Timothy Burns

Network Management on a Budget

ITEC 6885

2017

Monitoring a network includes many different things. The scope needs to be very broad to incorporate many details in between. Having a good plan in place along with helpful applications is key to having a healthy network and being able to troubleshoot potential problems when they occur. Many software companies have been created and do very well in specializing in network monitoring. However, while some software can be quite expensive and do provide a tremendous value, many smaller companies simply do not have the budget to make these kinds of purchases. In certain environments they are worth every penny. Smaller IT departments have smaller budgets and usually have to do without or find alternatives. Thankfully there is software available that is open source which can be used for free that in many cases can compete with the paid for alternatives. However, there are cons that should be kept in mind with using open source as well. This discussion will revolve around some of the methods that are used to monitor networks. Equally, which applications can provide the ability to use those methods and if there is a cost alternative application that can be used.

To begin looking at whether or not a program can satisfy the needs of a specific network, the goals of what should be accomplished should be highlighted. It would be a bonus if there were a one size fits all application that could check off all of the boxes, but it may be a few programs will be needed to work in conjunction with each other. The purpose of a monitoring plan should include the business purpose of the company. No company wants to have down time, but an ISP will place a higher priority on making sure all of the core networking devices are up and running in a healthy state. So, it could be that another business may have applications that workers rely upon to perform their jobs. In this case it would be imperative that they can not only reach the application, but that the hardware the application runs on is also at a peak performance state.

A model was created to help define an approach to network monitoring the best practices to use. The ISO network management model includes five areas that should be used as guides known as FCAPS." The basic idea behind FCAPS is very simple – it categorizes the plethora of information handled by a management system into five key functional areas: Fault Management, Configuration Management, Accounting Management, Performance Management and Security Management. ("FCAPS" 2005)"

Fault management pertains to making sure the network is up and running free from any errors." The goal of fault management is to detect, log, notify users of, and (to the extent possible) automatically fix network problems to keep the network running effectively. ("Network Management" 2002)" This is where a network management comes into play. A program that contains all of the defined network devices, which presents a display to notify of any issues pertaining to those devices. Many of these events can be monitored via SNMP. Files called the management Information database are used by SNMP to define events the devices use for alerts. Some products such as Cisco create their own MIB specifically for their devices.

Along with SNMP network devices create syslog files, which are events or notification created by a device. How detailed the events are up to the user. In the Cisco environment there are 8 different levels when it comes to logging levels. They range from an emergency level, which pertain to severe system malfunctions to Debugging Levels which will include interfaces changes and items of that nature. "By default, the router logs anything at the level of debugging

and greater. That means that logging occurs from level 7 (debugging) up to level 0 (emergencies). (Davis, 2006)" The level chosen also pertains to which layer the device is included. At the access layer interface changes may not be as crucial to log as users restart computers often. However, at the distribution layer, a port going down could mean that an access layer switch is down, which is very important to know.

Included under the fault management section is fault monitoring and notification. There is a difference between this and polling. SNMP devices can proactively send messages to monitoring systems based on what are known as traps. Traps are able to take predefined rules in MIB file and send notifications to a defined SNMP server. The types of traps used have a wide variety. These can be used to notify of when a system's fan is down or for environmental factors such as the temperature becoming too hot or cold. These two options for example can go hand in hand if an alert comes there relaying a fan has malfunctioned and admin may not have to drop any current task to address the issue as the temperature control will let me know when system is becoming too hot. There are also specific traps designed for routing protocols where alerts can be initiated for when an OSPF neighbor is no longer seen or joined.

Configuration management is the next area that is discussed in the FCAPS model. The first item that may come to mind when speaking of this is the literal configuration files of all devices. While there is the inclusion of this, it also contains hardware and software versions. Knowing where devices are located, what services each device provides and easily being able to identify who manages those devices can truly expedite the resolution of any problem. Smaller IT departments may not have this problem, but large corporations may have staff that work in different states. As a manager of multiple functions, it can be very easy to lose track of responsible for what.

Then there is the actual configuration piece. A network can change frequently due to upgrades or users just simply moving. Having a backup of all network devices provides many avenues of protection. For example, if a device decides to quick working having a backup of that device is very crucial in returning the area that was affect back to up and running in the quickest possible fashion. Also, what is key is not only having a backup of the configuration but a most recent backup of the config. As previously stated a network can change frequently and having and outdated backup can only detour resolving an issue.

Another factor to take into consideration is when changes are made to devices is an important matter to keep in mind is who made the changes. Change management goes hand in hand with keep a secure network as well. "Secure change management verifies that changes were implemented as intended, identifies when a change has unintended consequences, and highlights unapproved changes. (Cohen, 2014)" A key feature in a monitoring system performing audit logs of system changes. This can tell you what changes were made and by whom. The changes made will not only help keep track of who and what, but if an issue began occurring affecting the network, having a log of the changes made can help decipher if those changes were part of the possible cause.

Still looking under the configuration management piece, knowing the inventory of what is connected to the network is also helpful in many ways. There is the manual method by keeping a spreadsheet and keeping notes. However, a good network monitoring system should be able to query all of the devices and also note this as well. Keeping track of all hardware will help in knowing what software needs to be updated and if there are possible conflicts. Looking from the security aspect, it is almost a weekly occurrence that a security flaw is discovered on a vast amount of different software and firmware. Having a thorough understanding of what is on the network that could be vulnerable to the security flaws is critical to the safety of the network. Quickly being able to identify if the affect software is on your network and then applying the necessary patch or upgrade is all part of an administrator's job of managing the network.

The next topic in the FCAPS model deals with the performance of the network. This also covers many different areas pertaining to how well the network is functioning. Different points of the network can and should be monitored to inform you if its status. A prime example would be the CPU of a webserver. Having alerts for certain thresholds can be informative to know. Being able to reach a device to know it is on the network is one thing, but being able to use it with full functionality is another. If for instance if the CPU is maxed out at 100 percent on a webserver, it may be able to respond to a ping request but the hosted website may essentially be unusable. While this information is a great indicator of where the problem is, it is only the beginning of troubleshooting. The cause could be related process that got stuck in a loop, or it could a DDOS attack on the server. Other performance examples could be the memory on a machine or the port of the network speed that server uses. The point is that having the monitoring setup is key for healthy network.

Along with performance, creating a baseline is crucial to monitoring each specific case. **"**A network baseline measurement is a recording of network performance data over a known period of time for comparison, control and planning purposes. (Curtis, 2003)" A baseline will be different for each section of the network as well as they may be different for companies as well. Looking back at the webserver example. This particular webserver may be heavily used, so the resources may be higher than a different server on the network. Knowing what the average use of what the CPU and memory is usually consumed will identify where thresholds need to be setup. Normally, if the CPU operating at around 50 percent, setting an alert threshold at 70 percent may be acceptable.

Briefly getting into the heuristics, baselines provide great insight to the security of the network. In general, equipment will work harder and use more resources during normal daytime working hours, so in the evening hours is when it would be expected to see a drop in the utilization of those resources. So, creating different baselines for different times of the day is key. During off peak hours, it may be necessary to create a different set of rules and thresholds. Over the midnight hours if your expected CPU utilization is 20 percent, it may be that the max threshold during that time should be lowered to 50 percent. High utilization during off peak hours could potentially point to unauthorized access to resources. Going a step further, with having a good baseline the resource utilization can be mostly predicative baring some unforeseen event. A general guide may be used to know that between the hours of 8 and 9 the CPU and memory of a

server percentages should steadily increase to the average working baseline. In fact, there may be numerous increases and decreases based on the time of day. What needs to be of concern is any sudden spikes in resource usage. If this were to occur, hopefully it is a related to a reasonable explanation to due to an issue with an application, but the real concern is security related that there is some possibly unauthorized use of a device. Reasoning aside knowing this type of behavior is crucial and an overall simple approach of keeping track of network performance and knowing what is happening. One last factor to keep in mind when dealing with performance and baseline is that this is an ongoing task. As with any business, it should be assumed to grow and so will the use the use of the network and systems. This will involve taking periodic baselines of the resources and realigning the thresholds to keep the alerts fresh and useful. Additionally, this will help with future planning. Being able to look at historical data and seeing that a server's use is going up 5 percent each month then in 2 years it may be the that either the resources will need to be increased or a newer server will need to be purchased all together. Essentially this can all be done with an SNMP server and few queries.

Keeping in line on the performance aspect and moving on the to the more traditional network side is keeping track of the data crossing the network. This entails not only speed but also the applications. One avenue to do this, is by using a technology called Netflow. **"**Flow data is tried and true for accounting, network forensics, and creating baseline network profiles useful for identifying malicious or anomalous activity. It can also help business administrators make decisions about prioritization of resources or how to plan for necessary changes to the network. (Sarneso, 2016)" Net flow is a Cisco proprietary protocol, but there is also an alternative version for other products that provide the same functionality. Essentially, Netflow is configured on a desired port and inspects all traffic going in and out of that port. The details that are gathered include IP's, ports and other identifying marks. The information that is gathered is then sent to a collector or analyzer to display the data in a readable format. Being able to see that a port is only using 50 percent of its capacity is one thing, but also knowing how that percentage is broken down in terms of application used provides a whole different level of detail. From the data, if you are able to discern that most of the traffic on your network is http or https, you may identify either you need to plan for more internet bandwidth or make a use case to block certain sites during business hours. There are a number of other scenarios for having this type of data at hand.

Security management is the last topic covered under the FCAPS model. Protecting the network may seem like an area that doesn't belong with management network. While this is somewhat true, sticking to some best practices can go a long way to keeping the network safe. "Authentication, authorization, and accounting (AAA) is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security. (Rouse, 2010)" One of the obvious steps to reduce unauthorized access to network devices is by way of usernames and complex passwords. This will identify who can access the defined device. Logically it seems natural to only allow access to a network switch by the IT staff and depending on the size of the department, possibly even only to the network admins. To go even further, limiting what can access a network device can create another layer of security. This may not be appropriate for all applications, but using

access lists and reduced access will assist in keep the network safe. This implementation depends on how segmented the network is. If the finance department is on a different address space, then it would be best practice to not allow any address from within that space to reach the switching and routing infrastructure. In an extreme case it may even warrant limiting access to a single IP. Now that we have covered the who and the what, next is the why. Even though it may be configured that the network administrator is the only person that has access to a switch, accounting brings in the checks and balances to what is being configured on the devices and at what time. This can be extremely valuable to any size department, but especially useful for very large groups with multiple administrators and duties overlap. From an alert standpoint it is very good to know if the administrator is logging in overnight making changes if it is not considered to be normal working hours. Another helpful result is when disaster strikes. When there are technical issues going on, once the troubleshooting begins it is generally good to address any recent changes that may have taken place. By having a management system in configured, it can easily be seen what changes were made, who made the changes and how long ago they were made. If you can correlate a change to when a problem started occurring, most likely the problem will be solved or at least known.

As previously discussed, SNMP is a very powerful tool for monitoring all network devices. However, it was not mentioned that it can also make changes to those devices if designed to do so. This essentially becomes an admin account and should be treated as such in terms of security. There are two different ways to setup SNMP, read/only and read/write. Read only is considered to be at least the safer of the two as it can only see the information. Read/Write carries a little more weight as it can make changes against the device. Just as we previously discussed we want to limit where these SNMP queries and changes can originate from to limit the amount of exposure. SNMP has the ability to also limit what an SNMP account can see with the view feature. Much like an access-list, SNMP can be designed to only access the defined MIB trees. For example, you can setup an SNMP account to only be allowed to query system resources keeping the IP statistics information private. One last important key note pertaining to SNMP is the versions. There are three versions of SNMP, without going into too much background, SNMP version 3 is by far the most secure and "provides authentication, ensures data integrity, and prevents masquerading. ("SNMPv3" 2003)" "SNMPv1 and SNMPv2 are considered a weak mechanism to support any security enhancements due to their limited architecture which necessitates the introduction of a newer version for this protocol which is SNMPv3. (Sibai, Nguyen, Thach, Wu,)" Version 3 allows the use of usernames and passwords which can also be combined to take advantage of SHA or MD5, which was a much needed upgrade from the previous versions. That along with the optional use of encryption really sets this as the standard to use. With all of the enhancement and security features it be puzzling to wonder why the previous version would still be deployed.

So now that we have a general overview of some of the best practices are in terms of implementation we can look at some software that can be used for these purposes. There a plenty of competitive vendors to choose from in this space. However, there are also a wide range of choices of alternative or zero cost.

When it comes to open source software that offers network monitoring there are actually a nice range of choices. Nagios Core is a very popular open source network monitoring system as it has been around for quite some time and has an established respectable user base. Zabbix and PandoraFMS are both competitors in this field, each providing a very thorough offering. The one downside as with anything that comes for free the amount of support provided is somewhat lacking as there is none. Many though, have their own online community which is usually a great way for help with issues. Obviously though, the more adopters there are using a certain software the more help there will be. This may be a major contributing factor in which selection is made. Most open source programs including the ones mentioned also have some form of purchase options. Some may have a base option which is free but provide more features in a paid version including support. Additionally, there are some that may only allow a certain number of devices which may not be able to cover a large company with a large network. Another item to keep in mind is that many open sourced or free systems are Linux based. There will be a web based display to view the data in pictured graphs, but the configuration will be all text based. Nagios is a prime example, as the install and configuration changes and edits all need to be done within the command line. If there is not resource on staff that is comfortable using Linux, then it could limit the list of systems to choose from.

As stated there are other options, for an example purposes, this is one of the reasons for mentioning PandoraFMS. They do provide a free version of their software for windows. Again this comes with limitations including only being able to monitor 1000 agents. There are some configuration files to use as well, but this should make a Windows user feel much more comfortable.

Whether a company decides to use open source or not, one topic that needs to be kept in mind is how well a piece of software does with alerting and how customized the alerts can be. Briefly, one issue that some companies have is that they get too many alerts or alarms. Thus, it can be very difficult to decipher which alerts are legitimate and need to be looked at and which ones are false alarms. One size does not fit all, so while and ISP will want alerts on the slightest fluctuations in one of their routers, a company with a remote site will not want to be notified every time the last mile provider has issues on their line.

Connectivity is one of the most common items and equally contains different areas from simple health checks to make sure devices are online, to querying network interfaces verifying they are handling the amount of data passing through. Going from a very broad view to detailed, being able to see what kind of applications are passing through the network is very important.

One of the basic methods include making sure network devices are on the network. This is somewhat trivial but can really direct where troubleshooting begins when a problem arises. As we briefly discussed, Ping is one of the simplest programs that can easily check to see if a device on the network. Essentially, Ping asks the device, can you hear me know? If it receives a reply of yes, then you know it is up and running. This is an invaluable tool to have. For example, as a network admin if you receive a call stating that the wireless is down in a building you can ping the switch that the access points are connected on to make sure it is up and running. This simple task directs where to troubleshoot next and if the physical device needs to be manually looked at.

You could ping every device manually, but that is not very time efficient. Applications were designed to do this automatically based a defined schedule. This is a very simple task that most applications provide.

Nagios provides a great way of performing these tasks as default. As a quick overview “Switches and routers can be monitored easily by "pinging" them to determine packet loss, RTA, etc. If your switch supports SNMP, you can monitor port status, etc. with the *check_snmp* plugin and bandwidth (if you're using MRTG) with the *check_mrtgtraf* plugin. (“Monitoring Routers”)” Once a host is defined in the system you can setup a service to check every 5 minutes to see if the device is active. Nagios by default already has built in certain levels of alerts. Alerts can be triggered as Critical, Warning or OK. Each level by default has thresholds on what to check for. For instance, a device is set in critical condition if there is 60% packet loss of the RTA is greater than 600 milliseconds. If defined, an alert will be emailed notifying you of the alarm as well as once the alarm cleared and the device in the OK status. The checks and notifications can be customized as well.

Zabbix has a similar check as well, but takes a little more customization to achieve the same process as Nagios. You have the option to define how many pings to send, 4 for example and if 3 replies are received, the host is considered to be down.

Along with just checking to make sure a device is active, a check may be needed to make sure a service is running. One example could be a webserver where http and https needs to be verified periodically that they up and running. Again most applications can provide this including the one mentioned here. Very similar to pinging a device this service will check port 80 and 443 and if they don’t receive the expected response an alert will be triggered to send a notification.

Both of these checks are a great way to know if a host or service is down, but also a very basic view of possible networks issues. For example, if you receive an alert that the http service is down on the webserver and when you log in you see that the http service is actually running. Then there could be network issue between the NMS and the webserver related to network saturation or even a routing problem. The point is that having a good monitoring system in place configured properly will help tremendously in troubleshooting system or network issues.

As we went over SNMP is clearly a great way to check on any network device to verify a vast amount of information. However, looking at the security side, it should be impetrative to require that version 3 is supported. With the length of time since version 3 has been introduced, almost all applications, open sourced or not should be able to take leverage this newer version, but it should not be assumed. The software that has been discussed can be used to setup and monitor devices utilizing SNMP version 3. Additionally, there are customized alerts based on the alert level defined.

As of this point, none of the mentioned systems include any configuration management pieces. In the open source space, the choices are somewhat limited as well as their abilities. Equally, these options are generally Linux based. One of the popular options is known as Rancid. In the networking space this is compatible many different vendors. The reason being is that this is essentially a customizable job which runs the commands configured. The data is stored in a file

based architecture and when new checks are performed on each device the data is compared. If there is difference, the program can be configured to send an email with the differences. This is very simple approach to a necessity of keeping up network with backups and when changes were made.

As we went over previously, proactively being able to know how a network is performing is very helpful to stay one step ahead of issues. Using some one of the programs here should be able to assist with this within reason. This is one of the areas where the differences between enterprise software and free software stand out. With SNMP being used to grab most of the information, it should be displayed in a readable graphical format. Some versions may limit how much historical data can be kept in the system which would impact being able to easily compare different periods of time. A possible alternative method would possibly be to manually export data at set periods. Also, limitations may be in place to customize any thresholds that are in place. There may be default settings for critical alerts which may not be ideal for your network needs. Again, these all concerns that should be taken into consideration with considering a free version system.

It may be difficult to find a system that covers all needs. Monitoring a network's performance with protocols such as Netflow or SFLOW would be one of those categories. This is not to say that it does not exist, but finding a solution that does everything in the FCAPS model may be the issue. However, there are open source solutions separate from what has been covered that still do a great job. NTop is a well-known program that provides traffic analysis with ntopng. Again, there is free and relatively affordable paid for version. The main difference between the two pertain to reporting. Viewing traffic live is available as well as historical data, however being able to report in detail for certain time periods would need to paid for.

Looking towards security takes us to authenticating and authorizing users. In the Cisco world there is a proprietary protocol known as TACACS meaning it only works with Cisco products. The alternative to this is Radius which is essentially a no cost option. A popular method would be to use a Windows server. However, in the instance this is not option, FreeRadius is a linux based system with just as much opportunity. Using Radius is a very secure way to authenticating users as well as assigning privileges. It is worth mentioning that there are some extra options to using TACACS if the environment is Cisco. There is the ability to add time of day access which can limit unwanted logins during non-business hours. Additionally, logging successful and failed authentications as well as what commands were entered when logged in is very key when it comes to security. The well-known Cisco program for this is ACS. This can be used for logging and reporting and can provide some added features when dealing with Cisco devices. With all that being said, if the primary goal is to provide an authentication mechanism, radius is more than sufficient.

During this discussion, we briefly looked at the FCAPS model that can be used as a guide on some of the best practices that should be used when it comes to monitoring a network. There are others that can be used as well such as the Telecommunications Management Network and the Information Technology Infrastructure Library just to name a couple more. Simply put, a plan needs to be put in place. These models cover many different areas and there is not a once size fits

all check list. Essentially, you need to know what is connected to the network, how well each supporting device is running and are those devices secure. Depending on what type of service a company provides there may be more emphasis or details in a certain area.

In conclusion it can be said that no matter how small a budget may be, network management is attainable. Some of the open source software mentioned such as Nagios are a great way to accomplish simple checks to see if a device is up or not as well as being SNMP server to run system queries. There are many to choose from, with some being a better fit or easier to implement. It is worth mentioning that there are large companies that utilize some of these products for their environments due to their robustness and ability to customize. Consideration needs to weighed on the pros and cons of each option. The main item being that these will offer virtually no support. So if there is an issue with installing or configuring you are on your own, but not entirely. Most the well-known products have an online community that share an online knowledge base which are a great way to get assistance from peers. Most products have options to choose from so that if there are only enough resources to implement the free version, or if a need is felt to take advantage of some of the features in the enterprise version, they make an easy path to upgrade to do so. With what we have covered for many small and even mid-size companies the free version can handle any network's needs. No matter what the choice is, there are options to choose from.

References

1 - Monitoring Routers and Switches. Retrieved from https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/monitoring-routers.html

2 - Network Management System: Best Practices White Paper. (2007, July 11). Retrieved from http://www.cisco.com/c/en/us/support/docs/availability/high-availability/15114-NMS-bestpractice.html

3 - Davis, David. (2006, June 15). Get to know your logging options in the Cisco IOS. Retrieved from http://www.techrepublic.com/article/get-to-know-your-logging-options-in-the-cisco-ios/

4 - FCAPS White Paper. (2005) Retrieved from http://marco.uminho.pt/~dias/MIECOM/GR/Projs/P2/fcaps-wp.pdf

5 - Curtis, Debra. 2003, June 9). Network Monitoring and Business Communication in MSBs. Retrieved from http://www.bus.umich.edu/KresgePublic/Journals/Gartner/research/115400/115458/115458.html

6 - Sarneso, Emily. (2016, OCT. 3). Why Netflow Data Still Matters. Retrieved from https://insights.sei.cmu.edu/sei_blog/2016/10/why-netflow-data-still-matters.html

7 - SNMPv3 Simple Network Management Protocol. (2003, February). Retrieved from http://academy.delmar.edu/Courses/ITSY2430/eBooks/SNMP(Intro).pdf

8 - Sibai, M. S.,Nguyen, K. L., Thach C. P.,Wu, Yan. Enhancing Syslog and SNMP Traps/Notifications Security. Retrieved from http://cs.gmu.edu/~yhwang1/INFS612/Sample_Projects/Spring_07_GPN_1_Final_Report.pdf

9 - Rouse, Margaret. (2010, November). authentication, authorization, and accounting (AAA). Retreived from http://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting

10 - Cohen, Gidi. (2014, JAN 30). Best practices for network security management. Retrieved from http://www.networkworld.com/article/2173927/tech-primers/best-practices-for-network-security-management.html