Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 6 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Are Network Management Systems, Which are Becoming More and More Critical to the Reliability, Availability and Recoverability of Today's Data and Voice Networks Cost Effective?

By Steven Thomason
East Carolina University

Abstract - Network management systems are a necessary part of every production network. Nowadays management is always scrutinizes every dollar spent on hardware and software. The costs of these systems need be justified in the same manner that infrastructure and data center upgrades need to be justified. Network management systems not only are cost affective but also benefits the network management team in giving them the ability to look into their network to see what is going on. Without NMS you cannot answer questions such as why did the network go down or why is the network slow?

GJCST-E Classification : C.2.m

Strictly as per the compliance and regulations of:

Are Network Management Systems, Which are Becoming More and More Critical to the Reliability, Availability and Recoverability of Today's Data and Voice Networks Cost Effective?

Steven Thomason

Abstract - Network management systems are a necessary part of every production network. Nowadays management is always scrutinizes every dollar spent on hardware and software. The costs of these systems need be justified in the same manner that infrastructure and data center upgrades need to be justified. Network management systems not only are cost affective but also benefits the network management team in giving them the ability to look into their network to see what is going on. Without NMS you cannot answer questions such as why did the network go down or why is the network slow?

I. Introduction

One of the most important requirements of an IT organization is to maximize the uptime and availability of the network and its resources. Without having constant monitoring, the ability to look at historical data, proactive monitoring, and change management this becomes almost impossible to accomplish. Many times without a management solution you first find out about a problem when users start calling the helpdesk with complaints. This wastes time and extends the length of the outage costing companies anywhere from hundreds to hundreds of thousands of dollars an hour. In this paper we will use current monitoring system response data to demonstrate how efficient a managed WAN can be and compare that to possible scenarios that show what could happen using a manual process. The data has been derived from the WAN ticketing system provided by an outside vendor and compared to a separate internal help desk system.

The midsize company network I will be using as an example has 300 switches, 100 access points, 20 routers, 3 wireless LAN controllers and 16 WAN accelerators. There are also multiple firewalls and IPS' that are not part of this paper but are logged and monitored. 90% of the devices are Cisco hardware or software running on IBM or Cisco UCS systems. From this point forward they will be referred to ABC Company.

Author : East Carolina University.
E-mail : thomasons09@students.ecu.edu

Why have managed networks? First of all to define what is a network management tool we have rfc1470[i], which states that a network management tool is a tool that is used for monitoring and debugging TCP/IP Internets and interconnected devices. With an unmanaged network the only method you have of knowing when there is a problem is by word of mouth; a user calls the helpdesk after they lose connectivity to their application or someone shows up at your door asking if there is an issue with the network. The helpdesk personnel then do some basic trouble shooting which takes time. After determining that there is an actual problem and having determined whose area of responsibility it probably is then passes the ticket to the networking group. The ticketing system then generates an email to the person in the group designated to assign the tickets. At this point the networking group finally knows that there exists a problem with the communications network. The average time from initial call to making the appropriate people aware of the problem is between 30 minutes to 4 hours and this is only during normal 8 to 5 work hours. If an entire segment is down the time is closer to 30 minute. The more people affected the faster the problem is passed on. After the networking group has ownership of the issue they then begin their trouble shooting procedures. This again takes additional time, which translates to lost productivity, which translates to money.

Nowadays networks carry more than just data and are much more critical to the wellbeing of the business [ii] . There are data, voice, and video requirements placed on the network infrastructure at an ever-increasing rate. If the network goes down and carries the companies voice traffic problems are compounded since no one may be able to report any problems. So what is needed to help make the networking group more efficient and the network more reliable? At a minimum, networking groups need the ability to monitor and react to any issue that can affect

performance and reliability of the communications infrastructure.

The International Organization for Standardization Network Forum has divided network management into five functional areas[iii]:

1. Fault Management
2. Configuration Management
3. Performance Management
4. Accounting Management
5. Security Management

The primary purpose of having a network management system is to alert on network issues and aid in the quick recovery of the network and its services. Alerts can instantly notify personnel of a problem quickly and at times with the actual issue identified so that resolution can take place quickly. Fault management increases the ability to help identify faults and problems before they lead to actual downtime.

Configuration management is necessary to be able to keep track of the configurations on the devices running the network. By tracking changes and keeping historical copies of device configurations the system helps to restore devices that have had issues or need replacing. It also helps in the trouble shooting process in that you can determine when the last change was made, who made the change, and what that change was.

Performance management gives the networking team the ability to track device and component utilization, network throughputs, error rates, and other statics that help track usage and identify possible problems and bottlenecks. You can use this to answer questions such as why is the network slow? Is it due to a hardware issue or is an unauthorized process over utilizing it?

Two functional areas not addressed by this paper are accounting management, which involves tracking user utilization of network services and security management, which involves the protection of information through the network. While they are part of the ISO definition of network management they are not always part of most network management systems software. Individual logons for the management system addresses some of the concerns.

Below are two real life examples for ABC Company where monitoring would have aided in the ability to keep the network running as efficiently as possible.

In the first example demonstrating the need for network monitoring, there was an access point in a manufacturing area that saw very little usage. That access point stopped working. Users in that area saw slower performance but did not report the problem because they were still connected to a distant access point in another isle. Without proactive monitoring the performance would remain slow and if the next closest AP had an issue users would not be able to connect at all. A proactive system would have shown that the AP was down and made it possible to address the issue before it affected production. The down access point was found out about when the switch it was attached to had an issue.

Another issue that network management would help with is looking at what is using a network segment and how it is affecting the network. One instance occurred when the connection between a distribution center and the main server room experienced very poor performance. By connecting to the switches and routers at that site using SSH you could see that the interfaces were being highly utilized and there were no errors being generated. The line was up and VoIP phone calls were not affected. Knowing this information you could deduce that QoS was working correctly as calls were not affected but you did not have any idea what type of traffic was on the circuit and what it was doing. Was it a denial of service attack or someone copying a very large file or virus updates being pushed to all of the computers at an inappropriate time of day?

Management systems measure and keep track of metrics such as availability, uptime, latency, error rates, and other network characteristics. They give you the ability to manage very large networks from a central location[iv]. Networks that carry voice traffic also need to have the ability to look at voice statics such as jitter and echo. A good management system also has the ability to create a graphical map. A big advantage of this is the ability to see where the break in the network is located. Without this you would need to go device to device until you found the end of the working segment. Trace route is an example of command that can help determine where there is a break in communication but that only works for layer 3 devices.

ABC Company has several critical applications that cannot tolerate even brief drops lasting less than a few seconds. Handheld scan guns being used for warehouse management do not tolerate any downtime. The main ERP program will not handle any drop that lasts for more than a few milliseconds. Uptime is critical. A single blip in connectivity can cause the need to reprocess orders and shipments and manufacturing processes to be reentered or restarted.

A third party[v] that works with the MPLS provider monitors wide area network and WAN accelerators for ABC Company. They are responsible for monitoring the connections and performance of the WAN and its components. The third party has a system within the ABC Company network that gathers and monitors network statics. If an alert is received they review that alert with a combination of filters and human interaction. All interactions are logged in their management system. ABC Company looked at having them monitor the entire infrastructure but that cost was prohibitive and harder to justify. The performance of the monitoring company's system is compared to the internal systems within ABC

Company. This consists of a manual entry help desk system dependent on user interaction and an older network management system with limited abilities that monitors the LAN. It has the ability to determine if a device is completely down but not what types of issues may be occurring.

Reporting data for this paper was taken from an existing WAN monitoring system that is monitored 24x7x365 by a third party system. The data points used included the following: ticket creation time, 1st human response time, the number of human interactions per ticket, whether the local site contact or Telco was contacted, the time the site was fully functional and the total number of minutes before the ticket was closed. The network has a monitoring station that receives snmp and icmp packets to track uptime and interface errors. If there is an error then the system sends out an alert to the monitoring company where the alert is evaluated and the appropriate predefine action takes place. An example of a predefined action might be to ignore the error until 8:00 am due to the fact that the site is remote and no one is available until that time, call a local site contact, or wake someone up. An alert can signify anything that can lead to degradation in performance or availability. The management company first tries to resolve the issue if possible. If it looks like as if the problem is with a circuit the local Telco is notified and a technician is dispatched per predefined scripts.

In 2012 there were 75 interactions that generated alerts that required examination. The average response time it took for an actual person to review the alert was 13.3 minutes. The average time it took to resolve the issue was 481.9 minutes. An alert did not necessarily mean that a circuit or connection was down but it did mean that performance was degraded. The percentage of interactions that required local site personal to be contacted was 21 and 35% of the alerts required a technician from the local circuit provider.

Data from the first 10 tickets. Sample ticket at the end of the document.

Ticket Creation	1st Incident Response	Live Response Time	Number of Ticket Interactions	Contact local Site	Contact Telco	Circuit Fully Functional	Ticket Closure	Length of Downtime – minutes	Man-Minutes Spent on Issue
2/27/12 8:356	2/27/12 8:36	0.5	5	No	Yes	2/27/12 8:44	2/27/12 13:00	8.3	263.6*
2/28/12 20:41	2/28/12 20:49	8.1	5	No	No	2/28/12 20:51	2/29/12 1:55	1.9	306.1
3/13/12 22:56	3/13/12 23:01	5.7	3	No	No	3/13/12 23:01	3/14/12 3:07	0	245.8**
3/14/12 7:46	3/14/12 7:51	5.9	3	No	No	3/14/12 7:53	3/14/12 7:57	1.1	5.8
4/10/12 16:46	4/10/12 17:02	16.4	11	No	No	4/10/12 17:13	4/10/12 20:37	10.6	214.6
4/14/12 10:46	4/14/12 117:02	42.5	8	No	Yes	4/14/12 10:51	4/14/12 16:40	0.1	673.4*
4/19/12 21:26	4/19/12 21:28	2.3	39	No	Yes	4/23/12 11:31	4/23/12 18:00	5162.7	5551.8#
…	…	…	…	…	…	…	…	…	…
12/4/12 14:01	12/4/12 14:51	.5	1	No	No	12/4/12 14:56	12/4/12 14:56	5.1	5.1
12/17/12 20:21	12/17/12 20:28	7.6	4	No	No	12/17/12 20:46	12/18/12 0:16	17.8	227.9
12/31/12 21:06	12/31/12 21:12	6.8	4	No	Yes	12/31/12 21;21	1/1/13 5:19	8.8	13.34

Notes:

*Extended times were due to slow response times from the MPLS provider in determining what caused the actual drop with BGP routing.

** Riverbed outage – failed open so no downtime – however performance degraded for until restart.

Intermittent issues tracked down to bad card in Telco switch.

II. Out Sourced Management System

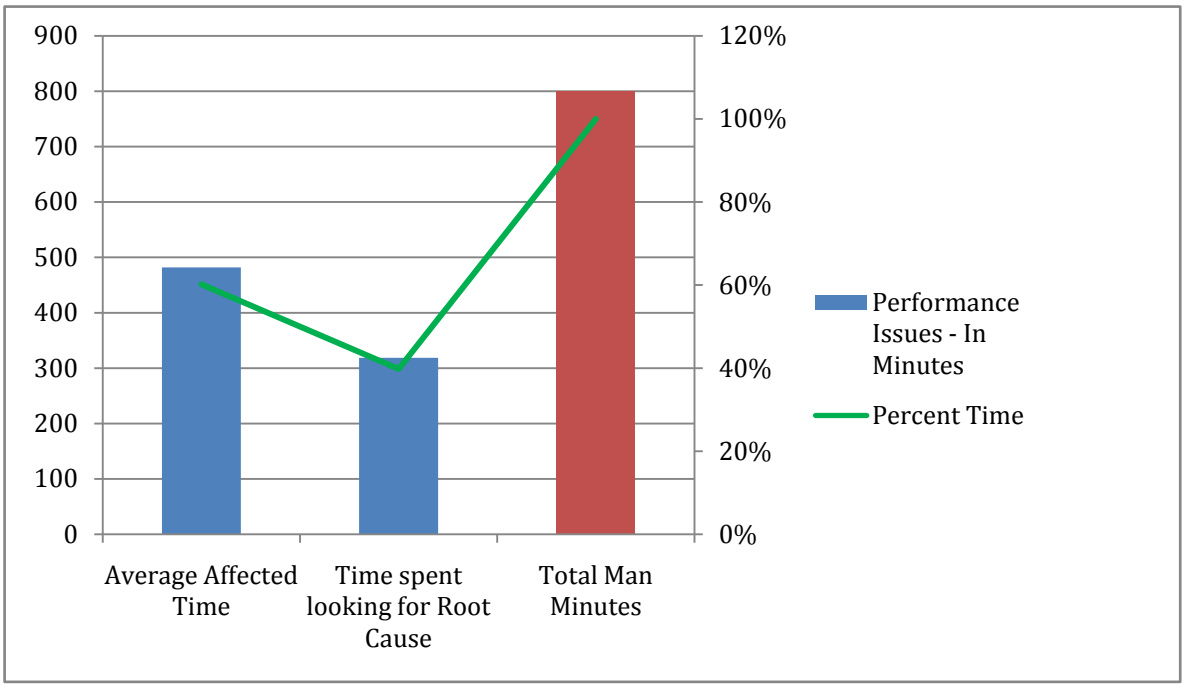
- Average time before an actual human looks at the event – 13.3 minutes.
- Average number of human interactions before the ticket is closed – 8.4.
- Average length of downtime or network impairment – 481.9 minutes or 8.3 hours.
- Average man-hours spent before closing the ticket – 13.34 or 800.6 minutes.

- Percentage of time spent to determine root cause after performance had been restored to previous state – 40% or 318.8 minutes.
- Percent of human involvement taking less than 15 minutes – 76%.
- Percent of human involvement taking less than 30 minutes – 95%.
- Keeps historical data for 1 year showing amount of traffic based upon IP ports.

III. Manual Help Desk System

- Due to the way the help desk system functions internal tickets can take well over 30 minutes before the 1st person in the networking groups is even aware of the issue.
- Percent of human involvement taking greater than 30 minutes – 95%.
- Help desk system creates tickets that are hard to research for past issues due to a lack of historical indexing.
- Keeps track of tickets but because it is not a dedicated network system it is hard to research past issues.

Finding out what the root cause of an alert is required and having the issue resolved was is the first step in the process. The average man-minutes spent until the ticket was closed was 800.6 meaning that 40% of the time on ticket was spent after resolution determining what the cause was.



By having the monitoring system in place for the WAN it meant that 76% of all tickets were initially addressed in less than 15 minutes. 91% were addressedin less than 30 minutes. Comparing this to an existing system within the company for the local area network shows a major difference in time to reaction.

The average time before being notified using the internal helpdesk system ranged from 30 minutes to over 6 hours especially if the issue occurred after hours and the after hour answering service was not able to notify the appropriate personnel. This system depended upon user input for notifications. A completely down system was easy to detect but in instances where performance was degraded it was not as easy to determine since often the end user did not report it until it became severe. A management notification system could have seen the performance issue and notified someone so that the issue could have been addressed before any downtime had taken place.

Management systems can vary quite a bit depending on the vendor and features. Retail cost for the Cisco Prime infrastructure and Collaboration software is approximately 85 thousand dollars for an average SMB. Using the data taken from the WAN monitoring service we found that out of 75 incidents there were 16 that took over 4 hours to address. ABC Company has determined that after 4 hours of downtime to manufacturing processes can cost over $100,000 per hour. If you take the best effort of the manual helpdesk system and add 30 minutes to each of those tickets you would have increased the loss by an additional $200,000. This would more than cover the cost of installing a management system for the network and the example does not even address the internal LANs in each location.

Cisco Prime Infrastructurevi, being reviewed by ABC Company, is only one of many management systems available. One of the main reasons for looking

at Prime is the current investment in Cisco equipment, training, and services. Some of the other more common management systems are Solarwinds[vii], SpiceWorks[viii], Paessler[ix], Tivoli Framework[x], and WhatsUp Gold[xi]. This is not an exhaustive list as there are many different vendors each with its own set of features. Prime manages wired and wireless access over local and wide area networks. It gives the user a combination of inventory, configuration management, visibility, and wireless management features. The system allows for the use of Netflow, NBAR, and Medianet agents for reporting. Prime also keeps historical data and gives the user a drill down functionality to help with trouble shooting issues. When combined with Cisco ISE – Integrated Service Engine it also give the user security and accounting functionality meeting all of the ISOs five functional areas.

A good management system allows for a smart notification system that analyses alerts and prevents alert overload. Is the alert identifying a critical issue or a temporary over utilization of a port?This way only the critical alerts get through so any notifications that are sent to a technician are the ones that are really important. The system needs to be able to differentiate between an end user reboot their PC and a connection to a MPLS network. The alerts not defined as critical are logged so that they can be review from the management console.

With budgets tight and executives wanting a positive ROI network monitoring needs to show it savings potential. According to white paper by Intermapper[xii]. There are several areas of potential savings that are generated by a network monitoring system.

a) Savings

- Staff/salary time savings
  - Automating processes and monitoring frees staff for other tasks and projects.
  - May not need to increase the number of staff personnel as the network grows.
- Minimizing or avoiding outages
  - Proactive actions when issues appear allow for action to take place before downtime occurs.
- Reducing support calls
  - If the network is up and functioning correctly there will be fewer trouble tickets created.
- Reducing time to fix
  - The sooner IT is alerted to a problem, the sooner the issue can be resolved.
- Guaranteeing and managing SLAs
  - Using the historical data retained by the management system it can be determined whether or not SLAs are being met.
- Reducing downtime
  - Configuration and change management allows for quicker restore of down devices and services.

Network management systems are not in expensive. They range from just sending alerts when a ping to a device fails to be able to meet all of the requirements for the 5 functional areas listed by the ISO.

b) Costs to Take into Account

- Initial purchase of solution
  - Unless you create the solution in house you will need to purchase the solution and in house solutions still require a developer's time.
- Product upgrades and support
  - All commercial products require maintenance contracts for support and upgrades.
- Required hardware and OS software
  - The purchased solution has to be installed on something. Even virtual solutions require disk space and licensing.
- Installation/implementation consulting
  - It takes time to learn a new solution even when installed by an outside consultant. Knowledge transfer is required.
- Training
  - Some of the larger products may require staff to attend training classes in person or over the web.
- Solution administration/management
  - While the solution can save many hours doing tedious tasks such as device management, configuration, and changes, it still requires human interaction.

To be successful a management system needs to have several metrics that can be used to justify its purchase and operation. According to a study by Solarwindsxiii one client determined the metrics to the number of man-hours/time spend each day trouble shooting issues, revenue generated, and costs saved. Each issue or ticket then was tagged to any SLA agreements. Having a network performance monitor allowed them to save over 20% in equipment replacement costs and gave them the ability to keep historical data so it became much easier to determine root cause of each issue. Another side benefit of using a management system is the reduction in human caused errors. Over 80% of critical network outages are caused by human error[xiv].

As companies grow and expand manufacturing can expand to become a 24-hour endeavor. As production schedules expand it becomes more critical to either have staff working all 3 shifts or a system that monitors all of the networking components and can alert staff of any issues at any time of the day.

Other functionality that can greatly reduce staff time is the ability to manage multiple devices from one central system. Using ABC Company as an example, they have 300 switches that at some point will need to be upgraded due to an increase requirement of security for functionality. Based on the average time of 30 minutes spent by a network administrator to manually upgrade each switch, it would take 15 hours to complete these tasks. This does not include the time it takes to research what the latest approved version is, can the switch handle the upgrade, downloading the software, or setting up the tftp server for distribution. Another part of the process would be to backup each configuration and save the current running configuration before even starting. Using a management system such as Prime Infrastructure [xv], the network administrator would only need to run a report to see if everything could be upgraded, plan on when the upgrades could take place, and create a job that would handle all of the upgrades automatically.

In another example the company managing the WAN devices that consisted of Cisco routers and Riverbed accelerators were able to automate the upgrade of all 13 WAN accelerators form version 6.x to version 7.0.x. This was done in order to keep the devices up to date for support requirements. Using an automated management console every Riverbed was upgraded to the latest code using a simple script reducing downtime and labor costs. Setting up the script took approximately 1 hour, running the upgrade on 15 devices took 30 minutes for a total of 2 man-hours. Manually upgrading 15 devices would take approximately 45 minutes per device resulting in a requirement of 11.25 man-hours. The ability to have process take place in a batch mode further demonstrates the usefulness and cost savings ability of management software.

Using the data derived from the third party monitoring service and comparing that to the information derived from the internal help desk system, can be shown that an automated system is obviously faster than a manual system. Adding on average over 30 minutes to every ticket costs time and as stated before when an incident is affecting down time that runs over 4 hours the costs to the company is well over the cost of using a network management system. As with the example above assuming that you have to upgrade the companies 300 switches once a year, which at 30 minutes per switch takes 150 man hours automating that saves you over 100 hours of a person's time based on a 75% savings in time. At $25 per hour that is a savings of over $2,800 and that is being conservative. So anyway you look at the benefits of using a network management system, you will save time and money, whether in reducing downtime, meeting SLAs, or reducing maintenance downtime.

To review, network management systems have the ability to save companies money and increase profitability and productivity. This gives existing employees more time to be proactive or keeps management from having to hire more highly trained and expensive engineers. Uptime of the network is increased and downtimes are shortened.

Using historical data, it also becomes much easier to justify increasing bandwidth when there is data demonstrating the overutilization of existing circuits. You also have the ability to remove any underutilized circuits to save money. Monitoring can also help to point out potential problems by measuring network metrics such as packet loss and error rates. Without monitoring you do not have the ability to know if the number of errors on an interface is from a temporary problem or a potential issue. Network Management software is not only cost affective but critical to the well being of a company's communication infrastructure.

End Notes:

[i] Network Working Group. Request for Comments. Web. 14 Feb. 2013. http://tools.ietf.org/html/rfc1470

[ii] Julia K. Brande "Computer Network Routing with a Fuzzy Neural Network." November 7, 1997. Retrieved from http://scholar.lib.vt.edu/theses/available/etd-11197-12405/unrestricted/ETD.PDF

[iii]AIRLINX Communications, Inc. Network Management. Web 15 Jan. 2013. http://www.airlinx.com/index.cfm/id/-1-11.htm

[iv]Dimitrios GEORGOULAS, Keith BLOW, Wireless Sensor Network Management and Functionality: An Overview, Wireless Sensor Network, 2009, 1, 257-267, doi:10.4236/wsn.2009.14032 Published Online November 2009

[v]GLS. Global Linking Solutions.www.GLS.com

[vi] TechTarget. A new Cisco network management strategy: Cisco Prime. Web. 15 Jan. 2013. http://searchnetworking.techtarget.com/news/2240034929/A-new-Cisco-network-management-strategy-Cisco-Prime

[vii] Network Management. Solarwinds, Web. 20 March 2013. http://www.solarwinds.com/network-management-software.aspx

[viii]SpiceWorks Network Management Software. Web. 22 March 2013. http://www.spiceworks.com/free-network-monitoring-management-software/,

[ix]Passler Network Management. Web. 17 March 2013. http://www.paessler.com/solutions,

[x] IBM. Tivoli Framework Management. Web. March 20, 2013. http://www-01.ibm.com/software/tivoli/products/mgt-framework/,

[xi] WhatsUp Gold. Web. 20 March 2013. http://www.whatsupgold.com/products/whatsup-gold-core/index.aspx,

[xii] Intermapper. 6 Ways to Calculate Returns from your Network Monitoring Investment. Web Feb. 2013. http://www.intermapper.com/uploads/pdf/InterMapper%20ROI%20Whitepaper.pdf

[xiii] Network Management. Solarwinds, Web. 20 March 2013. http://www.solarwinds.com/network-management-software.aspx

[xiv]HP. Your network enables your business. Web Jan. 2013. http://h20195.www2.hp.com/V2/GetPDF.aspx/4AA1-6185ENW.pdf

[xv] Cisco Prime Infrastructure Configuration Guide, Cisco Systems, Web Jan, 2013 http://www.cisco.com/en/US/docs/wireless/prime_infrastructure/1.2/configuration/guide/pi_12_cg.html

```
--------------------------------
This is a summary of your case and its current status

Customer Name :
=============
STM Industries (AT&T NI)

Site Name :
=========
Catawba, NC (Oxford DC)

Status :
=======
Closed

Priority :
=======
Informational

Opening Summary :
=======
Network alarm occured.

Opening Description :
===========
Ticket generation based on a network alarm. NOC investigating.

Equipment :
=========
STM_RTR_Catawba - Router - Cisco - 2811

Event Logs for this case :
========================

04/25/2012 11:31:01 -- close -- Smith, Amber
Ticket Closure: ATT ticket had no further updates (closed ticket)

BGP uptime 06:55:28

no errors

Serial0/0/0 is up, line protocol is up
  Hardware is GT96K with integrated T1 CSU/DSU
  Description: AT&T Circuit ID DHEC.918563.ATI
  Internet address is 192.168.199.37/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 12/255, rxload 72/255
  Encapsulation PPP, LCP Open
  Listen: CDPCP
  Open: IPCP, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters 06:48:04
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: Class-based queueing
  Output queue: 0/1000/0 (size/max total/drops)
  30 second input rate 442000 bits/sec, 76 packets/sec
  30 second output rate 76000 bits/sec, 78 packets/sec
     980698 packets input, 487014126 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     1086429 packets output, 112190832 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up

04/25/2012 04:50:28 -- priority change -- Smith, Jeromie
Priority change, from New Investigation to Informational.

04/25/2012 04:50:17 -- log -- Smith, Jeromie
continue to monitor and check carrier ticket at scheduled time
```

04/25/2012 04:50:17 -- log -- Smith, Jeromie
Priority Status change, from NOC Working Ticket to Awaiting Carrier Update. Priority status schedule is set to 04/25/2012 09:00.

04/25/2012 04:49:35 -- log -- Smith, Jeromie
Adding carrier ticket ID: 000000153625574

04/25/2012 04:47:29 -- log -- Smith, Jeromie
Opening ticket with the carrier:

ticket was already open

Checking carrier ticket:

04/25/2012,01:42:12:[AT&T] Activity Type Code Desc: PROGRESS COMMENTS
Activity Type Code: PROG
CGW ... hello csr, we have set this up for extensive testing, we will advise of test results accordingly, thanks, AT&T ...

04/25/2012,01:41:55:[AT&T] Activity Type Code Desc: TEST COMMENTS
Activity Type Code: TEST
User cc7965 has scheduled Complete Auto Test (force intrusive) to run at 04/25/2012 01:41:00 for 15 minutes with an estimated run time of 185
minutes.

04/25/2012,01:41:37:[AT&T] Activity Type Code Desc: TEST COMMENTS
Activity Type Code: TEST
unable to read the csr's CSU registers ...

04/25/2012 04:47:29 -- log -- Smith, Jeromie
Priority Status change, from NOC Working Ticket to NOC Working Ticket. Priority status schedule is set to 04/25/2012 05:00.

04/25/2012 04:42:58 -- log -- Smith, Jeromie
Logging into device to gather status:

STM_Catawba_RTR uptime is 45 weeks, 1 day, 18 hours, 49 minutes
System returned to ROM by power-on

bgp= 00:06:25

Serial0/0/0 is up, line protocol is up
Hardware is GT96K with integrated T1 CSU/DSU
Description: AT&T Circuit ID DHEC.918563.ATI
Internet address is 192.168.199.37/30
MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, LCP Open
Listen: CDPCP
Open: IPCP, loopback not set
Keepalive set (10 sec)
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters 32w6d
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 29508
Queueing strategy: Class-based queueing
Output queue: 0/1000/0 (size/max total/drops)
30 second input rate 7000 bits/sec, 8 packets/sec
30 second output rate 10000 bits/sec, 10 packets/sec
442685557 packets input, 3444254842 bytes, 0 no buffer
Received 0 broadcasts, 1 runts, 8 giants, 0 throttles
29581 input errors, 29581 CRC, 12182 frame, 5090 overrun, 0 ignored, 18545 abort
529237866 packets output, 968859321 bytes, 0 underruns
0 output errors, 0 collisions, 4 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
16 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up

04/25/2012 04:42:58 -- log -- Smith, Jeromie
Priority Status change, from NOC Working Ticket to NOC Working Ticket. Priority status schedule is set to 04/25/2012 05:00.

04/25/2012 04:36:04 -- log -- Manager, Event
STM_RTR_Catawba - PING - OK - 192.168.199.37: rta 14.875ms, lost 0%

04/25/2012 04:36:03 -- log -- Manager, Event
STM_RSH_Catawba - Riverbed Status - Steelhead 250 (250M): Healthy, optimisation service: running

04/25/2012 04:36:03 -- log -- Manager, Event
STM_RSH_Catawba - PING - OK - 172.25.1.4: rta 15.498ms, lost 0%

04/25/2012 04:36:03 -- log -- Manager, Event
STM_RTR_Catawba - HOST - OK - 192.168.199.37: rta 14.840ms, lost 0%

04/25/2012 04:36:03 -- log -- Manager, Event
STM_RSH_Catawba - HOST - OK - 172.25.1.4: rta 20.992ms, lost 0%

04/25/2012 04:28:12 -- log -- Smith, Jeromie
Reviewing ticket and ticket procedures

04/25/2012 04:28:12 -- log -- Smith, Jeromie
Priority Status change, from System Generated to NOC Working Ticket. Priority status schedule is set to 04/25/2012 04:30.

04/25/2012 03:56:04 -- log -- Manager, Event
STM_RTR_Catawba - PING - CRITICAL - 192.168.199.37: rta nan, lost 100%

04/25/2012 03:56:03 -- log -- Manager, Event
STM_RSH_Catawba - Riverbed Status - (Service Check Timed Out)

04/25/2012 03:56:03 -- log -- Manager, Event
STM_RSH_Catawba - PING - CRITICAL - 172.25.1.4: rta nan, lost 100%

04/25/2012 03:56:03 -- log -- Manager, Event
STM_RSH_Catawba - HOST - CRITICAL - 172.25.1.4: rta nan, lost 100%

04/25/2012 03:56:03 -- log -- Admin, System

STM_RSH_Catawba - Added equipment to the ticket.

04/25/2012 03:51:03 -- log -- Manager, Event
STM_RTR_Catawba - HOST - CRITICAL - 192.168.199.37: rta nan, lost 100%

04/25/2012 03:51:03 -- open -- Admin, System
Initial Ticket Creation.

This page is intentionally left blank