Network Management Outsourcing Services RFI Response

Confidential

Presented To:

Bruce Boardman
Machinery Hall
Room 001
Syracuse, NY 13244
bboardman@nwc.com
516-448-3772

Presented By:

Andrew Kramer
VP, Sales
PerformanceIT, Inc.
500 Sugar Mill Road
Suite 245A
Atlanta, GA 30350
Office: 678-323-1304
Fax: 678-323-1315
akramer@performanceit.com

PerformanceIT

Table of Contents

1 Executive Summary

1.1 Business Challenge

To put in place a robust, proactive network management outsourced services within budgetary confines. Concurrently, uptime and service level metrics need to be established to improve reliability, maximize performance, and achieve disaster protection. This should be accomplished without impacting the TacDoh's IT team, allowing them to focus on strategic projects.

"A strategic collaboration with PerformanceIT is an alternative approach that offers an almost immediate return on investment (ROI), accelerated productivity, and scalability to the demands of the enterprise".

A further dimension of the business challenge is the double imperative to satisfy escalating user expectations of technology beside the competing demands from management to increase productivity and boost service levels while simultaneously reducing costs or at a minimum, holding them steady.

In such an environment it is almost inevitable that resources should be stretched thinly, allocated to the most urgent of projects and to the regular daily containment of fires that break out in Information Technology departments everywhere.

For line IT managers caught in the cross hairs of this conundrum, the challenge is to balance the demands of these two distinct and often competing interests.

Proactive maintenance and continual real-time monitoring is difficult with current staffing levels. The cost of additional personnel is prohibitively expensive in the long term. In the short term it is burdensome and often results in additional work for existing over-extended staff. It is this same over-extended staff that is most commonly called upon to provide help with training and orientation of new employees, further impacting overall performance. When some of these new hires leave or become otherwise unavailable, the whole process begins again.

1.2 Strategic Collaboration: PerformanceIT IT Managed Services

A strategic collaboration with PerformanceIT is an alternative approach that offers an almost immediate return on investment (ROI), accelerated productivity, and scalability to the demands of the enterprise.

Collaboration delivers the integration of an experienced team of network, system, and database administrators that provide remote monitoring, maintenance and management of TacDoh's network infrastructure including their LAN, WAN, servers, databases, operating systems, and applications.

The result is improved effectiveness, efficiency, and agility based upon IT best-practices. It frees existing IT staff to concentrate on the projects and tasks that are strategic to long-term benefits.

A strategic use of resources creates a synergistic alignment within the IT department and serves as an example of sourcing intelligently from the external market. Additionally, it can be a vital part of maintaining the overall technical platform and the service delivery mechanism.

The strategic collaboration with PerformanceIT provides:

· 24 x 7 x 365 coverage	Dedicated, round-the-clock support teams replace outdated, reactive, ineffective on-call support methods.
· Rapid implementation	Standard installation is typically completed in less than 5 days (50 devices/day), delivering immediate, fully certified engineer response and repairs in less than one hour.
· Comprehensive monitoring	Includes state-of-the art monitoring hardware/software, eliminating the need for costly/complex monitoring software products. The solution eliminates costly, often failed implementation and associated risks.
· Centralized support	Problems are isolated the appropriate source (application, network, OS, database, user), reducing the need for multiple support agreements and finger-pointing among support providers or multiple vendors.
· Dedicated skilled administrators	Supplies crucial skill sets for a fraction of the cost of hiring additional staff or consultants.
· Augmented staff impact	Improves the effectiveness of IT staff by performing continuous critical system monitoring, maintenance, and management and proactively fixing problems before they threaten performance and availability.
· Maximized availability	Maximizes availability and prevents unplanned downtime. Prevention of a single outage can often pay for the service many times over.
· Improved focus	Frees existing IT resources for more strategic initiatives.
· Low total cost of ownership (TCO)	Delivers lower TCO with fixed and predictable support costs.
· Minimized staff turnover	Prevents headaches associated with staff turnover and lost knowledge.
· Enhanced job satisfaction	Aids in fostering overall job satisfaction with existing IT team and promotes job retention programs.

Ongoing service will be 24x7x365 and all alarm notifications are transmitted instantly to PerformanceIT's Support Operations Center where the SOC team responds to problems immediately and performs proactive maintenance. Real-time trouble tickets are generated with agreed upon service levels in place.

Real time performance reports are available on line. In addition, management is guided by wide ranging monthly reports and statistics in areas such as capacity planning, and forecasting. A recommendations summary lists action items for improving network performance, server operation and upgrades.

The Three Ms guide the Support Service Level Agreement with the customer:

· Monitoring	Knowing network and application status, monitoring of all critical parameters, and notifying engineers of events and threshold violations.
· Maintenance	Engineer response to events, continuous performance tuning, rapid fault management, and prevention of problems before costly outages or threats to performance can occur.
· Management	As noted above, a comprehensive array of web-based reports, viewable by management anytime, anywhere, combined with data collection, expert analysis, forecasting, capacity planning, and one-stop support for handling issues with multiple vendors.

1.3 Cost Justification

In considering projects of this kind, elaborate justifications must often be constructed to satisfy the demands of senior IT and finance management. Fortunately, the subscription nature of PerformanceIT managed hosting services make the analysis straightforward: At its highest level, effectively three engineers are available round the clock, 365 days a year at an annual cost of less than one administrator.

ROI analysis tells us certain things, such as: Whether to make an investment, which investment options to pursue, and expected financial outcomes. These outcomes are only valid if four conditions are true: 1. The expected functional benefits are attainable; 2. the model itself is technically sound; 3. the investment costs are accurate, and 4. the options presented are in alignment with corporate and functional strategic plans.

The answers to these questions are clear: For a small investment, the day-to-day tasks associated with LAN/WAN/Server management are strategically sourced - freeing in-house IT staff to work on critical projects. Savings are significant, availability and productivity for users is maximized, and the IT environment is stabilized.

1.4 Implementation Considerations

The benefits of this proposed project implementation are clear and many other organizations are yielding tremendous value from similar installations. There are a number of challenges to overcome to ensure this value, including the employment of the correct project management disciplines to reduce risks and ensure on time and on budget delivery.

Best practices must be employed. Chief among these is the clear delineation of scope and objectives. This roadmap prevents the focusing on non-value or non-critical value added work.

Traditional ROI methods can be very useful in comparing benefits to costs. However, the risk in not undertaking projects in a timely manner can often go uncaptured. A full analysis would reveal the cost of capital employed in staff undertaking non-strategic ongoing activity.

PerformanceIT's proposal for a strategic partnership is an example of an economic value add with minimal downside risk.

1.5 Service Level Agreement With Refundable Credits

PerformanceIT provides you with a simple, no-nonsense Service Level Agreement (SLA). If we fail, we owe you a refund, it is that simple. Further, PerformanceIT's SLA places no restrictions on your choice of hardware or software and asks for no specific controls over your environment. As partners, we believe that our interests our mutually aligned for maximized availability and performance. We trust in our TacDoh's ability to make the right decisions regarding their infrastructure with our guidance. This type of flexibility and trust is virtually unheard of in our industry.

1.6 No Questions Asked Cancellation

One of our core mission statements is as follows: "Every second that information systems are unavailable, money is needlessly lost and important customer relationships are damaged. We must keep our customers' systems always on, always up." If we fail in our mission, we expect to lose our customers' confidence. We therefore provide a no-questions-asked cancellation policy with 30-days written notice for any of our services.

2 Solution Summary

2.1 Methodology and Implementation

PerformanceIT will provide 24x7 monitoring of TacDoh's IT infrastructure by implementing our proprietary ProIT software and ProIT Network Management Station (ProIT NMS) at TacDoh's main data center. The implementation includes:

- † Installation of the ProIT NMS on the Client LAN/Configuration and tuning of the ProIT agents
- † Configuration of secure remote access to the ProIT NMS via VPN and SSH
- † Installation of a standard phone line (POTS) for failover and redundancy

2.2 ProIT Network Management Station (ProIT NMS) and Management Center

The ProIT NMS is a 1U (1.75 inch high) rack mountable Dell Model 1650 server running a fine tuned Red Hat 7.2 Linux kernel, PerformanceIT's ProIT v2.5 software, and a Cisco VPN client. PerformanceIT's ProIT NMS serves multiple purposes, including:

- † Collecting and logging alarms, events, and performance statistics
- † Providing secure access to the Client network for out of band management purposes
- † Providing the secure gateway for the delivery of alarms/events to the PerformanceIT NOC.
- † Providing a management and reporting portal for the client to view alarms/events, network performance, and health data Performance and alarm data are captured and presented in near real time.

2.3 ProIT Customer Center

The ProIT Customer Center (ProIT CC) is viewable via any browser by logging in at http://www.PerformanceIT.com. Within this portal, the client can achieve any of the following tasks:

- † Create, view and search all trouble-tickets and reports
- † Create and change Break/Fix Policy, Escalation Policy, Custom Monitoring Tasks, Authorization Limits, client contact information

2.4 Seamless Collaboration with TacDoh Staff

describe how the MSP will work to bridge the gap between systems and network management with tools and procedures that will be provided to the internal IT staff.

3 RFI Specific Requirements

3.1 General Reporting, Report Distribution, Rights

TacDoh Requirement: *Reports are needed by store, warehouse and corporate user. Their differing needs require access that ranges from local store to overall business delivery tracking. TacDoh IT wants to control access while delegating much of the responsibility for user access configuration to each business constituency. Ideally, this will include report viewing, running, creation and definition*.

The ideal report distribution will provide for online access and local report printing. It will also offer a security and access model that can be distributed and delegated. This would for example allow corporate to delegate and distribute report access and creation to each regional warehouse management team. Who could then distribute and delegate access to specific store staffs or groups of stores.

Finally if you offer ad hoc report creation, definition, or writing, please specify in detail the features available, and costs associated with each.

PerformanceIT Solution: ProIT limits access and functionality based on login roles. PerformanceIT will create accounts and assign them to TacDoh employees based on their access needs and role. ProIT does provide ad hoc report creation at no extra cost. The following table illustrates the differences between the Primary Roles:

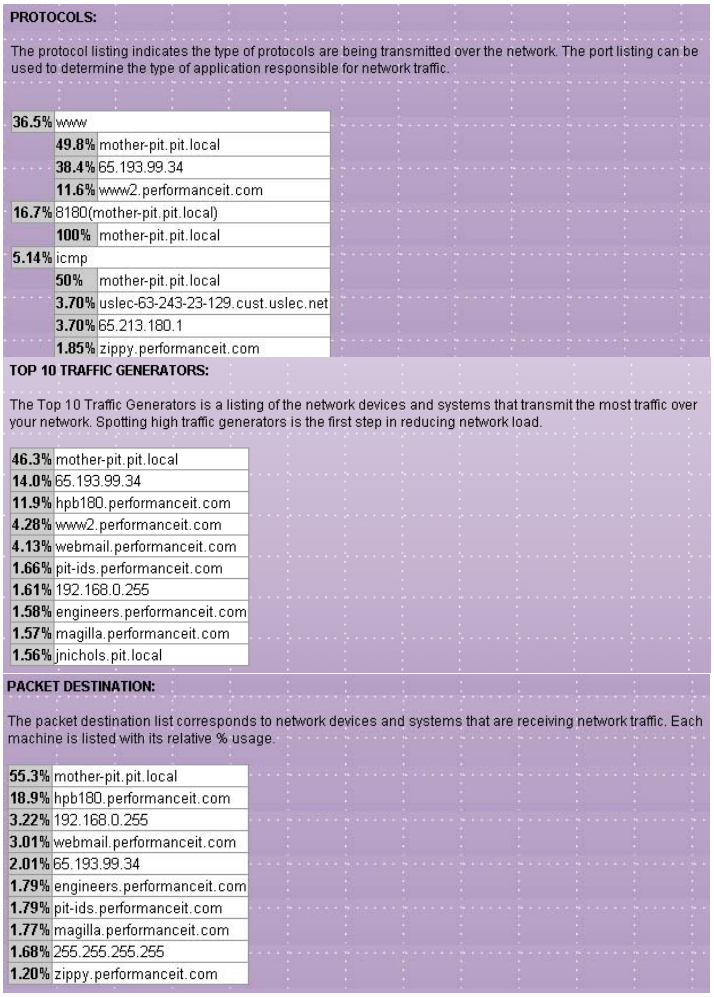
	Customer	Partner	Support	Manager	Administrator
Account Maintenance Tab (managed accounts)	no	no	no	no	**YES**
Tools Tab (diagnostic and remote scripts)	no	no	**YES**	**YES**	**YES**
Alarms Tab	**YES**	**YES**	**YES**	**YES**	**YES**
View Network Map	**YES**	**YES**	**YES**	**YES**	**YES**
Configure Network Map	no	no	**YES**	**YES**	**YES**
View Active Alarms	**YES**	**YES**	**YES**	**YES**	**YES**
Acknowledge/Clear Alarms	no	no	**YES**	**YES**	**YES**
View All Alarms	**YES**	**YES**	**YES**	**YES**	**YES**
Reports Tab (all reports)	**YES**	**YES**	**YES**	**YES**	**YES**
Analysis and Planning Tab (all tools)	**YES**	**YES**	**YES**	**YES**	**YES**
System Maintenance Tab	**YES**	**YES**	**YES**	**YES**	**YES**
Configure Managed Objects	no	no	**YES**	**YES**	**YES**
View Managed Objects	**YES**	**YES**	**YES**	**YES**	**YES**
View ETAs	**YES**	**YES**	**YES**	**YES**	**YES**
Modify ETAs	**YES**	**YES**	**YES**	**YES**	**YES**
Schedule Tasks	no	no	**YES**	**YES**	**YES**
Schedule Temporary Notification Blackouts	**YES**	**YES**	**YES**	**YES**	**YES**
Create and Change Base ETAs	no	no	no	no	**YES**

3.2 Standard Reports

TacDoh Requirement: *Standard reports should be available on a by store, by region, and overall network basis. The data elements should include Top 10 Applications by bandwidth, TopN Talkers, Utilization, Errors, Through put and availability. Historical Averages, minimums, maximums and 95 percentile overlays would be useful.*

PerformanceIT Solution: The reports mentioned above are available within ProIT as follows:

Figure 1 Top 10 Application By Bandwidth & TopN Talkers: ProIT NPA Report



PROTOCOLS:

The protocol listing indicates the type of protocols are being transmitted over the network. The port listing can be used to determine the type of application responsible for network traffic.

36.5%	www
49.8%	mother-pit.pit.local
38.4%	65.193.99.34
11.6%	www2.performanceit.com
16.7%	8180(mother-pit.pit.local)
100%	mother-pit.pit.local
5.14%	icmp
50%	mother-pit.pit.local
3.70%	uslec-63-243-23-129.cust.uslec.net
3.70%	65.213.180.1
1.85%	zippy.performanceit.com

TOP 10 TRAFFIC GENERATORS:

The Top 10 Traffic Generators is a listing of the network devices and systems that transmit the most traffic over your network. Spotting high traffic generators is the first step in reducing network load.

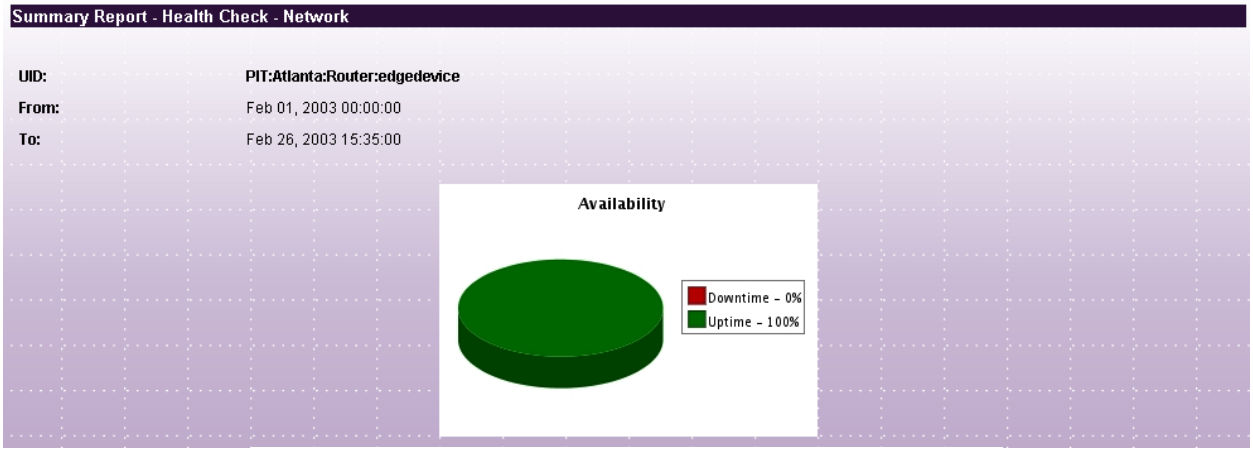
46.3%	mother-pit.pit.local
14.0%	65.193.99.34
11.9%	hpb180.performanceit.com
4.28%	www2.performanceit.com
4.13%	webmail.performanceit.com
1.66%	pit-ids.performanceit.com
1.61%	192.168.0.255
1.58%	engineers.performanceit.com
1.57%	magilla.performanceit.com
1.56%	jnichols.pit.local

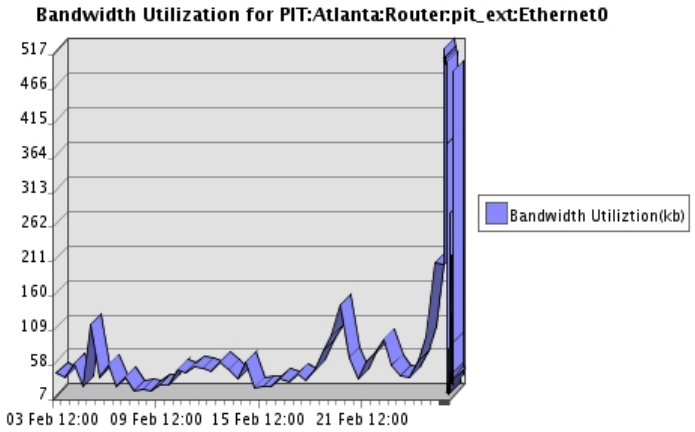
PACKET DESTINATION:

The packet destination list corresponds to network devices and systems that are receiving network traffic. Each machine is listed with its relative % usage.

55.3%	mother-pit.pit.local
18.9%	hpb180.performanceit.com
3.22%	192.168.0.255
3.01%	webmail.performanceit.com
2.01%	65.193.99.34
1.79%	engineers.performanceit.com
1.79%	pit-ids.performanceit.com
1.77%	magilla.performanceit.com
1.68%	255.255.255.255
1.20%	zippy.performanceit.com

Figure 2 Utilization, Errors, Throughput and availability: HealthCheck Report





Alarm and Log Summary

	Event				
	Critical	Major	Minor	Warning	Information
Alarms:	1	0	0	0	0
Log events:	0	0	0	0	0

Alarms List (partial)

Time	Severity	Synopsis

Monitored ETAs

ETA ID	Event		Time Frame (s)	Threshold	Pattern	Occurences	Enabled
	Category	Name					
CISCO 1000	Log	Critical Router Error	0		-[012]-	1	Yes
CISCO 2000	Log	Data Link Error	60		LINK-3-UPDOWN	20	Yes
CISCO 2001	Log	Enhanced Interior Gateway Protocol Errors	60		DUAL-3-SIA	5	Yes
CISCO 2002	Log	Data-Link Switching Error	60		DLSW-3-	5	Yes
CISCO 2003	Log	Serial Tunneling Errors	5		STUN-3-	1	Yes
CISCO 2004	Log	Remote Source-Route Bridging Error	60		RSRB-3-	2	Yes
LANWAN 1000	Network	Interface Down	0	=1			Yes
LANWAN 1001	Network	Port Unreachable	60	=1			Yes
LANWAN 2000	Network	% Interface Utilization	900	>70			Yes
LANWAN 2001	Network	% Interface Memory Utilization	1800	>70			Yes

Figure 3 Historical Averages: Trend Analysis Report & Event Correlation Graphs

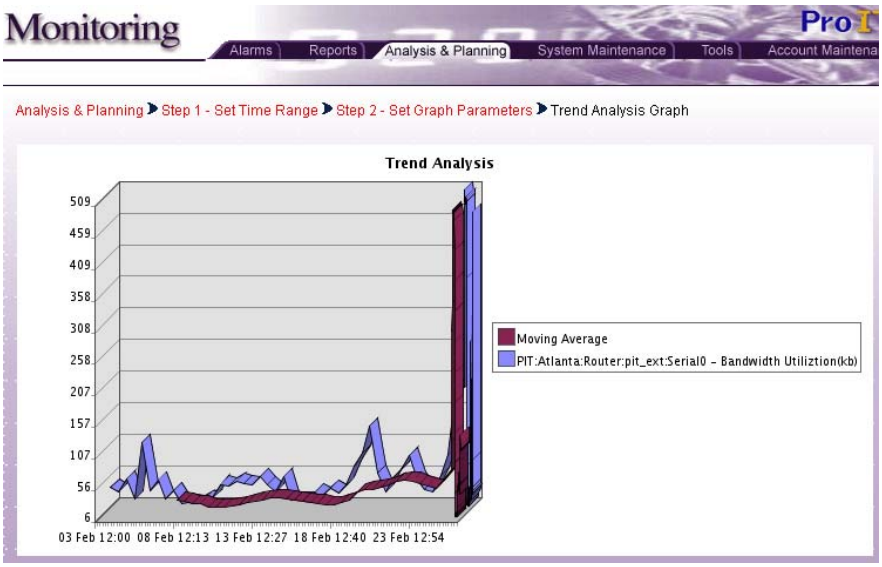
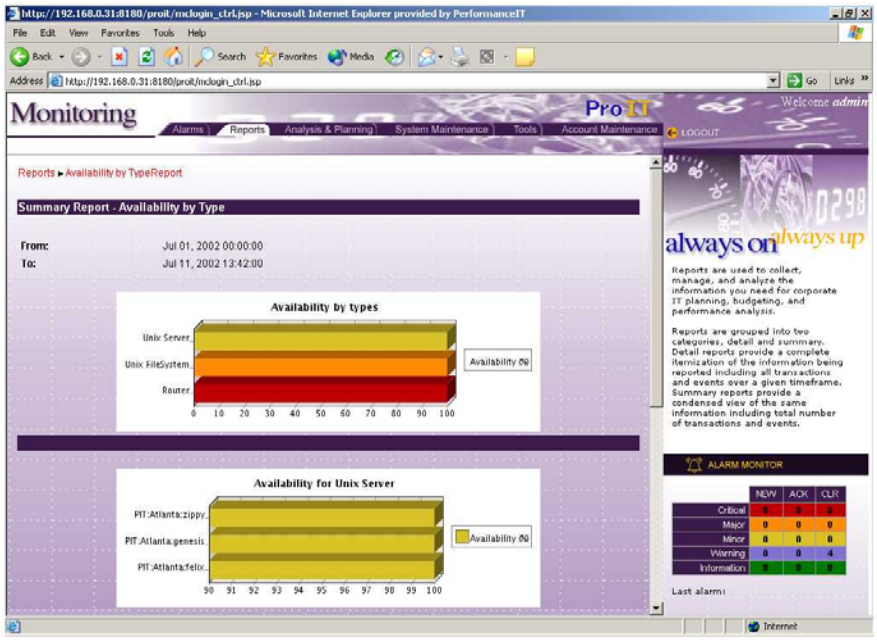


Figure 4 Availability Report



3.3 Application Flow Performance

TacDoh Requirement: *Application flow performance data is only available from the Adtran CPE FRADS. If you don't collect from that data source, but do offer alternative transactional analysis, please propose those solutions you feel appropriate. Also please break out each proposal separately, in order to clearly identify all of the cost associated.*

PerformanceIT Solution:

3.4 Sales Tracking Integration

TacDoh Requirement: *Response times are fed to an in-house application, TacDoh Mixer, which tracks POS activity and "SureWeKnowU" access. Currently this is an XML data feed. The data provided from the network management application to TacDoh Mixer include each stores local server's CPU and Memory usage and each store's network latency, utilization and transactional flow analysis split between "SureWeKnowU" traffic and POS traffic.*

Please specify if you are able to support this data feed and any additional cost.

PerformanceIT Solution: PerformanceIT's ProIT NMS has a full, flexible XML API and can also send/receive SNMP traps. Integration with the TacDoh Mixer application would be a customization that is anticipated to take three development days at a total cost of $4,500.00.

3.5 SLA Reporting

TacDoh Requirement A: SLA threshold violations and near violations need to be reported, as well as flagged with an e-mail notification. Ideally, this will provide from a configurable list, management of which can be delegated and distributed.

TacDoh Requirement B: Service levels include the WAN and local infrastructure at each store and warehouse distribution center. It is important that the network management solution encompass and manage all provider service levels. In addition to monitoring, it should include audit with provider, and status of ongoing audits and billing disputes with each WAN circuit provider. If this level of management is not available please indicate what interaction with WAN providers is possible. If there are separate costs associated with any WAN provider management please indicate what those are.

PerformanceIT Solution A: Advanced Notification and Escalation Engine

Many monitoring products can email, page, or send alerts to PDAs or other wireless devices and ProIT is no exception. The real challenge is to provide an intelligent way to decide *which* events get sent to *which* individuals at *what* time of the day or night.

ProIT's flexible notification features allow service providers or enterprise users the ability to dynamically assign and route events and tickets to specific people or teams, based on specified criteria, and at flexible times of the day or night.

Creating these rules can be achieved in either the ProIT Management Center or in the Customer Center in seconds with just a few clicks of the mouse.

Figure 5 Alarm Notification Rule Interface

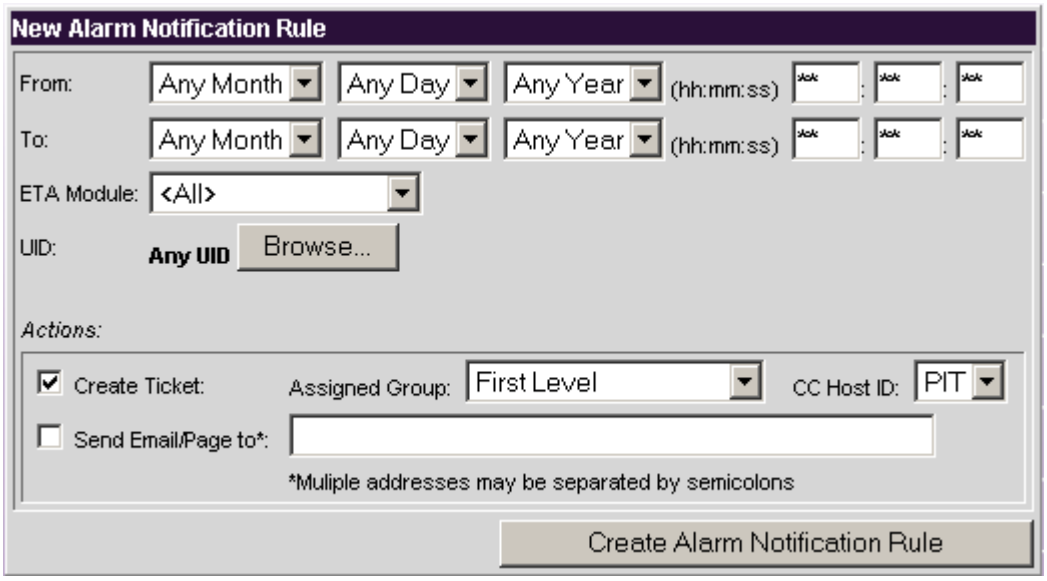
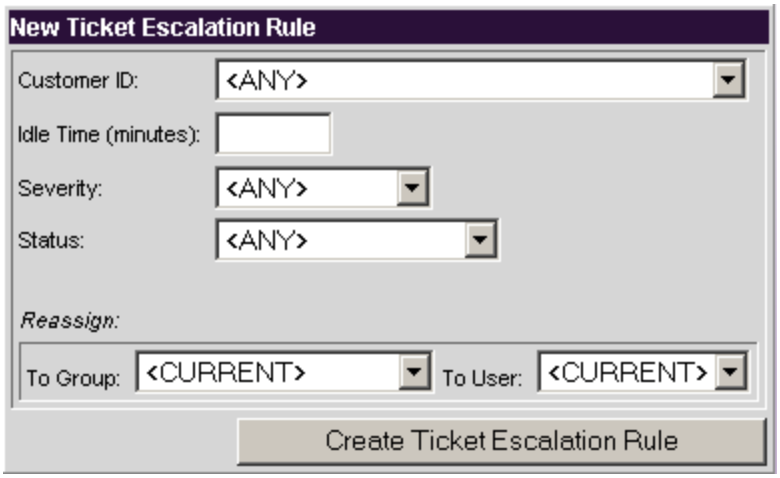


Figure 6 Ticket Escalation Rule Interface



PerformanceIT Solution B: Single Point of Responsibility, Full Third-Party Support

TacDoh will agree, and if necessary, obtain vendor's consent, to permit PerformanceIT to act as TacDoh's agent under the maintenance and/or service agreement(s). An addendum to this document will set out TacDoh Service agreements whereby PerformanceIT may contact a vendor on TacDoh's behalf under TacDoh's maintenance agreement with that vendor. TacDoh remains responsible for payment and renewal of the service agreements covering TacDoh hardware, software, and services.

In the event of a fault requiring maintenance or service covered under the respective vendor contract, PerformanceIT will act on the TacDoh's behalf and follow all processes and procedures set forth in those contracts to resolve the issue. PerformanceIT will open cases with respective vendors under those contracts and use best efforts to follow the issue to successful resolution with the third party vendor, specifically excluding legal actions or problems deemed as excluded from the maintenance contracts by the vendor(s).

3.6 Circuit Billing

TacDoh Requirement: *WAN payments will be done by TacDoh corporate accounting, but provisioning and WAN billing audits are to be outsourced. Network CIR, burst, and utilization need to be correlated to billing reports from WAN providers. These reports should be audited for accuracy and flagged where billing reimbursement is required. New stores come online regularly, usually with three month's notice.*

PerformanceIT Solution: PerformanceIT has not traditionally provided this service in the context of its outsourced network management services. The ProIT software provided would generate the reports and statistics needed to achieve such an audit. PerformanceIT can assume this accounting role as an optional service.

3.7 Performance Metrics

TacDoh Requirements:

- Monitoring is currently tracking minimum, maximum, average and 95th percentile for the following gathered on a 5-minute basis:
- In and out octets, values and percentage of utilization of every interface
- Errors values and as percentage of packets for every interface
- CPU utilization on every branch and warehouse server via HOST MIB
- Memory utilization of every branch and warehouse server via HOST MIB
- Disk-space utilization for every server via HOST MIB

PerformanceIT Solution: ProIT Event-Threshold-Action Modules, Built-in Best-Practices

PerformanceIT developed Event-Threshold-Action Modules as a way to standardize, automate, and improve the management of its diverse customers' IT infrastructures. Developed over six years, PerformanceIT established a "Top 25" best-practices approach to monitoring systems, devices, and applications. ProIT provides monitoring for this base list of important metrics and intelligent thresholds out of the box. After a device is auto-discovered by ProIT, an ETA Module is automatically applied.

Each ETA represents an event, its intelligent threshold, and the automated or recommended course of action for that event. ETAs are easily added or modified via the ProIT Management Center. ProIT monitors numerous more valuable performance metrics than are available via SNMP and HOST MIB. ProIT can be configured for obtaining those limited stats, though our recommendation is the use of ProIT ETAs for more in-depth monitoring. The following is a sample of the ETA Groups (a subset of an ETA Module) would be applied to meet the requirements:

Figure 7 SNMP ETA Group

Base ETA ID	Event		Threshold	
	Category	Name		
SNMP 1000	SNMP	% Input Errors	timethresh (>=50)	
SNMP 1001	SNMP	% Output Errors	timethresh (>=50)	
SNMP 1002	SNMP	% Input Discards	timethresh (>=50)	
SNMP 1003	SNMP	% Output Discards	timethresh (>=50)	
SNMP 2000	SNMP	% Interface Utilization	timethresh (>=75)	

Figure 8 Windows Server Performance Metrics and Disk Groups

Base ETA ID	Event		Threshold	
	Category	Name		
Disk 1000	Disk	% Utilization	timethresh (>=80)	
Disk 2000	Disk	Avg. Disk Queue Length	timethresh (>5)	
Disk 3000	Disk	Available Kb	timethresh (<200000)	

Base ETA ID	Event		Threshold	
	Category	Name		
NT 3009	Memory	Pages/Sec	timethresh (>20)	
NT 3010	Memory	Page Faults/sec	timethresh (>40)	
NT 3011	Swap	% Swap Utilization	timethresh (>50)	
NT 3012	Network	% Network Utilization	timethresh (>80)	
NT 3013	Network	Network Errors/sec	timethresh (>100)	
NT 3014	CPU	% Processor Time	timethresh (>70)	
NT 3015	System	Processor Queue Length	timethresh (>2)	
NT 4000	Memory	% Commited Bytes in Use	timethresh (>75)	

3.8 Bandwidth and Response Time

TacDoh Requirement: *The bandwidth and response time average, min, max and 95 percentile for the POS and "SureWeKnowU" applications. The "SureWeKnowU" application is all the browsing, mail, etc… coming from the wireless access points.*

PerformanceIT Solution: ProIT Service Threat Visualization Engine

The STV engine enables you to rapidly construct a logical application path (service group). PerformanceIT will create a service group for both the POS and SureWeKnowU applications.

Once constructed, ProIT establishes a performance baseline for each service group. ProIT will store the application performance data for each device (and each performance metric within each device) as a baseline. In just three more button clicks you can visualize which device (or component) is performing outside of the baseline and is causing a threat to performance.

Example:

The following example shows two devices within a Service Group and shows the actual vs. baseline performance of those devices and the performance metrics within those devices. In the example below, Memory is displayed as Purple (Warning state) as it is performing just one standard deviation away from the baseline. CPU Utilization on Felix is shown as yellow (Minor) because it is performing two standard deviations away from the baseline. You can surmise in this simple situation that a bottleneck and threat to performance may exist on the Felix server as it may be coming under increasing load.

Figure 9 Service Threat Visualization

PIT:Atlanta:delldc

Statistic		Average		Min.		Max.		Deviation			
Category	Name	Actual	Baseline	Actual	Baseline	Actual	Baseline	>1	>2	>3	>4
Memory	% Committed Bytes In Use	34.681	34.778	33	33	36	36	47	0	0	0
Memory	Page Faults/sec	510.389	525.382	6	6	3427	3427	10	0	0	0
Memory	Pages/sec	31.388	30.955	0	0	742.09	742.09	5	0	0	0
System	Processor Queue Length	0.188	0.194	0	0	12	12	0	0	0	0

PIT:Atlanta:felix

Statistic		Average		Min.		Max.		Deviation			
Category	Name	Actual	Baseline	Actual	Baseline	Actual	Baseline	>1	>2	>3	>4
Availability	Downtime	4294966528	4294966528	4294966528	4294966528	0	0	0	0	0	0
CPU	% Idle Time	99.81	99.843	98	98	100	100	0	28	0	0
CPU	Wait IO	0.048	0.03	0	0	1	1	0	0	0	0
Memory	Scan Rate	0	0	0	0	0	0	0	0	0	0
Process	Count	44.798	44.711	43	43	49	47	56	0	0	0
Swap	% Utilization	4	4	4	4	4	4	0	0	0	0
System	System Load	0.064	0.062	0	0	0.17	0.17	54	0	0	0
Users	Count	0	0	0	0	0	0	0	0	0	0

3.9 Data Storage Requirements

TacDoh Requirement: *Data needs to be saved in five-minute samples and kept for one year. The five-minute samples need to be rolled up to weekly, monthly and quarterly summaries. These roll up should be saved for five years. This is currently available via the corporate RDBMS.*

Describe data collection and retention periods available with your proposal. Please also indicate user access, and any associated additional functions and cost.

PerformanceIT Solution: ProIT NMS with ODBC connection to SQL Server

The ProIT NMS appliance ships complete with its own native database (PostgresSQL). For this requirement, the data storage capabilities of this hardware and database would not be sufficient. ProIT works seamlessly with a separate database server running Microsoft SQL 2000. With this solution, there is no theoretical limit to the retention period. An appropriately sized server with sufficient RAID disk is recommended. Annual statistics should be archived to tape or to an external NAS or SAN. There is no additional charge for this option assuming the client provides the server hardware, storage, and Microsoft Windows 2000 and SQL 2000 licensing.

3.10 On-site Support

TacDoh Requirement: *Network staffers have take general responsibility for on-site network troubleshooting and repair. Please indicate if you will be able to manage an onsite response.*

We realize that branch location will dictate cost. Use each of the warehouse distribution sites as centers from which dispatches would be figured, and indicate the costs associated. For example this might

include the distance in miles to a particular store attached to the Atlanta warehouse, as well as specific hours or response, and or guaranteed elapsed time until a tech will be onsite.

PerformanceIT Solution: Partnership with Fujitsu Technology Solutions

PerformanceIT provides integrated on-site support in partnership with Fujitsu Technology Solutions. PerformanceIT typically owns full responsibility and directs on-site support activities performed by either the client as “remote hands” or by Fujitsu support personnel.

3.11 Special Situations

Also please indicate the financial responsibility in each of the following outcomes:

Situation #1: *Not directly related to onsite communication, network or computing equipment, or cable plant - For example and act of God like lightning, or earthquake or building landlord powering drilling through power feed while remodeling adjacent store.*

PerformanceIT Response: PerformanceIT’s SLA ordinarily makes exclusions due to “circumstances that constitute a force majeure event.” That said, PerformanceIT would make no distinction at the time of the event and would engage in full ownership and fault management until problem resolution. For disasters and extenuating events such as earthquakes or floods, PerformanceIT would require a contract that integrates the services described herein into the client’s comprehensive Disaster Recovery and Business Continuity Plan where specific responsibilities and new charges would come into effect.

Situation #2: *No trouble found – For example when the dispatch arrives and test the trouble no longer exists or clears during testing.*

PerformanceIT Response: PerformanceIT must be able to prove to the customer’s satisfaction that the trouble indeed has been cleared and no longer exists. All activities related to this service are documented in the ProIT Customer Center online ticketing system in full view of the customer. In cases such as this, PerformanceIT may require that the customer provide approval before the ticket can be closed.

Situation #3: *WAN provider error – For example provider erroneously places disconnect on circuit.*

PerformanceIT Response: PerformanceIT NOC engineers would escalate the problem to the carrier and own the problem until it is successfully corrected. All documentation and proof required would be submitted to the carrier for the fasted repair time possible.

Please indicate any modular service level and cost associated in multiple options are available.

3.12 Management Applications

Currently, network management is supported through the following applications:

- *Adtran N-Form*
- *Cisco Works 2000*
- *HP OpenView Network Node Manager*
- *Concord Communication eHealth*

While primarily tools of the networking group, they are also used by help-desk, operations and systems personnel to support internal applications, systems and users. The cost reduction of these applications will help offset the outsourcing cost, but retraining costs need to be considered. Please indicate any network management tools that will be provided by you to the above groups, in support of internal applications, systems and users. Obviously, not having to re-learn tools is advantageous, but should that be a requirement, indicate training and facilities that will support remaining IT staff.

If there are additional modules or functionality, like special training classes, please indicate their cost separately.

PerformanceIT Response:

PerformanceIT expects that its ProIT Network Management Platform will replace HP OpenView Network Node Manager and Concord Communications' eHealth products, thereby eliminating the annual support and maintenance fees for both products. ProIT would integrate with CiscoWorks 2000 and Adtran N-Form to take advantage of advanced statistics and health metrics as well as leverage their element management capabilities.

ProIT was designed from the ground up to be easy to use, easy to deploy, easy to maintain, and work seamlessly between PerformanceIT as a service provider and an end-user client's internal support staff. Training for ProIT is $2,000 per student and can be completed in two business days.

4 Network Management Services Summary

As part of this proposal, PerformanceIT will perform network maintenance and management for the specified network devices. The network administration tasks that will be included as part of this service are detailed in the sections below.

4.1 Network Monitoring Overview

PerformanceIT will provide 24x7 monitoring of TacDoh's network infrastructure, utilizing its proprietary ProIT software. ProIT monitors and detects error messages/alarms directly from the devices via its comprehensive Full-5™-layer polling every 5 minutes (configurable). Upon any event, a fault identification process begins by using in-band and out-of-band diagnostic channels to isolate the cause of the problem. The PerformanceIT NOC will then open a trouble ticket, notify the client and work to rectify the situation.

4.2 Full-5™ Layer Network Event Detection (NED) and Methodology

ProIT's Full-5 Layer NED includes the following five (optionally six) event detection sources:

1. Polling of all configured IP addressable interfaces on a monitored device to test for basic network connectivity every 5 minutes (configurable). If the test fails, an "ifDown" event will be generated and delivered to the NOC staff to perform various troubleshooting steps.
2. Router Syslog Monitoring – PerformanceIT configures the logging facility on each device to log to the ProIT NMS. Regular expression based patterns are used to filter out meaningful messages and alarms are delivered to the NOC staff to perform various troubleshooting steps. The methodology functions as follows:
   - All defined level 0-2 messages are detected and result in a Critical alarm to the NOC staff.
   - All define level 3 messages are detected and result in a Warning alarm to the NOC staff.
   - All defined level 4 messages are detected and result in a Minor event that is logged for reporting purposes.
   - All level 5-7 messages are detected and result in an information-only event that is logged for reporting purposes.
3. TCP/UDP Port Monitoring: PerformanceIT monitors to ensure that a device is accepting connections for specified TCP or UDP ports.
4. SNMP Polling for RMON and MIB2 data. Via ProIT, PerformanceIT collects performance statistics via SNMP polling of the network devices.
5. SNMP Trap management. ProIT consolidates SNMP traps received from network devices into a consolidated log which is in turn monitored for alarm events which are categorized by severity.
6. Optionally, the ProIT Network Protocol Analysis module may be deployed to provide "sniffer" based information and monitoring capabilities which include: 1. top ten traffic generators (by IP or DNS), 2. top ten packet sources, 3, top ten traffic destinations, 4. total bandwidth utilization and 5. bandwidth utilization by protocol (application)

4.3 Base ETA Modules

The following ETA modules will be configured to monitor the critical events for TacDoh's infrastructure. Additional events can be added at any time.

Base ETA ID	Event		Threshold	
	Category	Name		
ROUTESCIENCE 2000	SNMP	Temp Violation	timethresh (=1)	
ROUTESCIENCE 2001	SNMP	Voltage Violation	timethresh (=1)	

Base ETA ID	Event		Threshold	
	Category	Name		
SNMP 1000	SNMP	% Input Errors	timethresh (>=50)	
SNMP 1001	SNMP	% Output Errors	timethresh (>=50)	
SNMP 1002	SNMP	% Input Discards	timethresh (>=50)	
SNMP 1003	SNMP	% Output Discards	timethresh (>=50)	
SNMP 2000	SNMP	% Interface Utilization	timethresh (>=75)	
SNMP 3000	SNMP	% Avg CPU Utilization	timethresh (>=95)	

Base ETA ID	Event		Threshold	
	Category	Name		
CISCO 1000	Log	Critical Router Error	timepat (1 times)	
CISCO 2000	Log	Data Link Error	timepat (20 times)	
CISCO 2001	Log	Enhanced Interior Gateway Protocol Errors	timepat (5 times)	
CISCO 2002	Log	Data-Link Switching Error	timepat (5 times)	
CISCO 2003	Log	Serial Tunneling Errors	timepat (1 times)	
CISCO 2004	Log	Remote Source-Route Bridging Error	timepat (2 times)	

Base ETA ID	Event		Threshold	
	Category	Name		
CISCO2600 2000	SNMP	Temperature Condition	timethresh (>100)	
CISCO2600 2001	SNMP	# Configuration Loss	timethresh (>50)	

Base ETA ID	Event		Threshold	
	Category	Name		
CISCO7200 2000	SNMP	Cisco Memory Pool Used	timethresh (>64000)	
CISCO7200 2001	SNMP	Cisco Memory Pool Free	timethresh (<10000)	
CISCO7200 2002	SNMP	Memory Pool Utilization	timethresh (>95)	
CISCO7200 2003	SNMP	% CPU Busy	timethresh (>95)	

Base ETA ID	Event		Threshold	
	Category	Name		
SYMBOL 2000	SNMP	Dialout Failures	timethresh (>100)	
SYMBOL 2001	SNMP	Answer Attempts	timethresh (>1)	
SYMBOL 2002	SNMP	Packets Sent Per Frequency	timethresh (>100)	
SYMBOL 2003	SNMP	Packets Recvd. Per Frequency	timethresh (>100)	
SYMBOL 2004	SNMP	CRC Errors	timethresh (>1000)	
SYMBOL 2005	SNMP	Duplicate Packets Received	timethresh (>100)	
SYMBOL 2006	SNMP	# Collisions	timethresh (>1000)	

Base ETA ID	Event		Threshold	
	Category	Name		
EXTREME 2000	SNMP	FCS/Alignment Error Packets	timethresh (>1000)	
EXTREME 2001	SNMP	Total Collisions	timethresh (>1000)	
EXTREME 2002	SNMP	Total Errors	timethresh (>1000)	
EXTREME 2003	SNMP	CPU Utilization	timethresh (>95)	
EXTREME 2004	SNMP	Max. CPU Utilization	timethresh (>=99)	
EXTREME 2005	SNMP	Overtemperature Sensor Status	timethresh (=1)	
EXTREME 2006	SNMP	Current Temperature(C)	timethresh (>100)	
EXTREME 2007	SNMP	External Redundant Power Alarm	timethresh (=1)	
EXTREME 2008	SNMP	Power Supply Alarm	timethresh (=1)	

4.4 Planning and Design

PerformanceIT engineers will help make sure the network configuration and design keep pace with TacDoh's enterprise network needs and perform Planning and Design tasks that are summarized into categories summarized in the following table. These tasks would be performed on a project oriented basis:

Table 1 Network Management: Planning and Design Tasks

Task Category	Description
Capacity Planning	Reviewing and analyzing bandwidth utilization statistics and determining LAN/WAN bandwidth requirements, CIR adjustments, etc. Monthly task.
Network Design	Performing quarterly review of the network design and making recommendations for optimized topology.
Network Baselining	Determining current network capabilities and performance levels. Performing quarterly comparisons against the baseline and feeding that data into capacity planning and analysis.
Interfacing with various departments	Working together with various internal departments to address concerns, craft project plans, and accept/implement change requests
Contingency Planning	Reviewing network design and faults for fault-tolerance, higher availability, and resiliency.
Configuration and testing	Determining appropriate standard configurations for production equipment and performing full battery of acceptance tests before rollout.

4.5 Implementation

PerformanceIT plans to provide full implementation service and support on a project-oriented basis for additions and expansions to the infrastructure. Tasks that would be included in these services are summarized in the following table:

Table 2 Network Management: Implementation Tasks

Task Category	Description
Installations	New equipment installations for the production network.
Project management	Managing the deployment of new kit and performing acceptance tests
Provisioning	Working with carriers to provision new bandwidth to the network

4.6 Operations

This section is the core of the proposed outtasked network management services. The services are summarized in the following table and in more detail the sections that follow:

Table 3 Network Management: Operations Tasks

Task Category	Description
Fault management	Handling all alarms, events, and trouble-tickets related to the covered network infrastructure. Performing root-cause analysis and problem resolution.
Carrier interfacing	Escalating WAN problems to carriers and owning problem until resolved.
Interdepartmental interfacing	Working with the internal support staff and departments to assure seamless services.
Configuration management	Performing configuration management, patches, and updates to all devices.
Performance management	Performing analysis and adjustments to optimize performance and throughput of the infrastructure.

4.6.1 Fault Management

PerformanceIT will manage the alarms, events, and trouble-tickets generated from the ProIT Network Management Platform as well as tickets created and sent manually by the client. Root cause analysis and appropriate repairs will be implemented using best-efforts and best practices for optimized mean-time-to-repair (MTTR). PerformanceIT will monitor the following items for hardware and software related issues, addressing both failure and diminished functionality for managed RSFW devices:

1. Physical interfaces using SNMP traps as well as more direct “show” and “debug” commands
2. Memory and processor utilization
3. (WAN) circuit availability

Routine reports will be generated based on the information gathered above as well as the information in the proceeding section, Performance Management.

4.6.2 Carrier Interfacing

From time to time, unplanned outages and events may require escalation of problems to the Carrier or other third-party source. PerformanceIT will own the problem until successfully resolved with appropriate documentation provided in the trouble-ticket.

4.6.3 Interdepartmental Interfacing

The outtasked services contemplated in this agreement are designed to reduce cost and improve results for TacDoh. To be successful, appropriate processes and technologies must be employed to create a true partnership with TacDoh’s internal staff. The ProIT NMS Management Center enables real-time collaboration among all support team members—both PerformanceIT personnel and TacDoh personnel. Via a browser, all members share the same view, control, and status of the managed infrastructure and can fine tune policies as-needed.

4.6.4 Configuration Management

PerformanceIT will adjust configurations, including changes in addressing, packet filtering, security and protocol support. PerformanceIT will inspect configurations on managed routers, switches, and firewalls (hereafter “RSFW”) to identify and document the following:

1. IOS or software/firmware version installed
2. System (software) configuration
3. All physical aspects, including, but not limited to, the following items: amount of Flash and DRAM, interface types, module specifications, and chassis serial numbers

PerformanceIT will prepare a network diagram(s) reflecting the network infrastructure discovered in steps one through three above. Backup copies of the IOS and system configuration files will be prepared and retained in a central location to allow for accelerated recovery in the event of corruption or failure occurring on any given managed RSFW device.

PerformanceIT will install and configure software upgrades where it is deemed necessary due to client needs regarding enhanced functionality and/or security concerns. Upgrades to router software are recommended and implemented to correct defects or to improve the performance, function or stability of the network. PerformanceIT maintains archived copies for router configurations to assist in the fault management process.

4.6.5 Performance Management

PerformanceIT maintains a complete set of important network information in the ProIT database. The most common information reviewed is for network availability and performance. Network availability is calculated and summarized and trended at month-end. Performance reports are updated monthly and provided in both detailed and summary formats. Additionally, a technical network map is kept current and available.

PerformanceIT will monitor and document the status of network circuits and their utilization. “Utilization” includes reporting on peak loads, apparent congestion (if any), and drops. To the extent that it is deemed appropriate, PerformanceIT will recommend and implement suggestions regarding the following for managed RSFW devices:

1. (WAN) Quality of Service , e.g., queuing/prioritizing certain types of network traffic on congested links
2. (WAN) Augmenting/reducing bandwidth, CIR, etc.
3. Load balancing, including configuration and optimization of the load balancer device

Before the ongoing, real-time analysis is started by PerformanceIT, an initial analysis of network responsiveness, congestion, etc., will be prepared to provide a “big picture” baseline for future reference. PerformanceIT will prepare revised “big picture” reports every three months, or as often necessary if the network undergoes a substantial change, e.g., additional sites being added, consolidation, merger, etc.

5 Network Security Management

5.1 Overview

Although not contemplated in the RFI, network security management is a crucial component of an effective network management strategy aligned with the business and availability goals for the infrastructure. PerformanceIT can provide integrated Enterprise Security Management (ESM) technology and services to augment those contemplated by the RFI to support the availability requirements set forth in the SLA. If chosen, PerformanceIT will inspect, document, recommend, and where necessary, implement changes with regard to security issues. This will include a review of the following items for managed RSFW devices:

1. Access-list and conduit configuration/application
2. Physical access control to RSFW devices, e.g., console access control
3. Password strength for various levels of access
4. SNMP community strings
5. Auditing of changes to RSFW configuration
6. VPN or other inbound connectivity not addressed in the preceding items
7. Firewall management. Monitor firewall for availability. Evaluate and process all rules, policy, and change requests to ensure security of protected network components.
8. Vulnerability Management: manage and schedule Qualys vulnerability scans to ensure security
9. Intrusion detection and threat remediation via the ProIT IDS appliance and integrated report portal.
10. Integrated security event monitoring of server, router, firewall, virus protection, and content filter event logs.

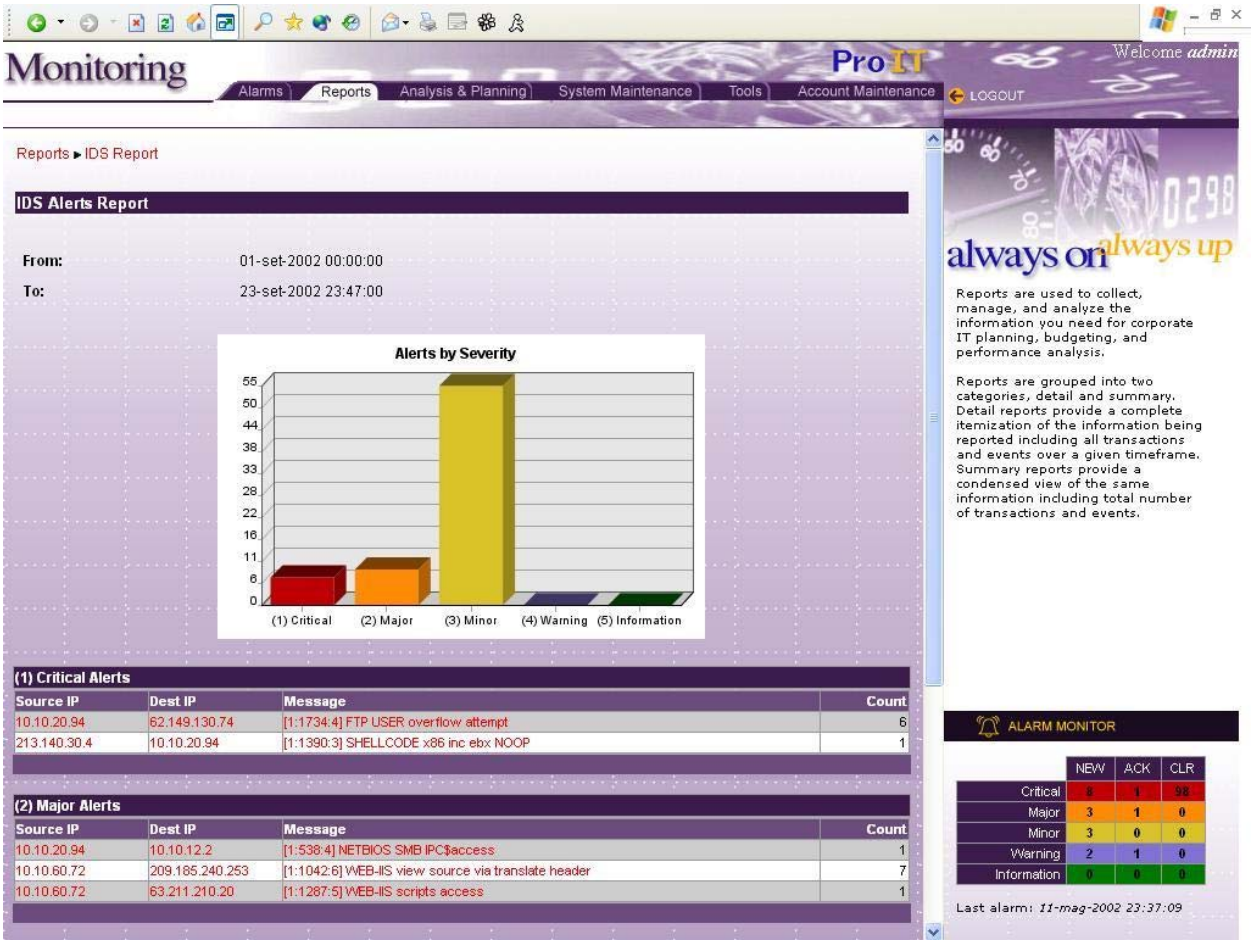
As part of the backup process noted in the prior section, access-lists and other software based protection components will be prepared and retained at a central location. While not strictly a function/responsibility of network infrastructure, PerformanceIT will inspect, document, and make recommendations regarding general application security, e.g., anti-virus software, e-mail attachment control, file transfer control, etc.

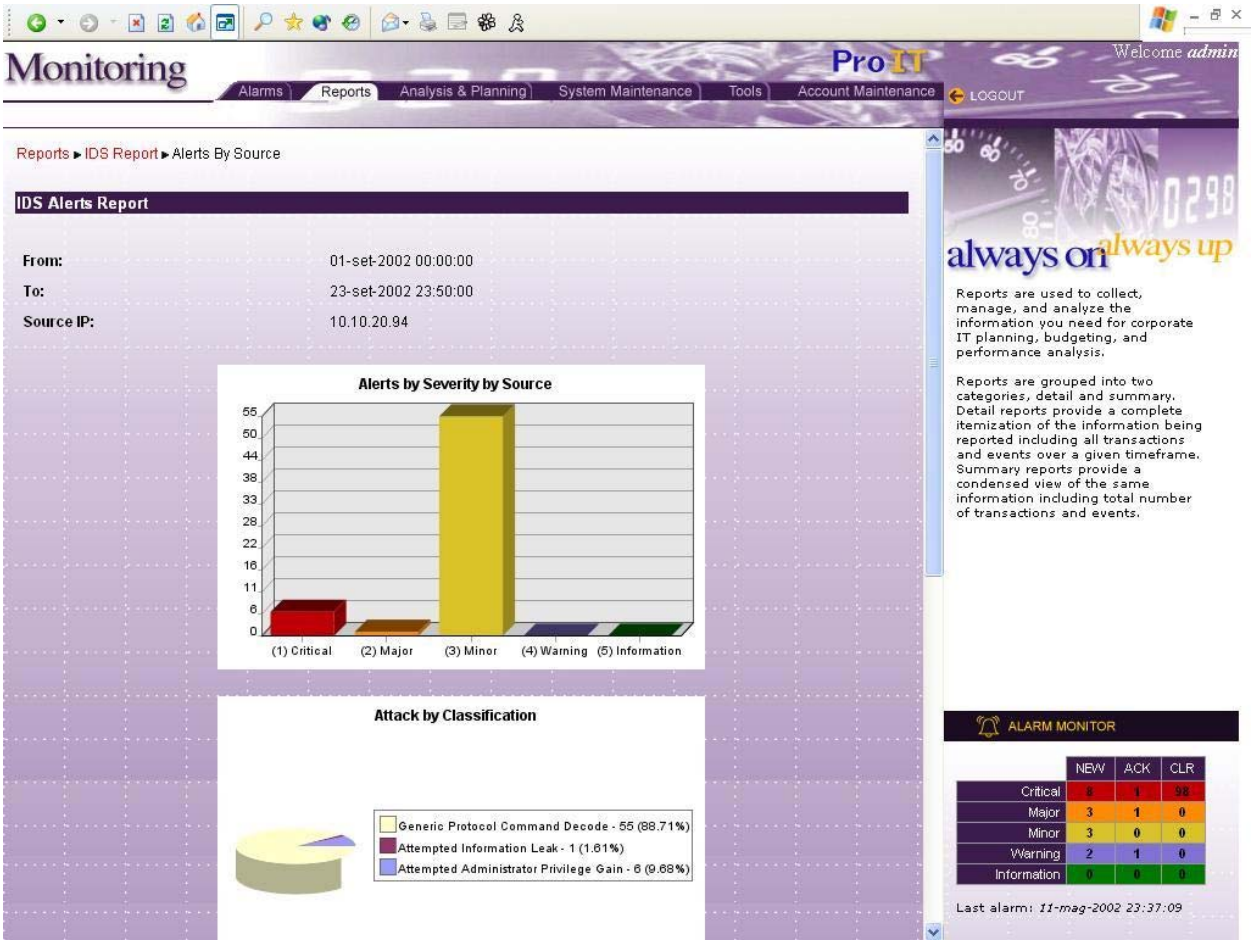
5.2 Incident Response Process

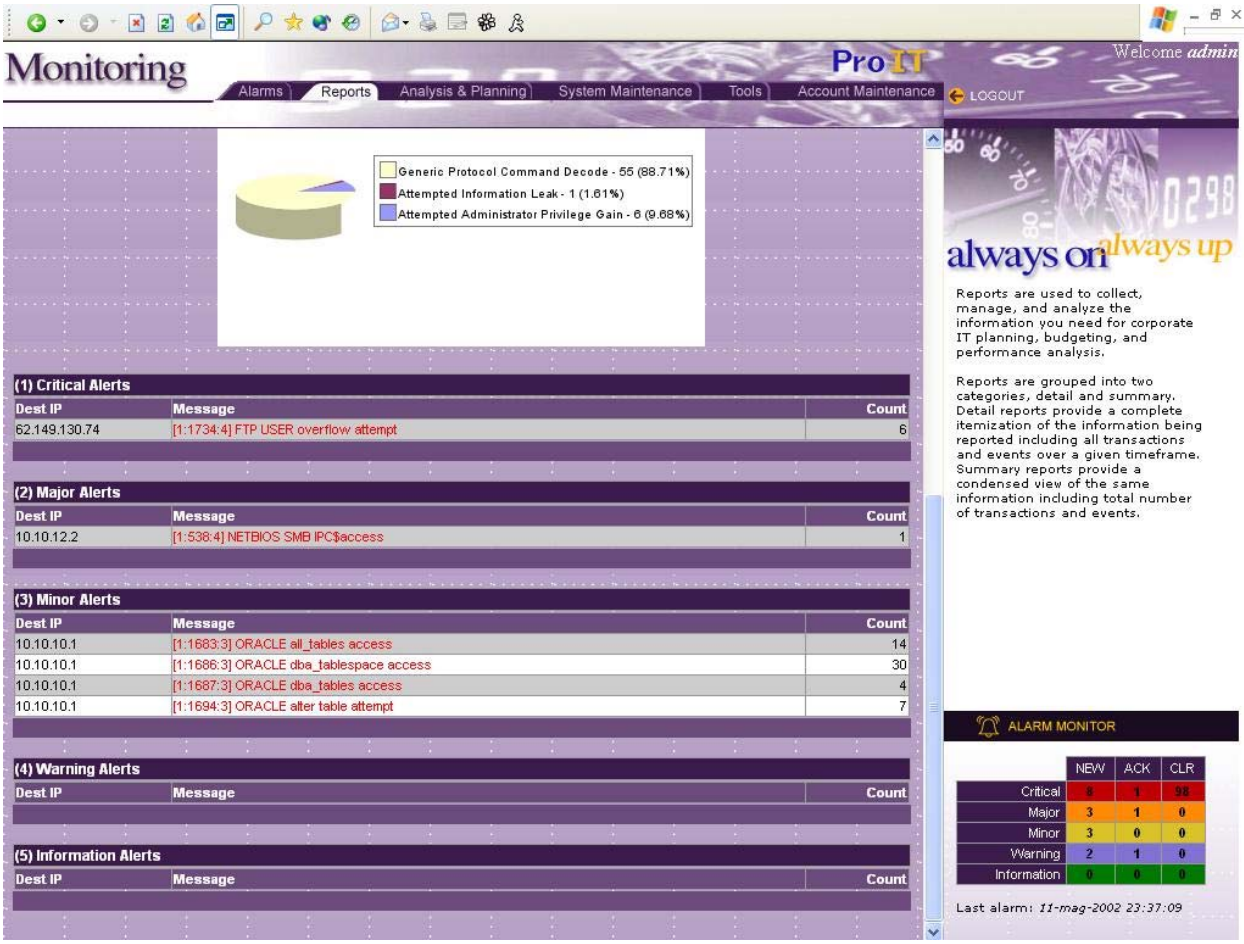
The PerformanceIT Security Incident Response Process is a standardized method of delivering high levels of service associated with the monitoring of systems included under the Managed Security Monitoring, Managed Intrusion Detection, and Managed Firewall services. After security events are aggregated and correlated by the ProIT technology and PerformanceIT security staff, they are categorized, prioritized, and responded to in a well-defined manner with all actions taken documented in the ProIT Customer Center.

5.3 Security Threat Analysis, Reporting, and Incident Response

The ProIT IDS appliance is linked to the security industry's best real-time databases for tracking ongoing threats, prioritization, and remediation procedures and tactics. In real-time, the ProIT IDS inspects network traffic and identifies attack signatures and prioritizes them based on industry expert rankings and information obtained from industry vulnerability lists such as the SecurityFocus (http://www.securityfocus.com) Vulnerability Database; WhiteHats.Org database, The National Infrastructure Protection Center (http://www.nipc.gov/), InfraGard (http://www.infragard.net/), and CERT (http://www.cert.org/). Automated links to the following industry sites are created so that PerformanceIT security engineers can perform the necessary research and remediation steps. If actions are required, they will be implemented as quickly and safely as best-practices allow: http://www.whitehats.org, http://www.securityfocus.com, http://www.cve.mitre.org.




Monitoring
ProIT
Welcome admin
Alarms
Reports
Analysis & Planning
System Maintenance
Tools
Account Maintenance
LOGOUT
Reports ▸ IDS Report ▸ Alerts By Source
IDS Alerts Report
From: 01-set-2002 00:00:00
To: 23-set-2002 23:50:00
Source IP: 10.10.20.94
Alerts by Severity by Source
55
50
44
38
33
28
22
16
11
6
0
(1) Critical
(2) Major
(3) Minor
(4) Warning
(5) Information
Attack by Classification
Generic Protocol Command Decode - 55 (88.71%)
Attempted Information Leak - 1 (1.61%)
Attempted Administrator Privilege Gain - 6 (9.68%)
always on always up
Reports are used to collect, manage, and analyze the information you need for corporate IT planning, budgeting, and performance analysis.
Reports are grouped into two categories, detail and summary. Detail reports provide a complete itemization of the information being reported including all transactions and events over a given timeframe. Summary reports provide a condensed view of the same information including total number of transactions and events.
ALARM MONITOR
NEW ACK CLR
Critical 8 1 98
Major 3 1 0
Minor 3 0 0
Warning 2 1 0
Information 0 0 0
Last alarm: 11-mag-2002 23:37:09

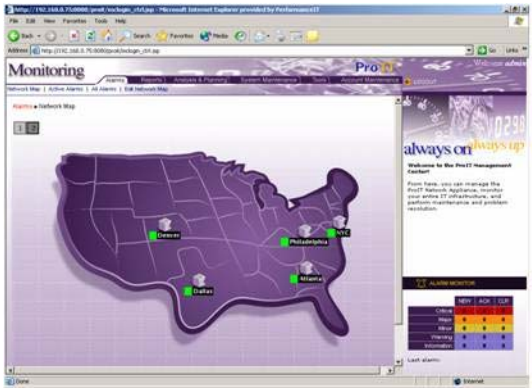

Monitoring
Alarms
Reports
Analysis & Planning
System Maintenance
Tools
Account Maintenance
ProIT
Welcome admin
LOGOUT
Generic Protocol Command Decode - 55 (88.71%)
Attempted Information Leak - 1 (1.61%)
Attempted Administrator Privilege Gain - 6 (9.68%)
always on
always up
Reports are used to collect, manage, and analyze the information you need for corporate IT planning, budgeting, and performance analysis.
Reports are grouped into two categories, detail and summary. Detail reports provide a complete itemization of the information being reported including all transactions and events over a given timeframe. Summary reports provide a condensed view of the same information including total number of transactions and events.
(1) Critical Alerts
Dest IP | Message | Count
62.149.130.74 | [1:1734:4] FTP USER overflow attempt | 6
(2) Major Alerts
Dest IP | Message | Count
10.10.12.2 | [1:538:4] NETBIOS SMB IPC$access | 1
(3) Minor Alerts
Dest IP | Message | Count
10.10.10.1 | [1:1683:3] ORACLE all_tables access | 14
10.10.10.1 | [1:1686:3] ORACLE dba_tablespace access | 30
10.10.10.1 | [1:1687:3] ORACLE dba_tables access | 4
10.10.10.1 | [1:1694:3] ORACLE alter table attempt | 7
(4) Warning Alerts
Dest IP | Message | Count
(5) Information Alerts
Dest IP | Message | Count
ALARM MONITOR
NEW | ACK | CLR
Critical 8 1 98
Major 3 1 0
Minor 3 0 0
Warning 2 1 0
Information 0 0 0
Last alarm: 11-mag-2002 23:37:09

6 Reporting Services

6.1 Alarm/Device Monitoring

Real-time alarm and device monitoring is provided directly to the TacDoh via the ProIT Management Center.

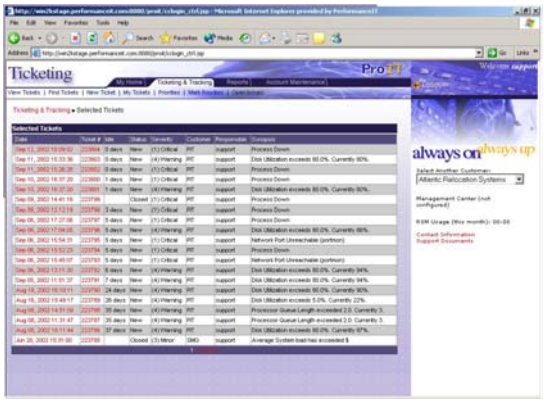
Figure 10 ProIT Management Center



6.2 Real-time Trouble-Tickets

Real-time trouble-tickets are provided to the TacDoh via the ProIT TacDoh Center.

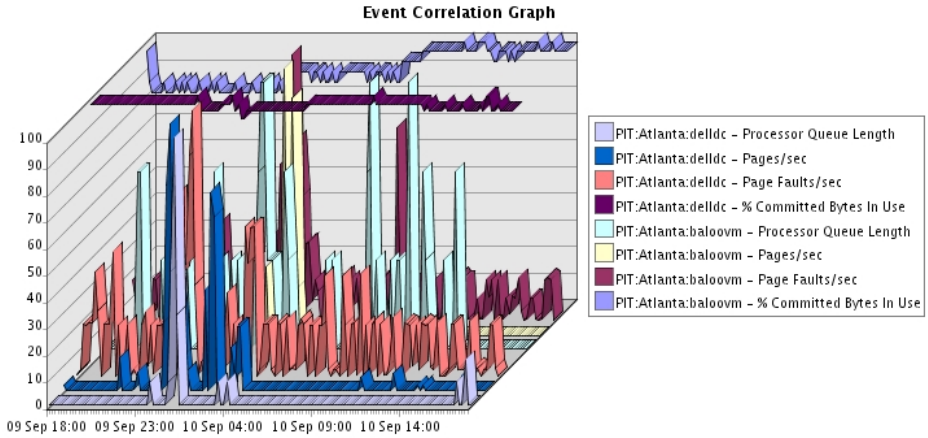
Figure 11 ProIT TacDoh Center



6.3 Performance Analysis and Capacity Planning Reports

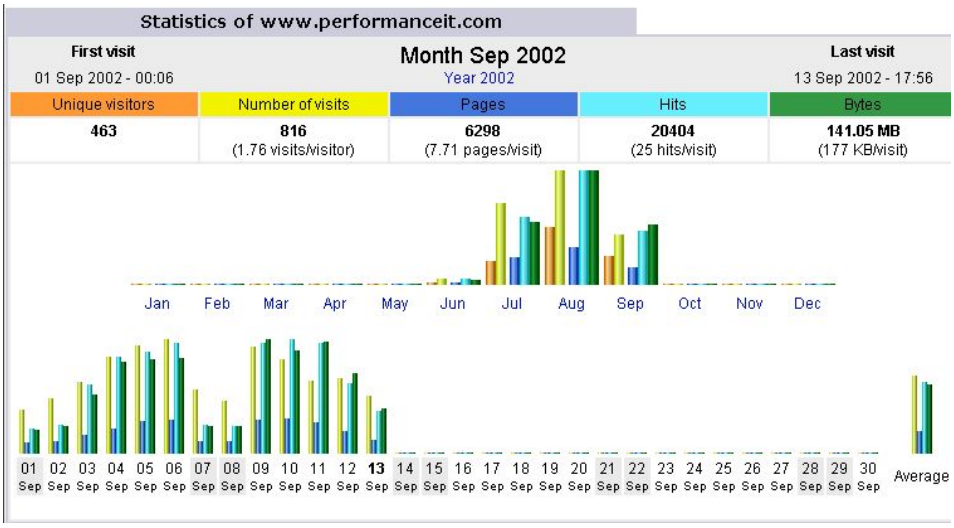
ProIT includes a robust reporting engine capable of reporting any metrics collected via the Management Center.

Figure 12 ProIT Management Center / Analysis & Planning Tab



6.4 Website Statistics: WebStats Module

The fully managed hosting service includes the configuration and implementation of the ProIT WebStats module for web server analysis.



The ProIT WebStats module provides the following useful and relevant web server and site statistics:

- Number of visits, unique visitors, and list of last visits,
- Days of week and Rush hours (pages, hits, kb for each hour and day of week),
- Domains/countries of hosts visitors (pages, hits, kb, 259 domains/countries detected),
- Authenticated users,
- Most often pages viewed and entry pages,
- File types,
- Web compression statistics (for mod_gzip),
- Browsers used (pages, hits, kb for each browser, each version, 78 browsers: Web, Wap, Media browsers...),
- OS used (pages, hits, kb for each OS, 28 OS detected),
- Visits of robots (258 robots detected),
- Search engines, keyphrases or keywords used to find your site (The 56 most famous search engines are detected like yahoo, google, altavista, etc...),
- HTTP errors (Page Not Found, ...),
- Analyzes Apache NCSA combined log files (XLF/ELF) or common (CLF), IIS log files (W3C), WebStar native log files and other web, proxy or wap servers log files).
- Supports unlimited log file size and split log files (for load balanced systems),
- Reverse DNS lookup during analysis

7 Third-Party Hardware and Software Support

7.1 Summary

TacDoh must have a maintenance agreement covering TacDoh Hardware and/or Software from the appropriate vendor. TacDoh will agree, and if necessary, obtain vendor's consent, to permit PerformanceIT to act as TacDoh's agent under the maintenance agreement(s). An addendum to this document will set out TacDoh Hardware and Software maintenance agreements whereby PerformanceIT may contact a vendor on TacDoh's behalf under TacDoh's maintenance agreement with that vendor. TacDoh remains responsible for payment and renewal of the maintenance agreements covering TacDoh Hardware and Software.

7.2 Process

In the event of a hardware or software fault requiring maintenance covered under the respective vendor maintenance contract, PerformanceIT will act on the TacDoh's behalf and follow all processes and procedures set forth in those contracts to resolve the issue. PerformanceIT will open cases with respective vendors under those contracts and use best efforts to follow the issue to successful resolution with the third party vendor, specifically excluding legal actions or problems deemed as excluded from the maintenance contracts by the vendor(s).

8 Network Infrastructure to be Managed

The following table represents the network infrastructure to be managed:

	Chicago	Newark	Atlanta	Branches
Equipment				
Cisco 2600 Router	0	0	0	300
Cisco 7200 Router	2	1	1	0
Cisco 6509 w MFRC	1	0	0	0
Extreme Summit24e2	20	0	0	300
Extreme Summit48i	10	0	0	0
Foundry FastIron Edge Switch 2402	0	5	5	0
Foundry FastIron Edge Switch 4802	0	5	5	0
Alcatel Omniswitch 6624	0	5	5	0
Route Science 3100 Path Control	1	1	1	0
Adtran IQ 710	0	0	0	300
Symbol 4131 AP	6	3	3	300
Total	40	20	20	1200
WAN Links				
T3	1	1	1	0
T1	1	1	1	0
FracT1	0	0	0	300

9 Service Level Agreement

9.1 Total Availability Definition

The total availability performance standard is 99.9%. Total site availability is defined as the amount of time each covered device was powered on and was available to users.

Formula: Total Availability % = Uptime/Schedule Uptime X 100

- Scheduled uptime: Total hours in the available time period which is defined as 24 hours a day, 7 days a week, less mutually scheduled downtime.
- Uptime = Scheduled Uptime – Outages
- Mutually scheduled downtime: Scheduled outages that are required by Client and PerformanceIT to perform routine maintenance.
- Outages: Downtime associated with any failure.

9.2 Notification and Response Time Guarantee

PerformanceIT implements five alarm/event severity levels. The following table shows the description, notification method, and response time guarantee for each severity level. TacDoh may elect to receive alarms/events by email or pager.

Severity Level	Description	Notification Method	Response Time Guarantee First Level / Engineer Response
1	Critical	Phone & E-mail	15 minutes / 60 minutes *
2	Major	Phone & E-mail	15 minutes / 120 minutes *
3	Normal	Phone & E-mail	30 minutes / 4 hours *
4	Warning	E-mail	30 minutes / 4 hours *
5	Informational	N/A	N/A

- *Severity 1 Alarms* – PerformanceIT to notify TacDoh's primary contact by telephone and/or e-mail (TacDoh specified) within 60 minutes of receiving the Alarm from the ProIT Network Appliance (ProIT NMS). If no response is received from the TacDoh within 30 minutes of notification, (total of 90 minutes from Alarm), a second notification will be issued to the primary contact in addition to notifying the secondary contact by both e-mail and telephone.
- *Severity 2 Alarms* – PerformanceIT to notify TacDoh's primary contact by telephone and/or e-mail (TacDoh specified) within 120 minutes of receiving the Alarm from the ProIT Network Appliance (ProIT NMS). If no response is received from the TacDoh within 30 minutes of notification, (total of 150 minutes from Alarm), a second notification will be issued to the primary contact in addition to notifying the secondary contact by both e-mail and telephone.
- *Severity 3 Alarms* PerformanceIT to notify TacDoh's primary contact by telephone and/or e-mail within sixty (60) minutes of receiving the Alarm from the ProIT NMS Appliance (ProIT NMS). If no response is received from the TacDoh, the e-mail alert will continue every four (4) hours. If no response is received within 24 hours after the initial notification, the ticket will be closed.
- *Severity 4 Alarms* If action is required, PerformanceIT to notify TacDoh's primary contact by e-mail only within four (4) hours of receiving the Alarm from the ProIT NMS Appliance (ProIT NMS). If no response is received from the TacDoh, the e-mail alert will continue every four (4) hours. If no response is received within 24 hours after the initial notification, the ticket will be closed.

9.3 Alarm Severity Definitions

Alarm severity levels are defined as follows:

- ***Severity 1* – Critical** – Confirmed system or device down.
- ***Severity 2*** – **Major** – Major application failures or system stability threatened.
- ***Severity 3* – Normal** –Process down, disk capacity violations and performance threshold violations such as system load and virtual memory usage.
- ***Severity 4* – Warning –** Non-critical performance metrics generating alarms that must be investigated to determine real severity. Examples of Warnings include process down and system load violations.
- ***Severity 5* – Informational** – Non-threatening conditions that may indicate degradation in performance over time.

While all detected events have a predefined severity level, tailoring based on TacDoh requirements can modify these levels. The Event Threshold Action (ETA) Matrix is the defining document.

Errors that major applications or the OS will generate may be informational in nature and PerformanceIT may choose to ignore some of these by default. This may be due in part to the relationship between versions of applications and OS running for which there may be no clear cause of action but does not threaten the integrity of the system.

9.4 Client or Third Party Liability

In cases of device failure, such failure will not be counted against availability if Client, or a third party not contracted by PerformanceIT for support of the effected system, is responsible for the failure; PerformanceIT has notified the third party or Client of the failure via email within two hours; PerformanceIT monitors the status of the third party or TacDoh's actions to correct the fault, escalates the problem to Client, and follows up with the vendor or client.

9.5 Damages and Exclusions

PerformanceIT has agreed to perform the services in a manner that meets or exceeds the service levels which Client requires. PerformanceIT agrees that if they fail to meet the performance standards, Client will be damaged by such a failure. Because the precise amount of such damages would be difficult, in most cases, to ascertain, PerformanceIT agrees that in the event of such failure, the TacDoh may at its sole and exclusive remedy, in lieu of other remedies available to it with respect to performance standards, elect to receive liquidated damages from PerformanceIT as set forth below. Such liquidated damages will take the form of performance credits against the charges due to PerformanceIT under this Agreement. PerformanceIT will not owe the TacDoh any such performance credits where PerformanceIT's failure to meet performance standard is a direct result of:

A. Failure of Client to perform its obligations under this Agreement

B. Circumstances that constitute a force majeure event

C. An outage caused by TacDoh's implementation of a Change without providing PerformanceIT with adequate testing time.

D. Hardware failure

9.6 Performance Standards

The table below sets forth the categories and performance standards which reflect the overall quality of PerformanceIT's performance of the Services. This table will be used to determine whether any performance credits are due to Client:

Category	Performance Standard	Minimum Service Level
Total Network Availability-Stores	99.9%	98%
Total Network Availability-Regional Warehouses	99.99%	99%

9.7 Credit for Failure To Meet Performance Standards

Credits for failure to meet the performance standards shall be calculated as effective starting Q1-2002, and calculated as follows:

Each of the relevant performance standards and minimum service levels shall have weighting as shown below (the sum of the weighting factors shall no exceed 1.0):

Category	Weighting
Total Network Availability-All Locations	1.0

A. PerformanceIT's failure to meet the prescribed performance standards or minimum service level(s) shall require granting of credits based upon the initial 3 month period (quarter) of consecutive quarters that PerformanceIT fails to meet the standard(s). See the table on the following page.

The following table shows how credits would be issued.

Occurrence	Credit for Missing Performance Standard	-or-	Credit for Missing Minimum Service Level
1st quarter	3/10		5/10
2nd consecutive quarter	6/10		7/10
3rd consecutive quarter	9/10		10/10
4th consecutive quarter	10/10		10/10
Subsequent consecutive quarters	10/10		10/10

For example, if the total 3 month or quarterly charge is $2,000 and PerformanceIT has failed to meet a category with a weighting of 1.0 for the first quarter, the applicable credit would be:

1.0 x 3/10 x $2,000 = $600

PerformanceIT will return to "meeting standards" with respect to performance standards attainment when the quarterly performance level for that category meets or exceeds the performance standard. Any subsequent failure to meet the performance standard for that category shall be deemed a "1st occurrence."

PerformanceIT will return to "meeting standards" with respect to minimum service levels attainment when the quarterly performance level for that category meets or exceeds the minimum service levels. Any subsequent failure to meet the minimum service levels for that category shall be deemed a "1st occurrence."

If PerformanceIT misses the minimum service level for a particular category, the TacDoh shall be entitled only to the "Credit for Missing Minimum Service Levels" specified in the chart above, as opposed to the sum of the "Credit for Missing Performance Standards" and the "Credit for Missing Minimum Service Levels."

10 Proposal Summary

10.1 Cost: Pricing Summary

PerformanceIT proposes to provide the outsourced network management services described herein as outlined in the following table.

Table 4 Pricing Summary

Initial Term	Total #Devices		Code	Imp Code	
Initial Term:	12	1280	p	s	
Non-Recurring Charges (NRC)	**QTY/Code**	**Rate**	**Description**		**Total**
Installation (Days):	25	$ 1,000	ProIT Implementation		$25,000
Travel + Actual Expenses (Days):	25	tbd	Travel + Actual Expenses to client location		actual
ProIT NMS Appliance(s):	12	$ 1,995	Standard ProIT NMS appliance(s) -Included		$23,940
ProIT IDS Appliance(s):	0	$ 1,995	Standard ProIT IDS appliance(s)		$0
ProIT Standard Edition:	0	$ 4,995	ProIT Standard Edition		$0
ProIT Enterprise Edition:	1	$ 9,995	ProIT Enterprise Edition-Included		$0
ProIT Devices Licenses (>50):	1230	$ 100	ProIT Device Licenses -Included		$0
NPA Modules:	1	$ 495	Network Protocol Analysis -Included		$0
WebStats Modules:	0	$ 495	Web site statistics & reporting		$0
URL Checking Modules:	0	$ 495	Performs URL checks on up to 10 URLs		$0
WebTransaction Modules:	1	$ 1,995	Web transaction monitoring -Included		$0
IDS Modules:	0	$ 1,995	Intrusion Detection System Modules		$0
Sub-Total:					$ 48,940
Annual Support & Maintenance Fee:	S	18%	Standard Support & Maintenance		$ -
Total:			Implementation Total		**$ 48,940**
Monthly Recurring Charges (MRC)	**Code/Qty**	**Rate**	**Description**		**Total**
24x7 IT Managed Services:	1280	$ 100	All Inclusive Per Device Management Fee		$128,000
Online Secure Remote Backup Service:	0	$ 25	Per GB fee for managed online backups		$0
Sub-Total:	**>>>>>**	**>>>>>**	**>>>>>**	**>>>>> >>>>> >>>>>**	**$ 128,000**
Total Less Term Discount:	**>>>>>**	**>>>>>**	**>>>>>**	**>>>>> >>>>> >>>>>**	**$ 128,000**

10.2 Integration

There are two components of integration for this project:

- † Technology integration with in-house tools and network infrastructure
- † People and process integration between the Outsourced managed service provider and TacDoh

PerformanceIT will achieve technology integration with all specified devices for effective monitoring and management within the implementation phase. Further integration with existing in-house tools such as CiscoWorks will be achieved gradually over the first six months.

PerformanceIT's ProIT Network Management Platform provides a browser-based multi-user system designed specifically to facilitate teamwork between the in-house support team and PerformanceIT as the MSP. Both teams would have a seamless view and control over the infrastructure monitoring, alerting, fault management, and project tasks. Most MSPs provide merely a "reporting portal" whereby the customer can "look but not touch" the tools used to monitor, maintain, and manage their infrastructure. With ProIT, the reverse is true: a world-class platform is deployed for use both by in-house staff and by PerformanceIT as the strategic MSP partner.

10.3 Service Level Management

Service Level Management encompasses the effective use of the network management tools deployed to assure proper reporting, measurement, and SLA enforcement. Because PerformanceIT completely owns and controls the source code for ProIT, service level management fine-tuned for TacDoh can be achieved much more easily. Service Level Management will be provided via the monitored “Service Groups” constructed within ProIT as well as Availability reports based upon TacDoh’s services.

10.4 Reporting

ProIT provides a flexible reporting capabilities as outlined previously in this proposal. TacDoh staff and management will be able to create and run reports that meet their needs, from their browser, and at any time. Additional customized reports can be created by PerformanceIT or by TacDoh staff using third-party reporting tools such as Crystal Reports via access to the ProIT database.

10.5 Summary

PerformanceIT respectfully submits this proposal to TacDoh Corporation management for its evaluation.

Respectfully submitted:

Andrew Kramer

VP, Sales

(678) 323-1304 Direct

akramer@performanceit.com