include:**

Managing MACs, especially when there are multiple sites or multiple racks involved, including some that may not have trained IT staff on hand

© 2012 Molex Incorporated. All Rights Reserved.

Layer 1 : Security Issues & Challenges

- **Every day IT infrastructure managers face a variety of Layer 1 Challenges and Threats as they work to maintain the quality of the installed network. These can include:**

  - **Managing MACs**, especially when there are multiple sites or multiple racks involved, including some that may not have trained IT staff on hand

  - **Securing valuable assets**, such as blade enclosures, Servers, engineering work stations, network printers, and IP phones

© 2012 Molex Incorporated. All Rights Reserved.

Layer 1 : Security Issues & Challenges

- **Every day IT infrastructure managers face a variety of Layer 1 Challenges and Threats as they work to maintain the quality of the installed network. These can include:**

  - **Managing MACs**, especially when there are multiple sites or multiple racks involved, including some that may not have trained IT staff on hand

  - **Securing valuable assets**, such as blade enclosures, Servers, engineering work stations, network printers, and IP phones

  - **Detecting & Locating 'rogue devices'** that are not authorized to be connected

© 2012 Molex Incorporated. All Rights Reserved.

Layer 1 : Security Issues & Challenges

- **Every day IT infrastructure managers face a variety of Layer 1 Challenges and Threats as they work to maintain the quality of the installed network. These can include:**

Managing MACs, especially when there are multiple sites or multiple racks involved, including some that may not have trained IT staff on hand

Securing valuable assets, such as blade enclosures, Servers, engineering work stations, network printers, and IP phones

Detecting & Locating 'rogue devices' that are not authorized to be connected

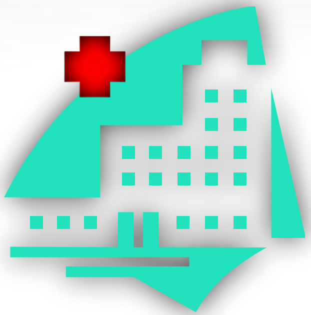
Troubleshooting at remote locations - Valuable time and money is spent investigating often mundane problems

© 2012 Molex Incorporated. All Rights Reserved.

Layer 1 : Security Issues & Challenges

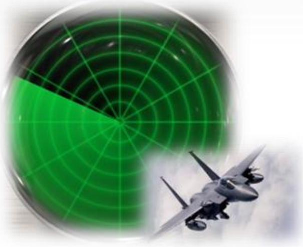
- **Zoom on some particular cases… and Continuous Business Operations**
  - Are you prepared for the unexpected ?
  - Forewarned is Forearmed !

AIRPORTS



HOSPITALS

FINANCE



MILITARY

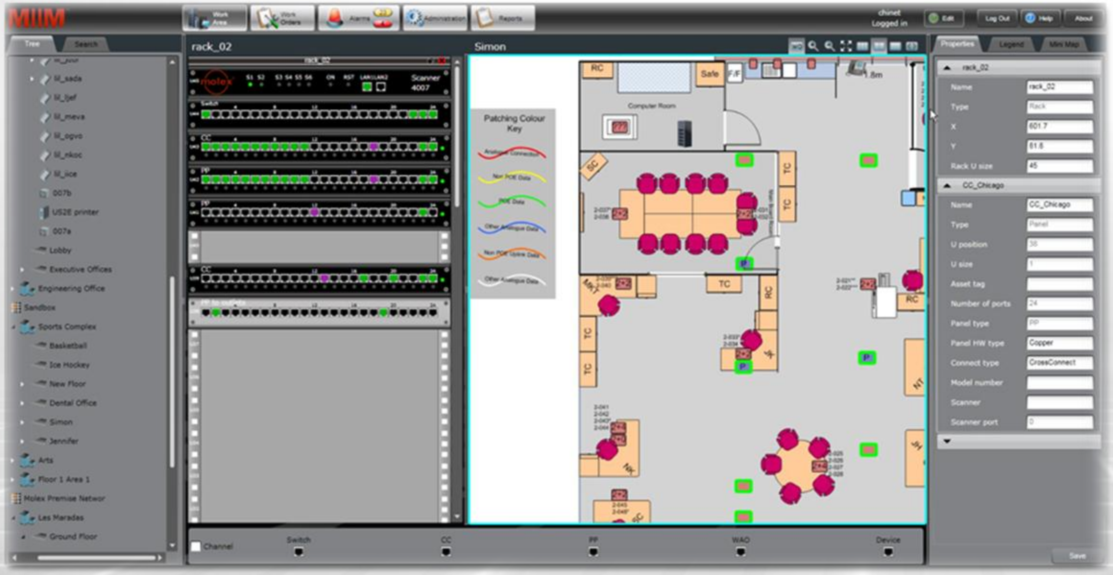
The theft of valuable assets negatively hits the bottom line of any organization.

Finding out at 10am on a Monday morning that a device went missing at 4pm the previous Friday is a problem.

© 2012 Molex Incorporated. All Rights Reserved.

Layer 1 : Security Issues & Challenges

- **Gain Control on your Layer 1 never before possible**
  - **Never again** maintain manual records of MACs
  - **Never again** update a network map or a spreadsheet
  - **Never again** confirm physical port availability
  - **Never again** manually distribute work orders
  - **Never again** physically confirm work orders are fulfilled
  - **Never again** wonder about connectivity status anywhere



rack_02

Name	rack_02
Type	Rack
X	601.7
Y	61.6
Rack U size	45

CC_Chicago

Name	CC_Chicago
Type	Panel
U position	38
U size	1
Asset tag	
Number of ports	24
Panel type	PP
Panel HW type	Copper
Connect type	CrossConnect
Model number	
Scanner	
Scanner port	0

© 2012 Molex Incorporated. All Rights Reserved.

Layer 1 : Security Issues & Challenges

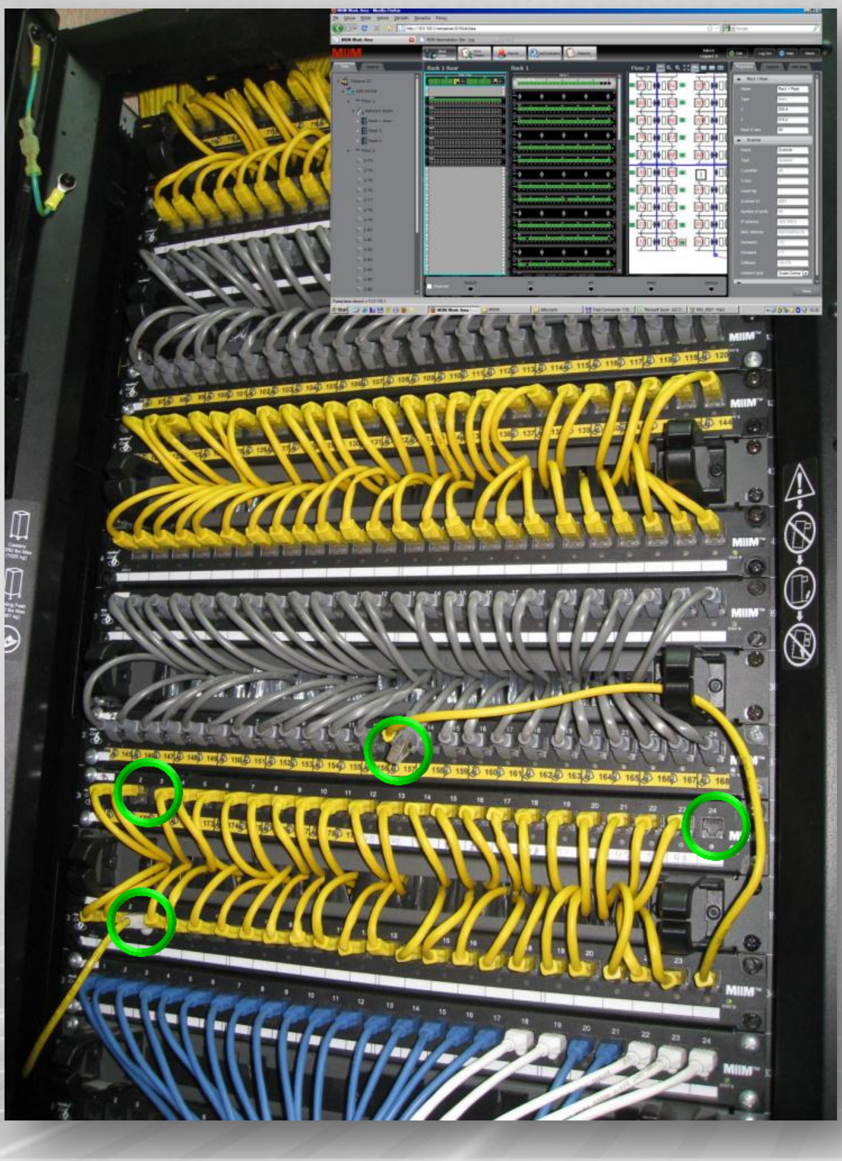
© 2012 Molex Incorporated. All Rights Reserved.

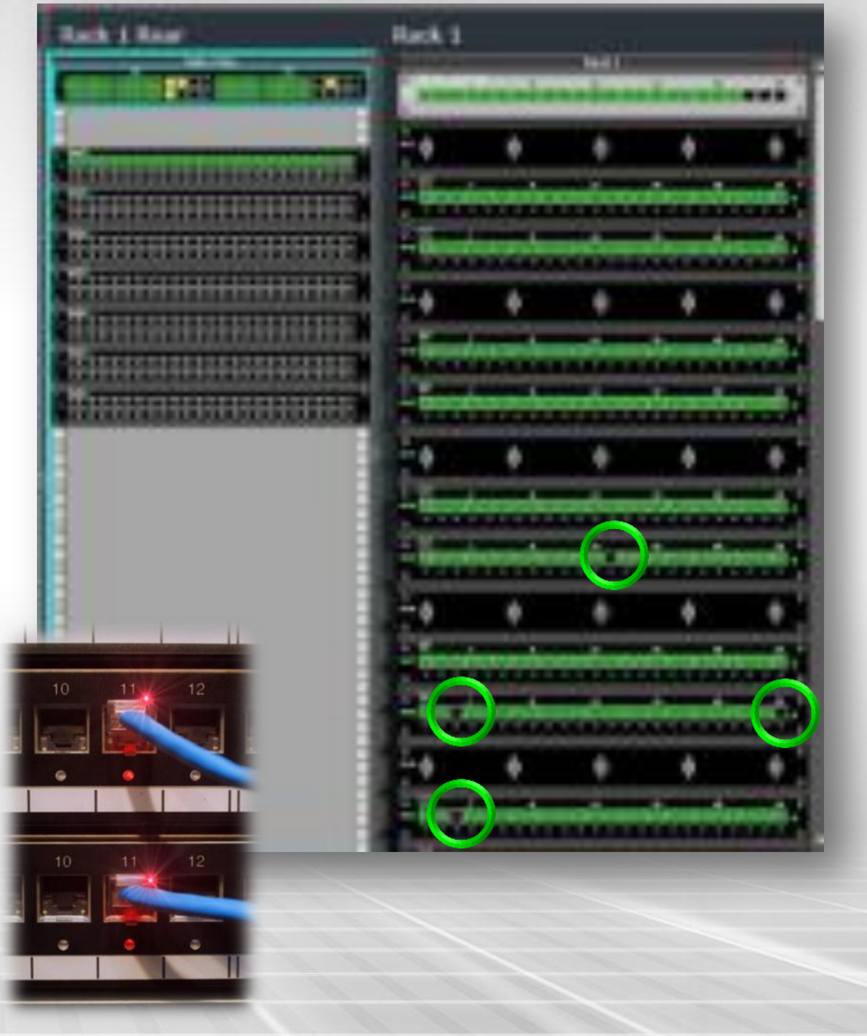
Layer 1 : Security Issues & Challenges

- MIIM becomes an integral part of your infrastructure management

© 2012 Molex Incorporated. All Rights Reserved.

Increasing visibility on Layer 1

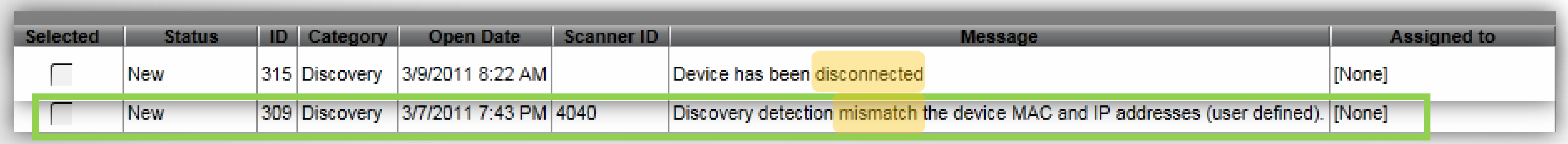




© 2012 Molex Incorporated. All Rights Reserved.

Enforcing a Proactive Approach

- **In addition to detection of breaks in the channel, device detection is desired with :**
  - Rogue insertions of unapproved devices
  - Removal of mission-critical network attached devices (such as a switch) from the network
  - Removal of high-value network attached devices (such as a printer) from the network.
- **Both Auto-Discovery & Event-Driven Discovery will map the logical network to the physical network:**

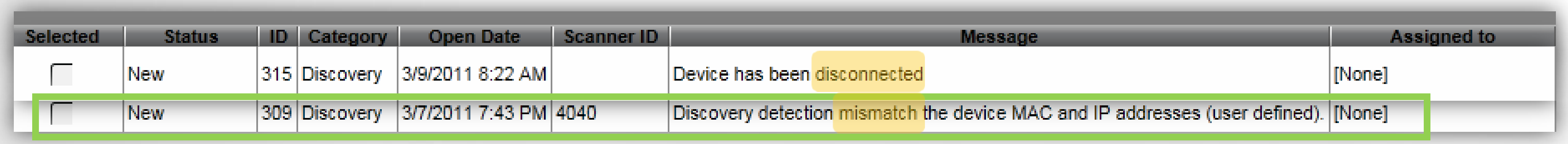


Selected	Status	ID	Category	Open Date	Scanner ID	Message	Assigned to
☐	New	315	Discovery	3/9/2011 8:22 AM		Device has been disconnected	[None]
☐	New	309	Discovery	3/7/2011 7:43 PM	4040	Discovery detection mismatch the device MAC and IP addresses (user defined).	[None]

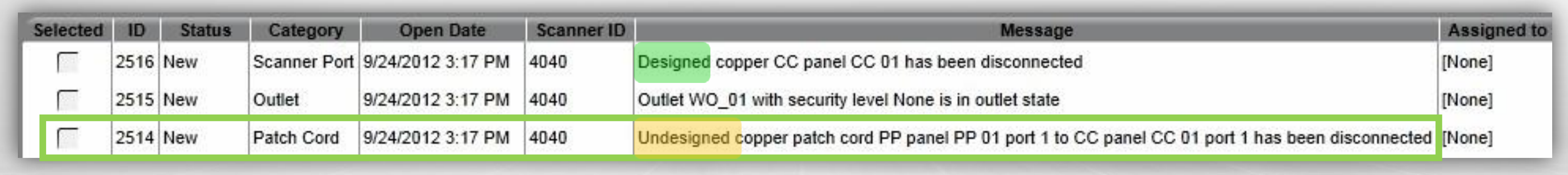
© 2012 Molex Incorporated. All Rights Reserved.

Enforcing a Proactive Approach

- **In addition to detection of breaks in the channel, device detection is desired with :**
  - Rogue insertions of unapproved devices
  - Removal of mission-critical network attached devices (such as a switch) from the network
  - Removal of high-value network attached devices (such as a printer) from the network.
- **Both Auto-Discovery & Event-Driven Discovery will map the logical network to the physical network:**



Selected	Status	ID	Category	Open Date	Scanner ID	Message	Assigned to
□	New	315	Discovery	3/9/2011 8:22 AM		Device has been disconnected	[None]
□	New	309	Discovery	3/7/2011 7:43 PM	4040	Discovery detection mismatch the device MAC and IP addresses (user defined).	[None]

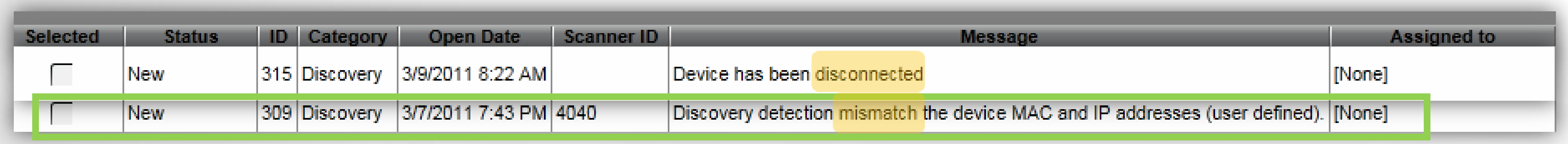


Selected	ID	Status	Category	Open Date	Scanner ID	Message	Assigned to
□	2516	New	Scanner Port	9/24/2012 3:17 PM	4040	Designed copper CC panel CC 01 has been disconnected	[None]
□	2515	New	Outlet	9/24/2012 3:17 PM	4040	Outlet WO_01 with security level None is in outlet state	[None]
□	2514	New	Patch Cord	9/24/2012 3:17 PM	4040	Undesigned copper patch cord PP panel PP 01 port 1 to CC panel CC 01 port 1 has been disconnected	[None]

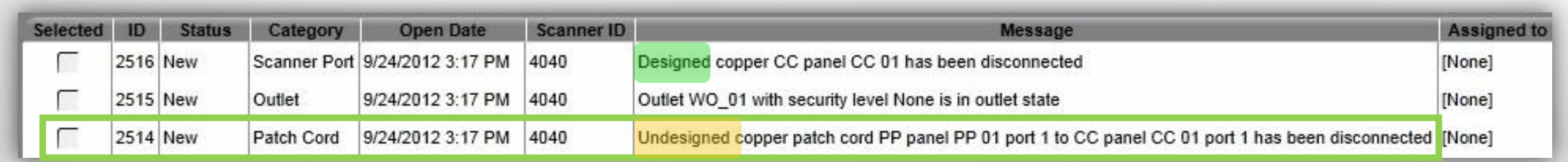
© 2012 Molex Incorporated. All Rights Reserved.

Enforcing a Proactive Approach

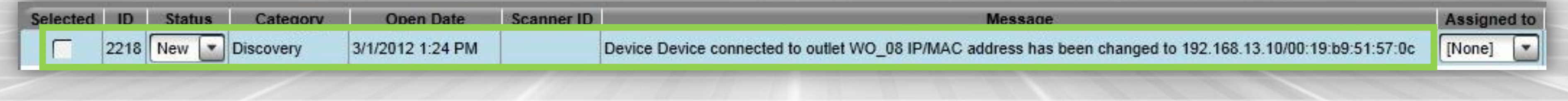
- **In addition to detection of breaks in the channel, device detection is desired with :**
  - Rogue insertions of unapproved devices
  - Removal of mission-critical network attached devices (such as a switch) from the network
  - Removal of high-value network attached devices (such as a printer) from the network.
- **Both Auto-Discovery & Event-Driven Discovery will map the logical network to the physical network:**



Selected	Status	ID	Category	Open Date	Scanner ID	Message	Assigned to
□	New	315	Discovery	3/9/2011 8:22 AM		Device has been disconnected	[None]
□	New	309	Discovery	3/7/2011 7:43 PM	4040	Discovery detection mismatch the device MAC and IP addresses (user defined).	[None]



Selected	ID	Status	Category	Open Date	Scanner ID	Message	Assigned to
□	2516	New	Scanner Port	9/24/2012 3:17 PM	4040	Designed copper CC panel CC 01 has been disconnected	[None]
□	2515	New	Outlet	9/24/2012 3:17 PM	4040	Outlet WO_01 with security level None is in outlet state	[None]
□	2514	New	Patch Cord	9/24/2012 3:17 PM	4040	Undesigned copper patch cord PP panel PP 01 port 1 to CC panel CC 01 port 1 has been disconnected	[None]



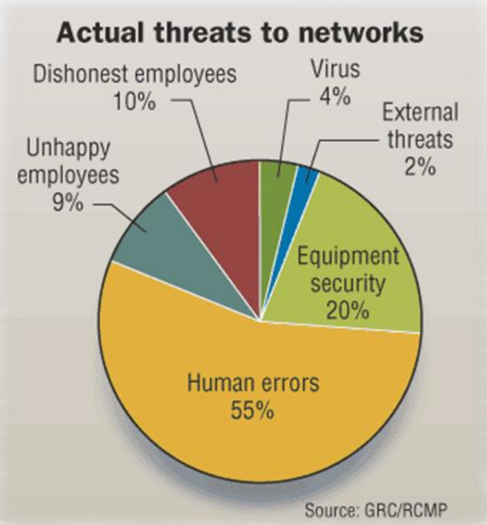
Selected	ID	Status	Category	Open Date	Scanner ID	Message	Assigned to
□	2218	New ▼	Discovery	3/1/2012 1:24 PM		Device Device connected to outlet WO_08 IP/MAC address has been changed to 192.168.13.10/00:19:b9:51:57:0c	[None] ▼

© 2012 Molex Incorporated. All Rights Reserved.

Enforcing a Proactive Approach

- Remember : good people can do bad things as well ☹…
- The employee who brings a router from home
- Or worse: a WAP (just trying to be helpful)!
- Moving the office VoIP phone to a conference room – how to track its location for emergency response?
- The night cleaning crew and the vacuum cleaner – breaking the RJ45 plug for a critical piece of equipment
- The contractor working on the HVAC system in the ceiling – and breaking the connections of a Consolidation Point…

Inside threats are often not malicious – but from good people doing bad things…

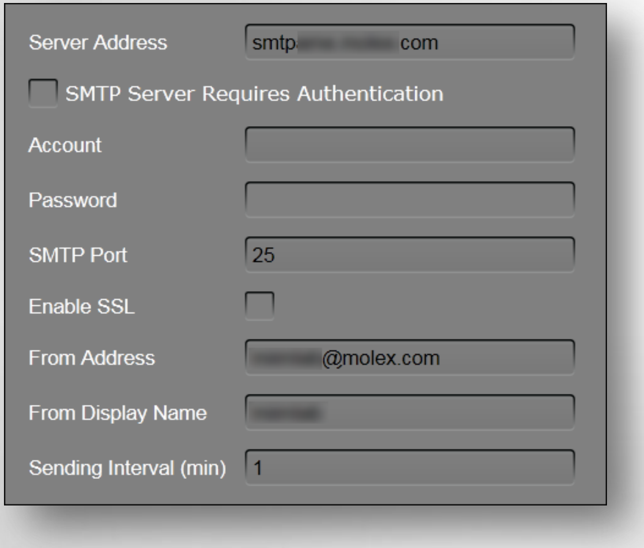


Source: GRC/RCMP

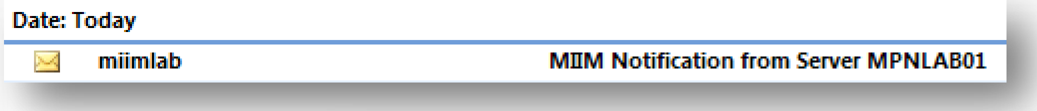
© 2012 Molex Incorporated. All Rights Reserved.

Being informed of a security breach

- **Be Informed & Receive alarms Anywhere & at Anytime**
  - By e-mail and via SNMP Traps

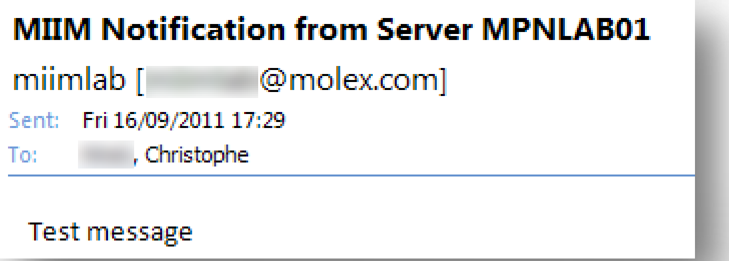


Server Address	smtp[redacted]com
□ SMTP Server Requires Authentication	
Account	
Password	
SMTP Port	25
Enable SSL	□
From Address	[redacted]@molex.com
From Display Name	[redacted]
Sending Interval (min)	1



Date: Today

miimlab MIIM Notification from Server MPNLAB01



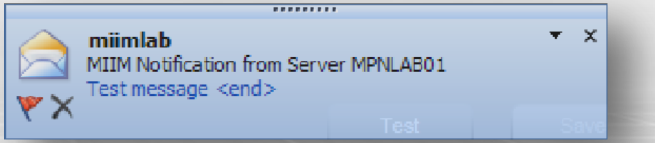
MIIM Notification from Server MPNLAB01

miimlab [[redacted]@molex.com]

Sent: Fri 16/09/2011 17:29

To: [redacted], Christophe

Test message



miimlab

MIIM Notification from Server MPNLAB01

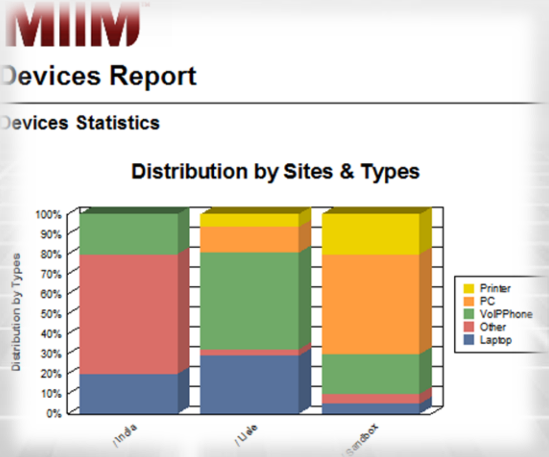
Test message <end>

© 2012 Molex Incorporated. All Rights Reserved.

Summary

- **Monitoring End-Devices, Servers & Switches**
  - The physical layer is often neglected with regards to security
  - BUT : Without the physical layer there is no Layer 2, 3, …

  - If you can monitor connectivity of the physical layer you may:
    - Know precisely what is connected, and where on your Network – **Auto and Event-Driven Discovery**
    - Improve the security of your company’s assets with instant notification of end-device connects & disconnects - **Even if the device is turned OFF**
    - Recognize rogue channels and rogue end-devices – **Using standard RJ45 cords**
    - Augment your existing security systems with event logs – **Multiple notification possibilities**
    - Augment your existing network management tools with the status of the physical layer - **Reporting**



MIIM

Devices Report

Devices Statistics

Distribution by Sites & Types

© 2012 Molex Incorporated. All Rights Reserved.

Thank You !

molex®

one company › a world of innovation