

About Link Analyst 5

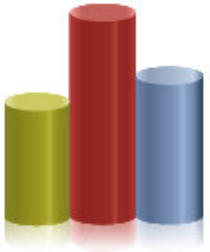


Link Analyst provides insight into the devices on your network and the routes that connect them.

- See what devices are up or down
- Know what business areas are affected
- Graph and compare data over time
- Use data in planning network upgrades
- View and drill down on device maps
- Easily troubleshoot using Observer[®]



High Level Resource Monitoring



Dynamic Reporting



Device and Route Monitoring



Event Notification



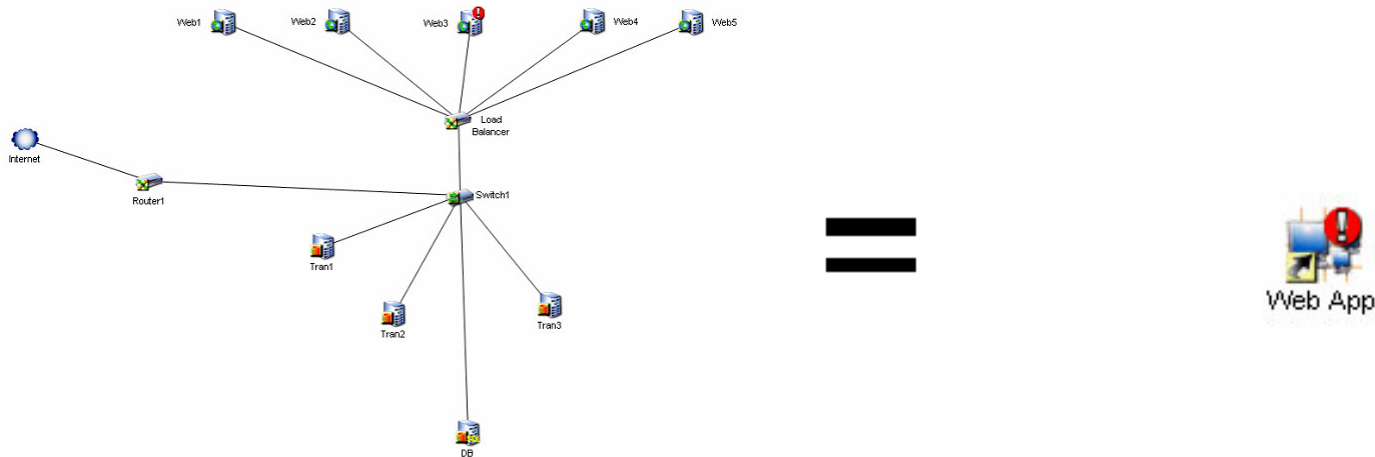
Active Discovery



Scenario 1: The Problem (Data Center)



Link Analyst deployed at data center to monitor critical multi-tier application.



Situation

Users report intermittent issues displaying web pages. There does not appear to be a pattern specific to workstation or user.



Scenario 1: How Link Analyst Helps



- Looks at system as a whole
- Availability, reliability, resource issues identified
- Alert generated and administrator notified of problem
- In addition to generating an e-mail, Link Analyst can take corrective action such as restarting a service
- Issue recorded to alarm report

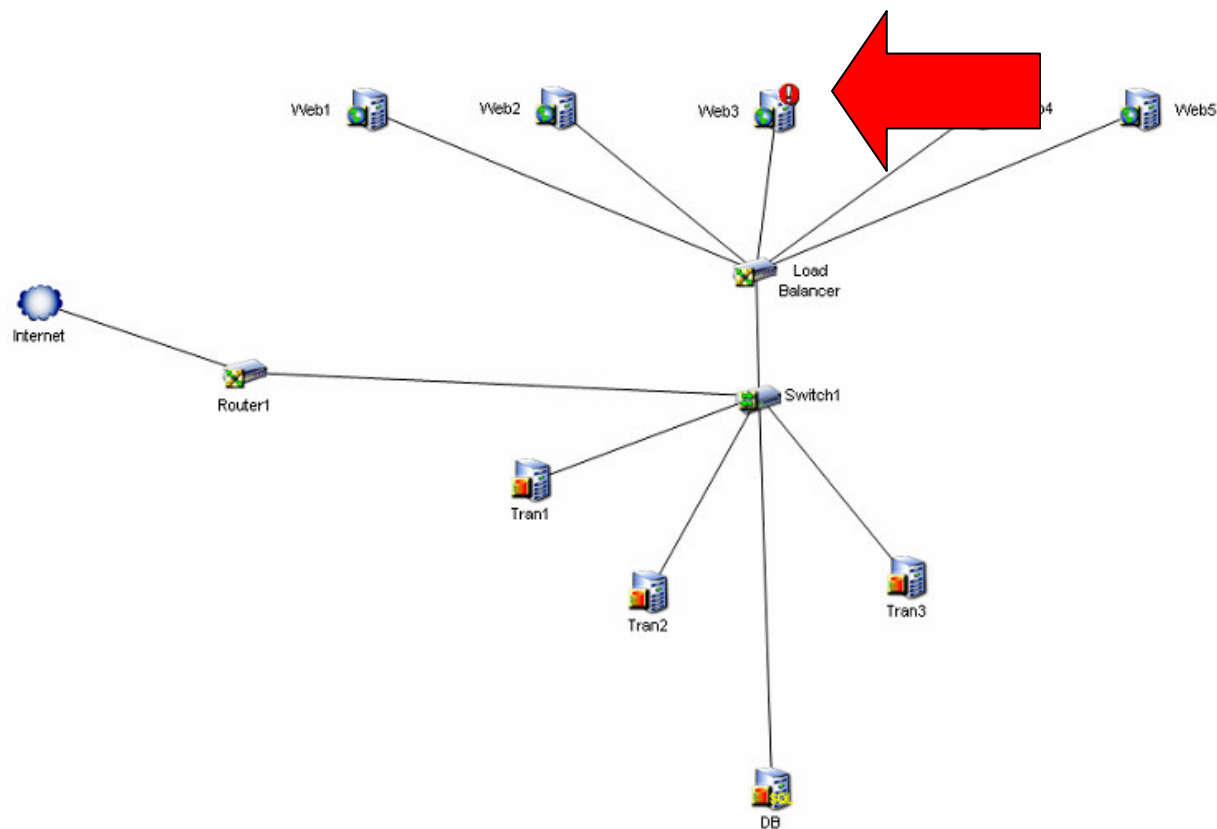


Scenario 1: Notification



Web service on Web3 fails

- Web3 shows service is down



Scenario 1: Alarm Report



[Business Group Alarms]

Alarms Report

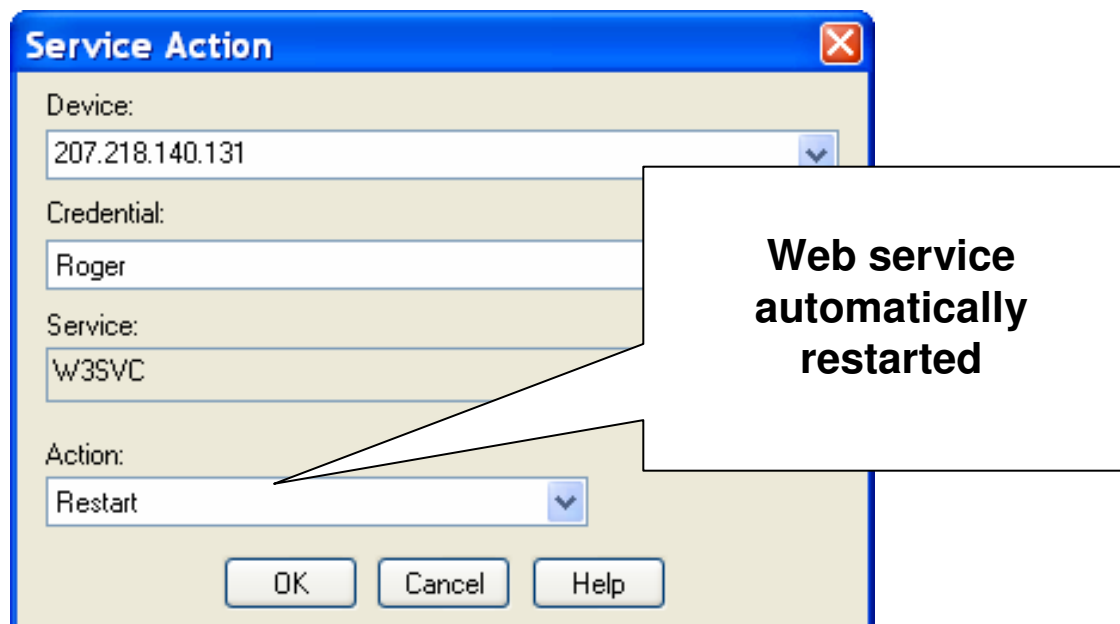
Business Group	NI
Report generated	07/17/2007 10:44:53
Last poll time	07/17/2007 10:44:46

Device (IP)	Type	Alarms
LEXMARK207.37 (207.218.140.37)	Printer	Monitor alarms: Paper Low Alert
Web3 (207.218.140.246)	Web Server	IP Services down: HTTP

[Generate Printable Report](#)

Event recorded, displayed in Alarms Report

Scenario 1: Restart Service and Notify

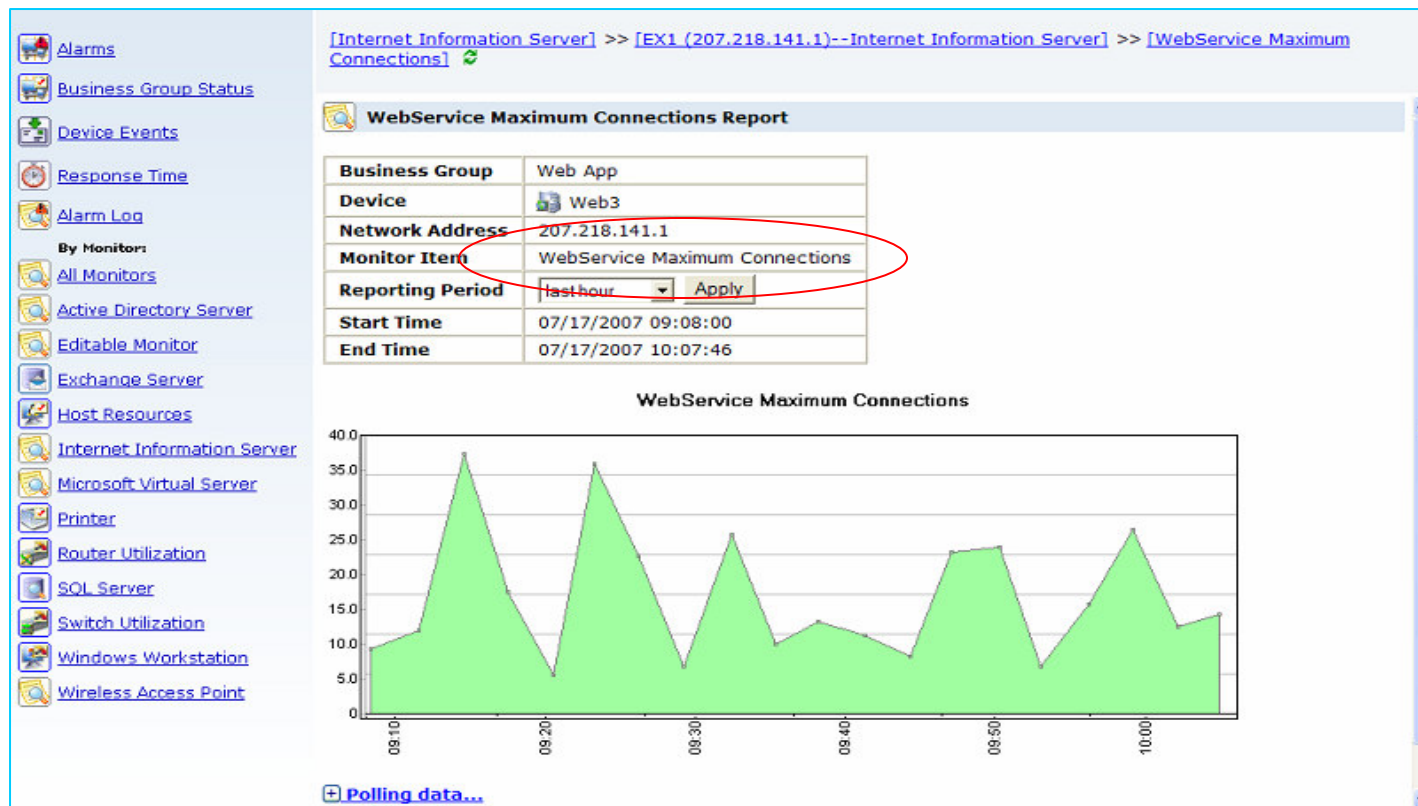


- E-mail sent to Roger, the data center manager, describing failure
- Roger views historical usage reports, server event logs using Link Analyst

Scenario 1: Investigate and Resolve



- Web3 was servicing more simultaneous users than it could handle



Scenario 2: The Problem



Corporate office deploys Link Analyst to monitor departments such as Finance, Production, and Development.

Situation

End of quarter orders must be processed and much of the work occurs after business hours. There have been critical system slow-downs.

A reboot of the database server temporarily resolved the issue, but no cause or solution has been discovered.



Scenario 2 – How Link Analyst Helps

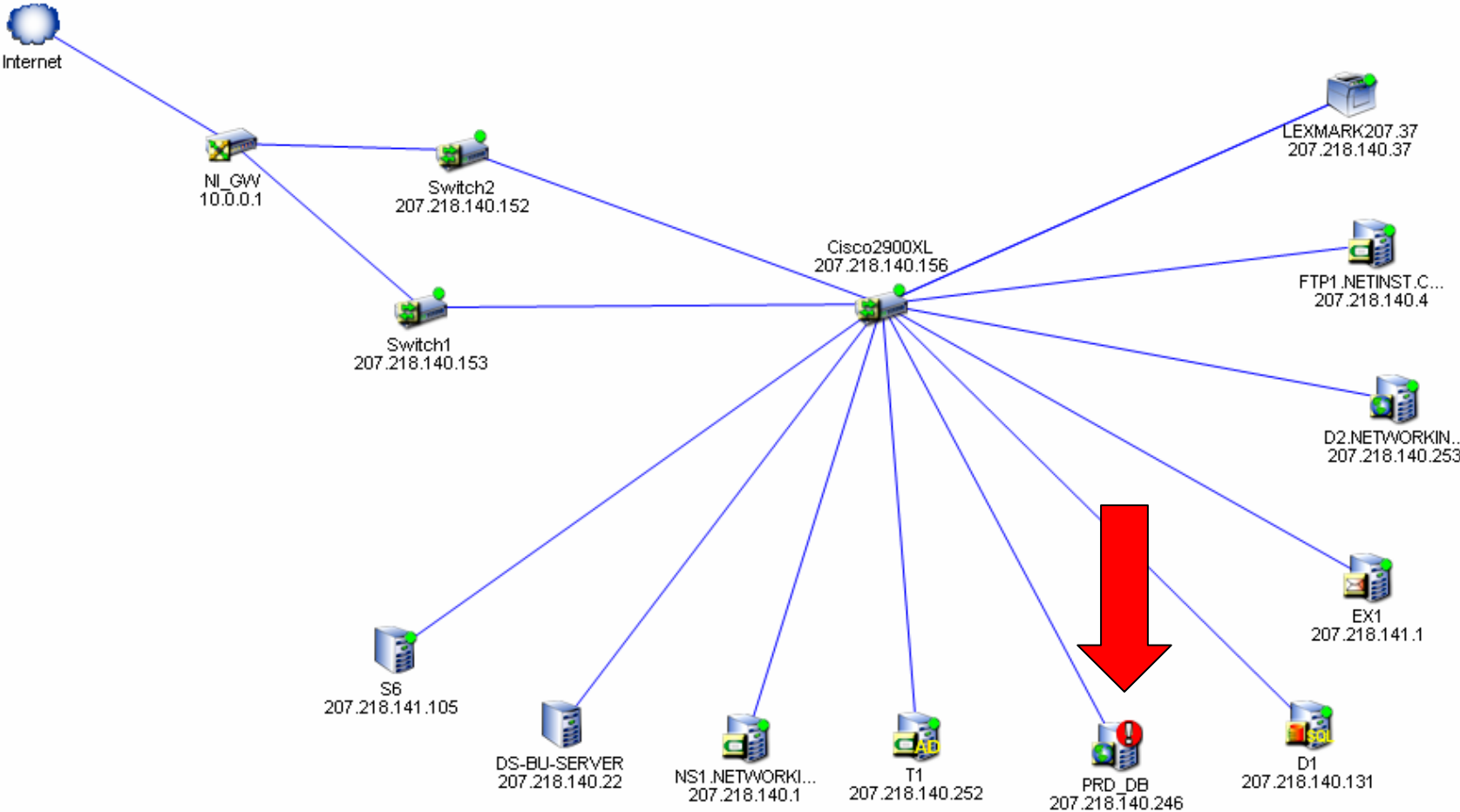


- Link Analyst monitors all production group devices
- If a system is down or performance is suffering it will be detected
- The administrator will be alerted and can take appropriate action



Scenario 2: The Result

The database server alarms due to high CPU utilization



Processor Utilization Report for PRD_DB

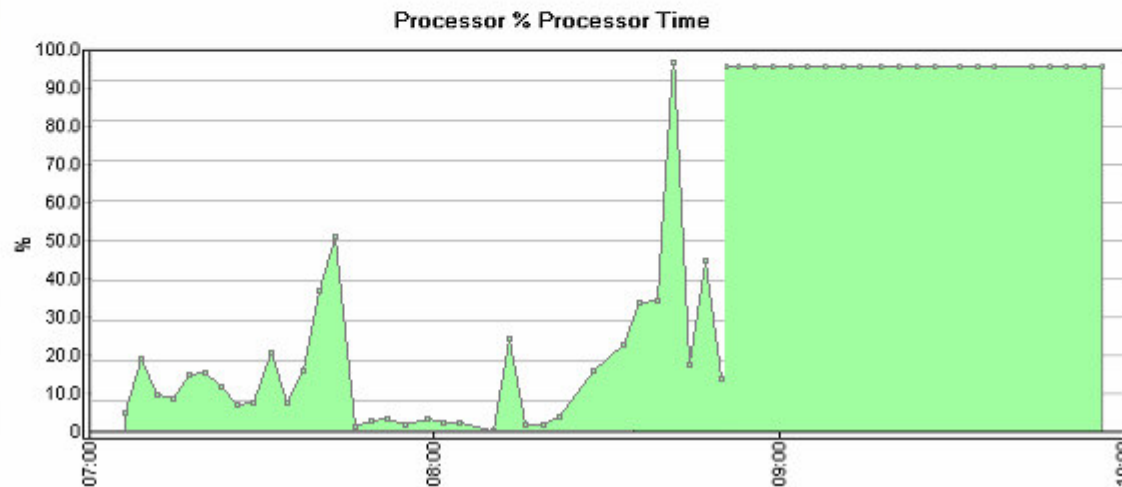


- Alarms
- Business Group Status
- Device Events
- Response Time
- Alarm Log
- By Monitor:**
- All Monitors
- Active Directory Server
- Editable Monitor
- Exchange Server
- Host Resources
- Printer
- Router Utilization
- SQL Server
- Switch Utilization
- Windows Workstation

[Windows Workstation] >> [PRD_DB (207.218.140.246)--Windows Workstation] >> [Processor % Processor Time]

Processor % Processor Time Report

Business Group	NI
Device	PRD_DB
Network Address	207.218.140.246
Monitor Item	Processor % Processor Time
Reporting Period	last 4 hours <input type="button" value="Apply"/>
Start Time	07/20/2007 06:45:00
End Time	07/20/2007 10:44:27



Running Processes on PRD_DB



Processes information:

Process Name	PID	Mem Usage	Handles
avscan.exe	1152	25596 K	64
csrss.exe	336	1572 K	402
inetinfo.exe	1284	1092 K	176
logon.scr	2704	1672 K	22
lsass.exe	420	4124 K	456
mainserv.exe	1176	1424 K	75
msdtc.exe	1044	620 K	180
services.exe	408	18380 K	306
smss.exe	288	320 K	23
spoolsv.exe	1004	3112 K	130
svchost.exe	684	2124 K	278
svchost.exe	760	1512 K	143
svchost.exe	796	1288 K	175
svchost.exe	1224	516 K	71
svchost.exe	812	12804 K	1080
svchost.exe	1320	1368 K	59
svchost.exe	1700	1132 K	154
svchost.exe	1944	1992 K	179
svchost.exe	600	1252 K	90
System	4	216 K	995
System Idle Process	0	16 K	0
vmnat.exe	1560	616 K	64
vmnetdhcp.exe	1668	892 K	43
vmount2.exe	1520	576 K	93

- A check of running processes shows a scheduled virus scan is running and causing the slowdown
- This is not usually an issue, since orders are rarely processed at 11:00 PM, but end of quarter is a special circumstance

- **SNMP**

- **MIB – Management Information Base**

- Tracks the types and location of information on SNMP device

- **OID – Object Identifier**

- String used to query specific piece of information from SNMP device

- **WMI**

- For monitoring and management of Windows systems

- Requires Administrator permissions to query

- Used to identify environment-independent information

Create and Monitor Business Groups



Know which part of your business is affected – instantly

- Create groups by department, device type, function, or customize
- View reports, monitor resources, track inventory by Business Group
- Click within a group for easy sub-level analysis



Dynamic Reporting

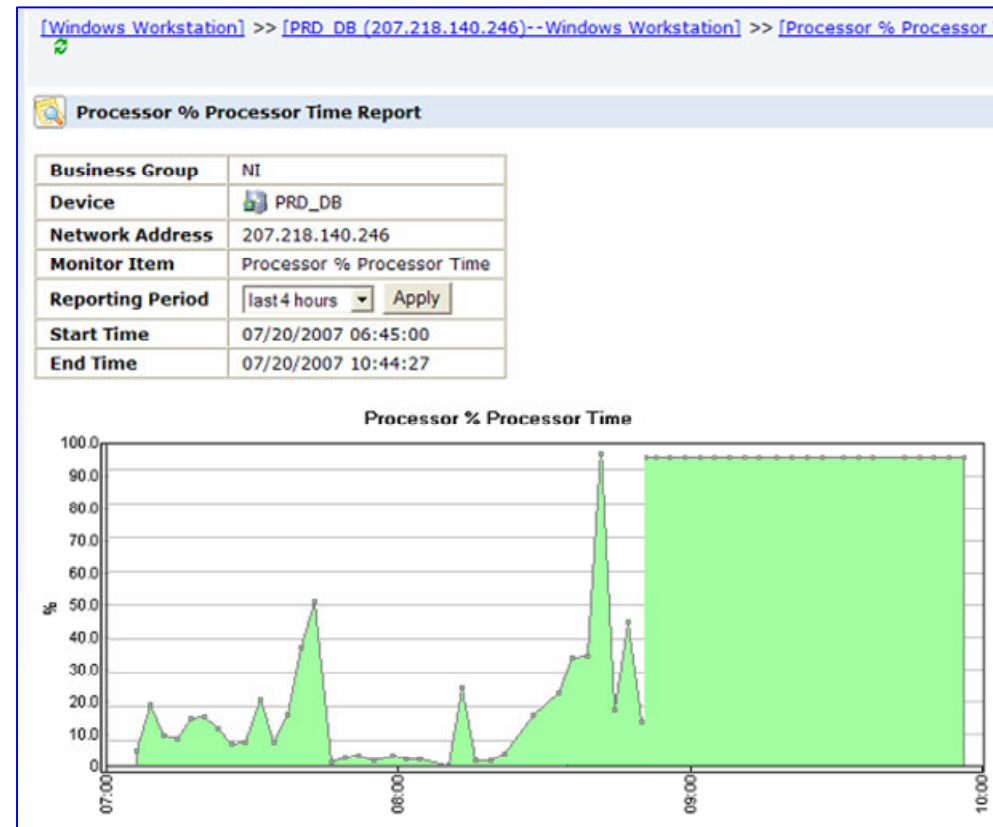


Customize, view, expand, and compare reports for in-depth analysis on routes, devices, and groups.

Track statistics over time for use in network trending and analysis.

Report Types Include:

- Alarms
- Business Group Status
- Device Events
- Response Time
- Alarm Log



Monitoring Reports



- Report on failing devices with Alarms and Alarm Logs
- See overall health with Business Group Status and Response Time Reports
- Gain visibility into Event Logs and Syslogs with Device Events
- Group devices by role or function using monitors
- Show key statistics specific to device function



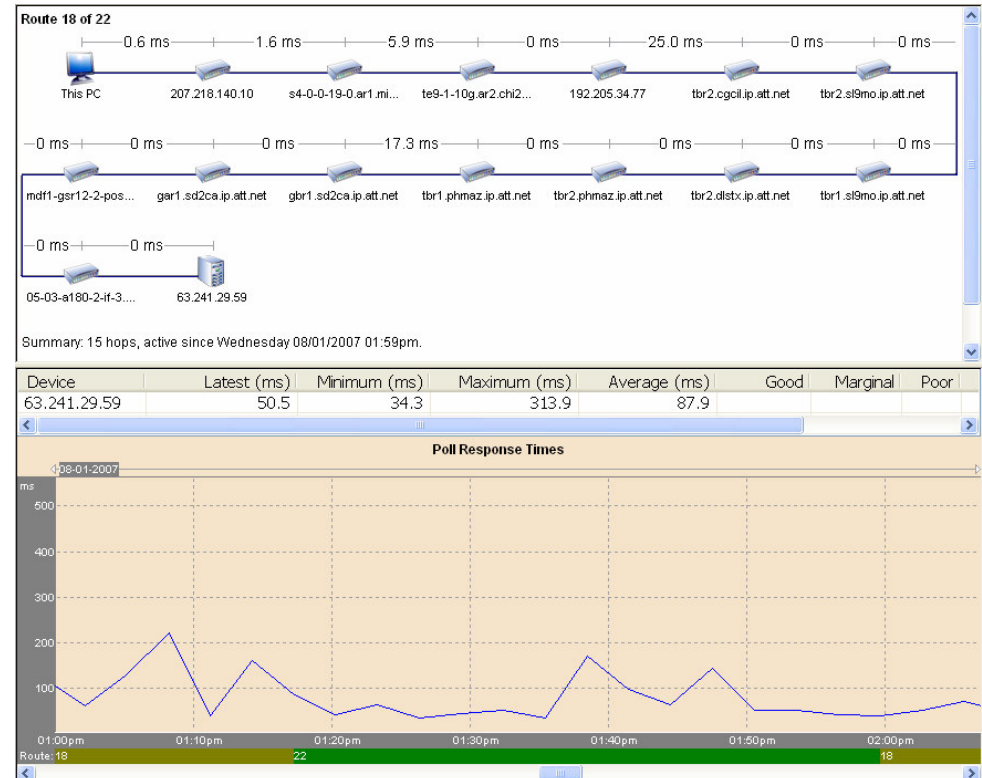
Device and Route Monitoring



Use SNMP & WMI data to monitor Active Directory Servers, Host Resources, Internet Information Servers and more, or create custom monitors.

Know at a glance which devices, routes, and IP services are up or down.

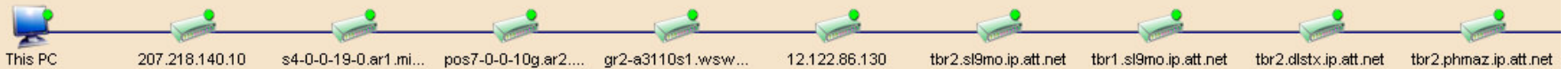
- Monitor virtual servers and workstations
- Set configurable alarms and thresholds
- Graph statistics over time



Graphic Display of Routes Taken

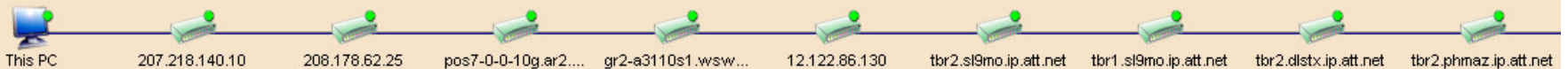


Route 1



Summary: 15 hops, first seen Friday 05/18/2007 11:03am, last seen Friday 05/18/2007 04:38pm

Route 2



Summary: 15 hops, first seen Friday 05/18/2007 11:03am, last seen Friday 05/18/2007 02:58pm

Route 3



Summary: 12 hops, first seen Tuesday 06/19/2007 09:59am, last seen Friday 06/22/2007 05:09pm

Route 4



Summary: 12 hops, first seen Tuesday 06/19/2007 10:11am, last seen Friday 06/22/2007 03:45pm

Route 5



Summary: 15 hops, first seen Thursday 06/21/2007 09:35am, last seen Thursday 06/21/2007 03:00pm

Route 6



IP Services Monitor



Know at a glance which devices or services are up or down

The screenshot shows the NI IP Services Monitor interface. The top navigation bar includes 'Monitoring', 'Topology Discovery', 'Inventories', and 'Alarmed'. Below this is a menu with 'Reports', 'Monitoring Map', 'Devices', 'IP Services', and 'Response Times'. The main area is a table with columns for 'State', 'Device', 'DNS', 'FTP', 'HTTP', 'NET', and 'IPCD3'. A callout box labeled 'Alarmed device' points to the row for 'S1 (207.218.140.130)', which has a red downward arrow in the HTTP column. Other rows show various devices and services with green upward arrows indicating they are up.

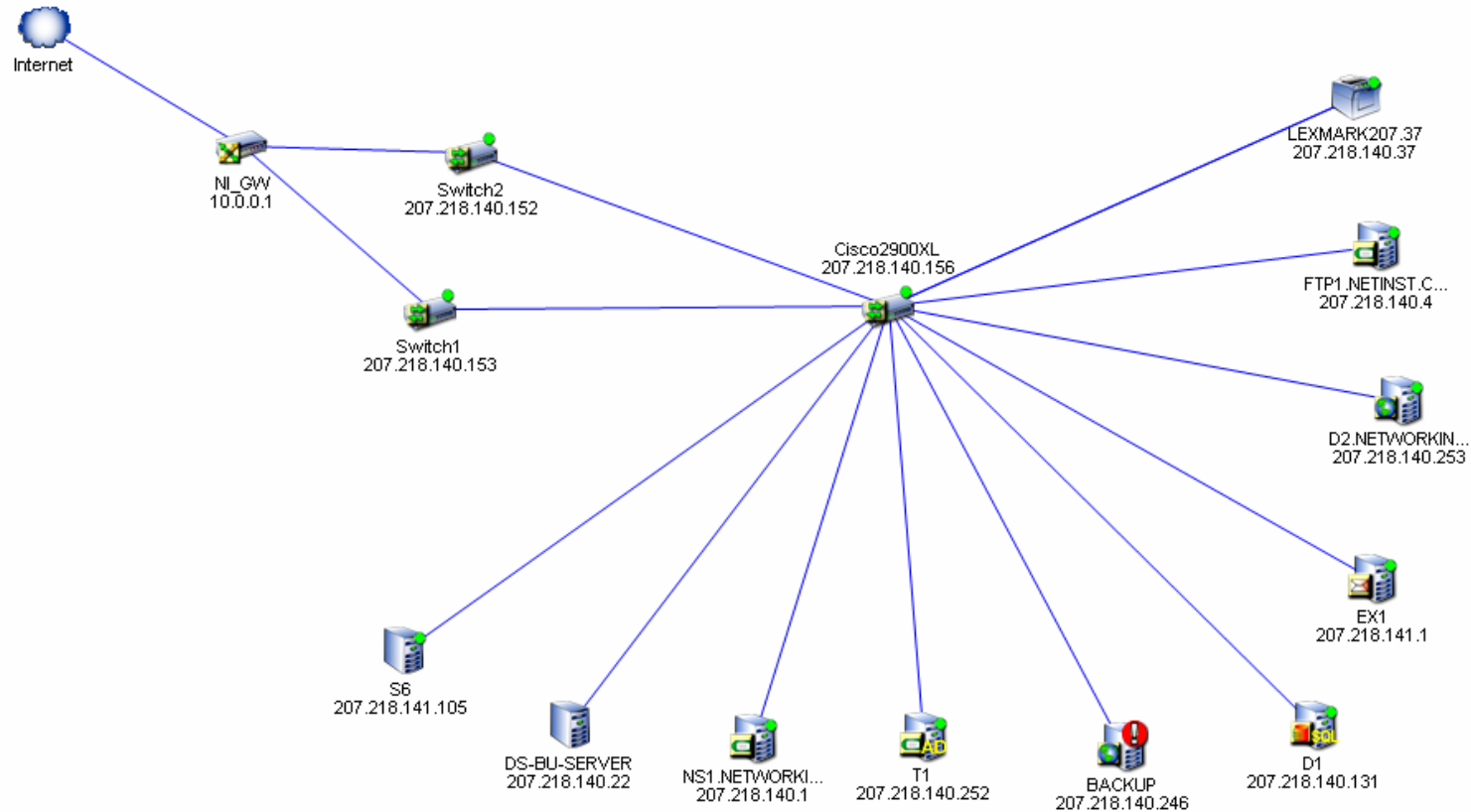
	State	Device	DNS	FTP	HTTP	NET	IPCD3
1		NI_GW (10.0.0.1)					
2		Switch1 (207.218.140.153)					
3		Switch2 (207.218.140.152)					
4		FTP1.NETINST.COM (207.218.140.4)					
5		S1 (207.218.140.130)					
6		NS1.NETWORKINSTRUMENTS.COM ...					
7		Cisco2900XL (207.218.140.156)					
8		EX1 (207.218.141.1)					
9		DS-BU-SERVER (207.218.140.22)					
10		BACKUP (207.218.140.246)					
11		D2.NETWORKINSTRUMENTS.COM (...)					
12		D1 (207.218.140.131)					
13		S6 (207.218.141.47)					
14		LEXMARK207.37 (207.218.140.37)					

Polling starts in 8 seconds...

Production Group Monitoring Map



Add, remove, and arrange the devices you wish to monitor



Monitors



Credentials Library | Data Management | Alarm Responses
General | IP Services | Discovery | Inventory Objects | Global Inventory Alarms | **Monitors** | Notifications | Web Access

Monitors ▲	Monitor Elements ▲	Type	Details
Active Directory Server	Buffer Manager - Page Reads/sec	Parameter: WMI Script	Performance counter, single ↘
All Monitors	Buffer Manager - Page Writes/sec	Parameter: WMI Script	Performance counter, single ↘
Editable Monitor	Cache Manager - Cache Hit Ratio	Parameter: WMI Script	Performance counter, single ↘
Exchange Server	Cache Memory	Parameter: WMI Raw Performance Counters	Win32_PerfRawData_MSSQ
Host Resources	Current Users	Parameter: WMI Raw Performance Counters	Win32_PerfRawData_MSSQ
Internet Information Server	Databases - Active Transactions	Parameter: WMI Raw Performance Counters	Win32_PerfRawData_MSSQ
Microsoft Virtual Server	Databases - Data Files Size	Parameter: WMI Raw Performance Counters	Win32_PerfRawData_MSSQ
Printer	General Statistics - Logins/sec	Parameter: WMI Script	Performance counter, single ↘
Router Utilization	Latches - Average Latch Wait Time	Parameter: WMI Script	Performance counter, single ↘
SQL Server	Locks - Deadlocks/sec	Parameter: WMI Script	Performance counter, single ↘
Switch Utilization	Locks - Lock Requests/sec	Parameter: WMI Script	Performance counter, single ↘
Test	Log Files Size	Parameter: WMI Raw Performance Counters	Win32_PerfRawData_MSSQ
VMWare Virtual Server	Page Life Expectancy	Parameter: WMI Raw Performance Counters	Win32_PerfRawData_MSSQ
Windows Workstation	Percent Log Used	Parameter: WMI Raw Performance Counters	Win32_PerfRawData_MSSQ
Wireless Access Point	Server Memory in Use	Parameter: WMI Raw Performance Counters	Win32_PerfRawData_MSSQ
	SQL Users	Parameter: WMI Raw Performance Counters	Win32_PerfRawData_MSSQ

New... Properties... Delete

New... Edit... Delete

Alarms



Be alerted when a device is unreachable or has poor response time

Choose sound, pager, or e-mail alerts, or set Link Analyst to launch a program or generate a trouble ticket

[Business Group Alarms] ↻

Alarms Report

Business Group	NI
Report generated	06/25/2007 15:21:54
Last poll time	06/25/2007 14:50:51

Device ▲ (IP)	Type	Alarms
S1 (207.218.140.130)	Web Server	Device is down

[Generate Printable Report](#)

Drill Down on Failing Device



- Alarms
- Business Group Status
- Device Events
- Response Time
- Alarm Log
- By Monitor:
- All Monitors
- Active Directory Server
- Editable Monitor
- Exchange Server
- Host Resources
- Printer
- Router Utilization
- SQL Server
- Switch Utilization
- Windows Workstation

[Business Group Alarms] >> [BACKUP (207.218.140.246)]

Device Status Report

Business Group	NI
Report generated	08/01/2007 13:48:08
Device	BACKUP
Network Address	207.218.140.246

Device alarms:

- IP Services down: [HTTP](#)

Response Time:

Polling Time	Response Time (ms)	Status	Last 4 Hours
8/1/2007 1:47:37 PM	0.202		

IP Services:

POP3	NNTP	iPCD3	FTP	TELNET	SMTP	LPD	HTTP	SNMP	DNS

Alarm Logs



The screenshot shows the NI Monitoring software interface. The top navigation bar includes 'Monitoring', 'Topology Discovery', 'Inventories', and 'Alarmed Devices: 2'. Below this is a sub-menu with 'Reports', 'Monitoring Map', 'Devices', 'IP Services', and 'Response Times'. The left-hand navigation pane lists various monitoring categories: Alarms, Business Group Status, Device Events, Response Time, Alarm Log (selected), and a 'By Monitor:' section with options like All Monitors, Active Directory Server, Editable Monitor, Exchange Server, Host Resources, Printer, Router Utilization, SQL Server, Switch Utilization, and Windows Workstation.

The main content area displays the 'Alarm Log' section. It includes a filter table with the following data:

Business Group	NI
Reporting period	last 4 hours <input type="button" value="Apply"/>
Start Time	06/28/2007 08:18:54
End Time	06/28/2007 12:18:54

Below the filter table is a table of log entries:

Device (IP)	Type	Log Entries
[ALL DEVICES]		7
BACKUP(207.218.140.246)	Web Server	1
Cisco2900XL(207.218.140.156)	Switch	1
NI GW(10.0.0.1)	Router	1
S1(207.218.140.130)	Web Server	2
Switch1(207.218.140.153)	Switch	1
Switch2(207.218.140.152)	Switch	1

Below the log entries table is a link: [Generate Printable Report](#)

The status bar at the bottom of the window displays the text: 'Polling starts in 12 seconds...'

Active Discovery Benefits



- See what devices are connected and how they are connected
- Get graphical or table-based display of a network, segment, or remote locations on the WAN
- Monitor response time and performance of devices anywhere on the network

Network Devices ▲	Type	SNMP	WMI	Interfaces	MAC address	IP address	IP...
+	Cisco	Wireless Access Point	Yes	3			
+	Cisco2900XL	Switch	Yes	13			
+	FastEthernet0/1				00:04:DD:F1:09:C1	207.218.140.156	
+	FastEthernet0/10				00:04:DD:F1:09:CA	207.218.140.156	
+	FastEthernet0/11				00:04:DD:F1:09:CB	207.218.140.156	
+	FastEthernet0/12				00:04:DD:F1:09:CC	207.218.140.156	
+	FastEthernet0/2				00:04:DD:F1:09:C2	207.218.140.156	
+	FastEthernet0/3				00:04:DD:F1:09:C3	207.218.140.156	
+	FastEthernet0/4				00:04:DD:F1:09:C4	207.218.140.156	
+	FastEthernet0/5				00:04:DD:F1:09:C5	207.218.140.156	
+	FastEthernet0/6				00:04:DD:F1:09:C6	207.218.140.156	
+	FastEthernet0/7				00:04:DD:F1:09:C7	207.218.140.156	
+	FastEthernet0/8				00:04:DD:F1:09:C8	207.218.140.156	
+	FastEthernet0/9				00:04:DD:F1:09:C9	207.218.140.156	
+	VLAN1				00:04:DD:F1:09:C0	207.218.140.156	
+	CiscoAG	Wireless Access Point	Yes	4			
+	CiscoSwitch.netinst.com	Switch	Yes	9			
+	D1	Windows Computer	Yes	Yes	2		

Right-click a Device to Dig Deeper



- Get Device Status Reports
- Troubleshoot using tools such as Ping and Trace Route
- Start or stop services
- Access device's web interface using HTTP or HTTPS
- Use Observer for advanced network analysis



Current Inventory Information



Track static items such as hard drives, memory, and processors

NI-Corp

Monitoring Topology Discovery Inventories **Alarmed Devices: 1**

Take Snapshot Inventory Active Inventory Status... Inventory Schedule... Manage Inventories...

Inventory Reports

Select an entry from the list and click "Report"

7/19/2007 10:41:55 AM

Report

or select entries in both lists and click "Compare"

8/3/2007 12:48:06 PM

Compare

[Summary]

Business Group	NI-Corp
Report Type	Inventory comparison
Inventory	8/3/2007 12:48:06 PM
Compare to	7/19/2007 10:41:55 AM
Report generated	8/3/2007 12:48:40 PM

Show details

Device	Network address	New	Missing	Changed
backup	207.218.140.246	0	0	0
BigIron1	207.218.140.153	0	0	0
BigIron2	207.218.140.152	0	0	0
Bills Dell-3024	207.218.140.66	0	0	0
Cisco	207.218.140.64	0	0	0
Cisco2900XL	207.218.140.156	0	0	0
CiscoAG	207.218.140.155	0	0	0
CiscoSwitch.netinst.com	207.218.140.150	0	0	0
D1	207.218.140.131	0	0	0
d2.networkinstruments.com	207.218.140.253	0	0	0
Dell-3024	207.218.140.67	0	0	0
DS OFFICE PROCURVE	207.218.140.24	0	0	0
ds-bu-server	207.218.140.22	0	0	0
EX1	207.218.141.1	0	0	1
JBD039506312	207.218.141.47	0	0	1

Polling starts in 30 seconds...

