

info@networkintegritysystems.com www.networkintegritysystems.com

We Bring Security To Light[™]

Application Note: Deactivating Switch/Router Ports in Response to Intrusion Events

Each Interceptor channel has an optical switch that can block traffic flow in response to intrusion events. In extrinsic configurations, where there are several unmonitored fibers alongside a monitored fiber, and the Interceptor cannot block traffic flow when there is an intrusion event. One way to solve this problem is to have the Network Management Application react to Interceptor intrusion events by sending interface-down commands to the switches or routers that use the unmonitored fibers. In this manner, multiple fibers can be blocked in response to an Intrusion event on a single monitored fiber.

This application note will explain how to automatically turn switch and router interfaces off in response to intrusion events from an Interceptor. The program "What's Up Gold" is used in this app note, although the technique is not limited to that program. It is assumed that What's Up Gold has already been configured to monitor the Interceptor as described in application note "NIS WUG appnote".

1 The IF-MIB

Most switches and routers support the SNMP IF-MIB, which provides information and control of all the interfaces on that device. The variable *ifAdminStatus* is a writeable variable that allows interfaces to be turned on and off. The OID for *ifAdminStatus* is ...

1.3.6.1.2.1.2.2.1.7.x

 \dots where x is the interface number. The interface number normally matches the physical label on the device, but this may not be the case on complex devices.

ifAdminStatus is an integer with 1 meaning "up", and 2 meaning "down".

2 Add your switch

WUG must know about your switch to be able to control it. First, add an SNMP credential by clicking "Configure->Credentials...", then "New". The example below shows the creation of an SNMP v2 credential. SNMP v3 is preferred if your switch supports it.



info@networkintegritysystems.com www.networkintegritysystems.com

We Bring Security To Light[™]

Add New SNMP v2 Credential Type	×
Name:	_
Description:	
public	ОК
SNMP write community:	Cancel
private	Help

Name	۵	Description	Туре	New
🗾 my switch			SNMP v2	<u>E</u> dit
i≣ my v3 cred			SNMP v3	<u>C</u> opy <u>D</u> elete
				OK Cancel

Next, get WUG to discover your device by clicking "Tools->Discover Devices...". Ensure your new SNMP credential is selected for the scan...



We Bring Security To Light[™]

Network Integrity Systems 1937 Tate Blvd. SE Hickory, NC 28602 Phone: 828.322.2181 Fax: 828.322.5294

info@networkintegritysystems.com www.networkintegritysystems.com

WhatsUp Gold Discover Devices							
<u>F</u> ile Ad <u>v</u> anced <u>H</u> elp	*						
Settings 📀		Devices Discovered 📀					
Scan Settings (Range)	Host Name	Address	Brand	Model	Operating System		
SNMP Credentials (1/2)							
my v3 cred - SNMP V3 wr switch - SNMP V2							
Credentials Library							
Windows Credentials (0/0)							
Scan Method (Ping)							
Scan Advanced Settings							
	Progress		0.00 %				
			0.00 70				
		Device	e Information	1	0		
Start a discovery session							
Ŭ	Uevice Information	🕎 Scheduled Di	scoveries (0)	🔒 Saved Result	s (0)		

Adjust scan settings so that your switch will be detected...



info@networkintegritysystems.com www.networkintegritysystems.com

We Bring Security To Light[™]

WhatsUp Gold Discover Devices						x	
<u>F</u> ile Ad <u>v</u> anced <u>H</u> elp							
Settings 📀		Devices Discovered 📀					
Scan Settings (Range)	Host Name	Address	Brand	Model	Operating System		
<u>S</u> can Type:							
IP Range Scan 🔹							
Start Address:							
10.2.1.61							
End Address:							
10.2.1.61							
SNMP Credentials (1/2)							
Windows Credentials (0/0)							
Scan Method (Ping)							
Scan Advanced Settings	Progress		0.00 %				
		Device	Information	1		0	
Start a discovery session							
	Uevice Information	Scheduled Dis	scoveries (0)	🚽 Saved Resul	ts (0)		

Click "Start a discovery session" to discover your switch...



info @network integrity systems.com www.network integrity systems.com

We Bring Security To Light[™]

🧼 WhatsUp Gold Discove	er Devices								
<u>File</u> Ad <u>v</u> anced <u>H</u> elp									
Progress Su	ummary 📀		Devices Discovered 0						0
Device	Summary	Host Name	Address	Brand	Model	Operating System	Role	Status	
🔓 Device Limit	2500	10.2.1.61	10.2.1.61	Allied Telesis			Router 🔻	complete	📑 Ne
😻 Existing Devices	1								
Discovered Devices	1								
Netwo	rk Traffic								
😻 SNMP Bytes (in/out)	11792 / 10988								
🚅 PDU (in/out)	141 / 164								
🚅 Scanned	1 of 1								
Session	Metrics								
遭 Scan Start	3/9/2010 11:17:00 AM								
遭 Scan End	3/9/2010 11:17:31 AM								
🕗 Elapsed Time	00:00:31								
Session	Settings	4							
💻 Scan Type	Range	-			m				
SNMP Credentials	(1 / 2)	Progress			100.0	00 %		-	
Generation Windows Credentials	(0 / 0)				Device Infor	mation			0
Start a new dis	covery session								
Add completed	d devices to WhatsUp Gold	Device Information	C Scheduled Di	iscoveries (0)	Saved Results	; (0)			

After this finishes, click "Add completed devices to WhatsUp Gold"...



info@networkintegritysystems.com www.networkintegritysystems.com

We Bring Security To Light[™]

🧼 Add device:	to WhatsUp Gold			- • ×		
Add Devices to WhatsUp Gold This dialog allows you to add devices or update device settings to the WhatsUp Gold database. Only fully discovered devices are shown.						
Group Name:	RangeScan (3/2/2010 12:21:09 PM)	Default N	lame			
Device Limit:	2500 New Selected: 1	Existing Devices:	1 Available Devices	: 2498		
Selected	Host Name	Address	Primary Role	Status		
10.2	2.1.61	10.2.1.61	Router	New Device		
-		III				

Select the switch, and click "Add devices to WhatsUp Gold". The switch will now have an Active Monitor for every interface in the switch. By default, monitors for interfaces that were down at detection time will be disabled. Double click on the device and click on "Active Monitors" to enable the monitors you need...



We Bring Security To Light[™]

Network Integrity Systems 1937 Tate Blvd. SE Hickory, NC 28602 Phone: 828.322.2181 Fax: 828.322.5294

info@networkintegritysystems.com www.networkintegritysystems.com

roperties	Active Monitors		_			_
General	Active Monitors attach	ed to this device:				
Performance Monitors	Monitor Name	△ Argument	Critical	Network Interface	Comment	^ <u>A</u> d
	Interface	7	No	(default)	Allied Telesyn Ethe	Edi
Active Manitem	Interface	8	No	(default)	Allied Telesyn Ethe	
Active Monitors	Interface	9	No	(default)	Allied Telesyn Ethe	<u>R</u> emo
	Interface	10	No	(default)	Allied Telesyn Ethe	
Passive Monitors	Interface	11	No	(default)	Allied Telesyn Ethe	
2	Interface	12	No	(default)	Allied Telesyn Ethe	Critic
Actions	Interface	13	No	(default)	Allied Telesyn Ethe	=
^	Interface	14	No	(default)	Allied Telesyn Ethe	Dical
Condentiale	Interface	15	No	(default)	Allied Telesyn Ethe	Disat
	Interface	16	No	(default)	Allied Telesyn Ethe	Enab
	Interface	17	No	(default)	Allied Telesyn Ethe	
Polling	Interface	18	No	(default)	Allied Telesyn Ethe	
	Interface	19	No	(default)	Allied Telesyn Ethe	Ress
Notes	Interface	20	No	(default)	Allied Telesyn Ethe	Kesu
	Interface	21	No	(default)	Allied Telesyn Ethe	-
3 March	Then i a co		×1	71.7 10	AIR LT L DI	
Meriu	* Click the 'Critical' b	utton to select critical	monitors and se	et their polling order.		
Attributes						

View the switch through the WUG web interface to confirm that it is being monitored properly...



info@networkintegritysystems.com www.networkintegritysystems.com

We Bring Security To Light[™]

🧼 WhatsUp Gold	- Device S × +	ost/NmConsole/W	orkspace/DeviceSta	atus/DeviceStatus.asp	o?nDeviceID=4		
D	evice Status		10.2.1.61	Device Properties Mo	re Device <u>R</u> eports:		Workspace View:
	Home	Devices	Reports	Alert Center	vice Status	Add Content	General
Contact: Description: Location: MACAddress: MACAddressVend Model: Name: OID: OS:	Allied Telesyn Etherni 0:30:84:5E:E9:80 lor: ALLIED TELESYN INT 1.3.6.1.4.1.207.1.4.67	et Switch AT-8024GB TERNAIONAL		Tue 03/09 11:22 AM Tue 03/09 11:22 AM Tue 03/09 11:22 AM Tue 03/09 11:22 AM Tail of Action Activity Date	Interface (11) - Allied Tele HTTP Ping Log (Single Device) Action Name	esyn Ethernet Switch Trigger	Up Up Up Menu
Douico Activo Mo	nitor Statos		Мори		No action activity	recolus.	
Device Active MO	intor states		<u>iwenu</u>	Free Form Text/HTML			Menu
Interface (1) - Al Interface (1) - A Interface (11) - A Interface (12) - A Interface (13) - A Interface (13) - A Interface (14) - A Interface (15) - A Interface (16) - A Interface (17) - A Interface (21) - A Interface (22) - AI Interface (22) - A Interface (23) - A Interface (23) - A Interface (24) - A Interface (25) - A Interface (25) - A Interface (3) - AI Interface (5) - AI Interface (5) - AI Interface (5) - AI Interface (6) - AI Interface (6) - AI Interface (6) - AI Interface (9) - AI	ied Telesyn Ethernet Swith lilied Telesyn Ethernet Swi lilied Telesyn Ethernet Swith lied Telesyn Et	ch (10.2.1.61) itch itc	Unknown Unknown Up Unknown	Please	add text using the configur	e menu item for this p	pane.
♦HTTP		Up					
ірѕwітсн	Knowledge Base	Training	Ipswitch Inc.		Ipswitch Wh	atsUp Gold Premium E	Edition v14.1.2 Build 1

3 Add IF up/down actions

Now we will add Actions to bring interfaces up and down. For this example, we will add actions to control interface 20. Click "Configure->Action Library..."



info@networkintegritysystems.com www.networkintegritysystems.com

We Bring Security To Light[™]

🥹 Act	ion Library			X
Nar	ne Default Web Alam Email dang@netwo Sound-Down20 Sound-Down5 Sound-Lp5	Type Web Alam E-mail Action Sound Action Sound Action Sound Action	Description Play sound in the Action created by Play sound on D Play sound on D Play sound on Lin5	<u>N</u> ew <u>E</u> dit <u>C</u> opy Delete
				OK Cancel Help

Click "New" and select SNMP Set...

🤣 Select Action Type	×
What type of action would you like to create?	OK Cancel Help

Fill in the form as follows. Ensure you use your own values for IP address, SNMP credential, and Instance.



info@networkintegritysystems.com www.networkintegritysystems.com

We Bring Security To Light[™]

🕹 New SNMP Set Action		X
<u>N</u> ame:		
my switch IF20 up		
Description:		
SNMP Set Action		
Device Settings		
IP address or host name:		
10.2.1.61		
SNMP v1/v2/v3 credentials:		
🗐 my switch	▼ <u>.</u>	
Object Details		
Object identifier:	I <u>n</u> stance:	
ifAdminStatus	20	
Value <u>t</u> ype:		<u>A</u> dvanced
Integer	•	ОК
<u>V</u> alue to set:		Cancel
1		Help

Use the "copy" button to duplicate this action, and edit the copy as follows. Note that "Value to set" is now 2. Also note that the system automatically translated the object name to an OID.



info@networkintegritysystems.com www.networkintegritysystems.com

We Bring Security To Light[™]

🕹 Edit SNMP Set Action		×
<u>N</u> ame:		
my switch IF20 down		
Description:		
SNMP Set Action		
Device Settings		
IP address or host name:		
10.2.1.61		
SNMP v1/v2/v3 credentials:		
🗐 my switch	▼ [2"	
Object Details		
Object identifier:	I <u>n</u> stance:	
1.3.6.1.2.1.2.2.1.7	20 🖃	Adversed
Value <u>t</u> ype:		<u>A</u> dvanced
Integer	•	ОК
<u>V</u> alue to set:		Cancel
2		Help

The action library should now appear as follows...



info@networkintegritysystems.com www.networkintegritysystems.com

We Bring Security To Light[™]

9	Action Library			×
		1		
	Name 🗠	Туре	Description	<u>N</u> ew
	■ Default Web Alarm M Email dang@netwo	Web Alarm E-mail Action	Play sound in the Action created by	<u>E</u> dit
	💩 my switch IF20 down	SNMP Set	SNMP Set Action	<u>C</u> opy
	💩 my switch IF20 up 🌒 Sound-Down20	SNMP Set Sound Action	SNMP Set Action Play sound on D	Delete
	Sound-Down5 Sound-Up5	Sound Action Sound Action	Play sound on D Play sound on Up5	<u>T</u> est
				OK Cancel Help

4 Bind Interceptor Active Monitors to IF up/down actions

Now we will bind these actions to the up/down state of Interceptor channel 1. Double click on your Interceptor and examine the active monitors...



info@networkintegritysystems.com www.networkintegritysystems.com

We Bring Security To Light[™]

Device Properties : 192.168.1.50						
Properties Active Monitors						
General	Active Monitors attached to this device:					
Performance Monitors	Monitor Name Argument Critical Network In	terface Comment <u>A</u> dd				
Active Monitors	Image: Channel 1 HALT No (default) Image: Channel 2 HALT No (default)	Edit				
Passive Monitors						
Actions		Disable				
Credentials		Enable				
Polling						
Votes		Rescan				
Menu Menu	Menu * Click the 'Critical' button to select critical monitors and set their polling order.					
Attributes						
Tasks		OK Cancel Help				

Edit "Channel 1 HALT", and then click Add. Pick "Chose an action from the action library", and then fill in the form as follows...



info@networkintegritysystems.com www.networkintegritysystems.com

We Bring Security To Light[™]

🥹 Action Builder	
Select Action and State	•
Select an action from the Action Library: my switch IF20 down Execute the action on the following state change: Down Only if the following state was reached: Not dependent on previous state Blackout schedule	
< <u>B</u> ack <u>F</u> inish Cancel Help]

Repeat the process for the "Up" state. For "Up", the prior state must be specified...



info@networkintegritysystems.com www.networkintegritysystems.com

We Bring Security To Light[™]

🥹 Action Builder	x
Select Action and State	K
Select an action from the Action Library: my switch IF20 up Center the action on the following state change: Up Colly if the following state was reached: 0 minutes - (Down) Blackout schedule	
< <u>B</u> ack <u>F</u> inish Cancel Help	

The completed action list should appear as follows...



info@networkintegritysystems.com www.networkintegritysystems.com

We Bring Security To Light[™]

🧼 Active Monitor Properti	es for Channel 1 HALT
Categories	© Apply this Action Policy.
Polling	OR
	Apply individual actions. State Change △ Action to Perform Add
Actions	Down my switch IF20 down Edit Up my switch IF20 up Remove
	OK Cancel Help

Click OK. The switch interface will now automatically go up and down in response to up/down transitions on the Interceptor channel....



info@networkintegritysystems.com www.networkintegritysystems.com

We Bring Security To Light[™]

🤣 Ipswitch WhatsUp Gold v14.1.2 - [Network Explorer - RangeScan (3/2/2010 12:21:09 PM)]						
🔝 Eile Edit View Configure Tools Reports Window Help					_ 8 ×	
🔚 RangeScan (3/2/2010 12:21:09 PM)						
X	Display Name	△ Host Name	Address	Device Type	Status	
My Network		10.2.1.61	10.2.1.61	Allied Telesis, In		
All devices (dynamic group)		192.168.1.50	192.168.1.50	NIS Interceptor		
All routers (dynamic group)						
Dynamic Group Examples RangeScan (3/2/2010 12:21:09 PM						
	4					
	Device View	k Map View				
Ready	<u>***</u>	·····				

