Cloud Application Monitoring for Efficient Network Management in Public Schools

Dr. John Pickard, East Carolina University

Dr. Pickard is an Assistant Professor at East Carolina University in the College of Engineering and Technology. He teaches undergraduate and graduate Information and Computer Technology (ICT) courses within the Department of Technology Systems. Dr. Pickard plays an active role in building positive and sustainable industry relationship between the college, local businesses, and industry partners. Current industry recognized certifications include; Cisco Certified Network Professional, Microsoft Certificated Professional, EMC Information Storage and Management, IPv6 Forum Certified Engineer (Gold), IPv6 Forum Certified Trainer (Gold), and Cisco Certified Academy Instructor. Dr. Pickard received his Ph.D. in Technology Management at Indiana State University. He also holds an MBA from Wayland Baptist University and a B.S. in Professional Aeronautics from Embry-Riddle University. Research interests include: IPv6, IPv6 adoption, wireless sensor networks, and industry-academia partnerships.

Mr. Dale Drummond, East Carolina University

Dale Drummond is an Undergraduate Student at East Carolina University in the College of Engineering and Technology. He is currently pursuing his Bachelor of Science in Information and Computer Technology with a concentration in Computer Networking. Mr. Drummond is currently Team Lead/Sr. Network Management Engineer at MCNC, the company which operates the North Carolina Research and Education Network (NCREN). Research interests include IPv6, IPv6 adoption, Application Performance Monitoring, DevOps, and Network Operations Optimization.

Dr. Philip J. Lunsford II, East Carolina University

Phil Lunsford received a B.S. in Electrical Engineering and a M.S. in Electrical Engineering from Georgia Institute of Technology and a Ph.D. in Electrical Engineering from North Carolina State University. He is a registered professional engineer and is currently an Associate Professor at East Carolina University. His research interests include cyber security, telemedicine applications, network performance, and the cross-discipline application of technologies.

Ciprian Popoviciu, Nephos6, Inc.

Dr. Ciprian Popoviciu, MBA, has over 20 years of experience working in various technical and leadership roles in the networking and cloud computing area. Prior to starting Nephos6 he managed the architecture team of Cisco's Engineering Infrastructure Services organization where he defined the strategy and led the execution of the internal DC consolidation and transition to cloud. He is an industry recognized domain expert in IPv6 who, over the past 15 years worked on the strategy, architecture, implementation and validation of IPv6 adoption by large service providers and enterprises Worldwide. Ciprian worked with various governments on defining national level and agency level IPv6 strategies and standards. Ciprian authored two Cisco Press books and co-authored 5 IETF RFCs and multiple patents. Ciprian is an IPv6 Forum Fellow and a Cisco Champion. He is a frequent speaker to industry events and conferences and he is an active contributor to various technology and scientific publications.

Cloud Application Monitoring for Efficient Network Management in K-12 Schools

Abstract

With the increased movement of administrative, operational, and educational tools from on-premise resources to hosted or Software as a Service (SaaS) offerings, K-12 and post-secondary school administrators are placing increasing demands on the network, applications used, and staff supporting those applications. As the importance of the network's role in day-to-day education operations increases, new ways to measure how the network and services provided over the network are performing are needed.

This paper will present the details of a multi-semester undergraduate research project to measure the quantifiable benefits of shifting from a traditional network monitoring approach to application performance or user experience approach in a K-12 school system. This novel approach aids school administrators and IT support staff in reducing the time needed to identify, isolate, and resolve performance issues experienced by end users.

Distributed network performance monitoring agents are used to collect extensive User Experience focused data for external web resources identified by the school administrators and IT Support staff as being vital to school operations or delivery of their curriculum. Measurements for DNS resolution time, TCP/IP communications response time, and HTTP load times (User Experience) are captured by each monitoring agent, recorded and then analyzed. The monitoring agents, both wired and wireless, are distributed at 36 individual schools: 20 elementary schools, seven middle schools, and nine high schools. Monitoring agents are also placed at the school district's Central Office (CO) and Internet Service Provider (ISP). Identical measurements are recorded from each agent at a polling interval ranging from 10 minutes to 1-hour dependent on the importance of the service being monitored. Higher importance services are monitored more frequently than lower importance services. Data analysis is applied to establish a performance baseline for each service, at each agent location, over the same time window.

The data collected and presented enables the limited IT staff of the school district to identify performance issues promptly and automatically narrow down the fault domain. The methodologies employed and shared in this study will allow for automatic and proactive notification of the support staff, enabling issues to be addressed before being reported by end users.

Keywords

Undergraduate laboratories, undergraduate projects, user experience, network analytics, K-12 schools, technology management, cloud services, performance monitoring

Problem statement

K -12 schools across the nation are moving the resources that their information technology departments once provided locally, to Cloud Services offered by many different providers [1], [2], [3]. A 2013 study by the Fordham University, Center for Law and Information Policy, conducted a nationwide survey of school districts to determine the prevalence of cloud services in the district's IT resource portfolio. In that survey it was found that of the school districts which replied, "95% of districts rely on cloud services for a diverse range of functions including data mining related to student performance, support for classroom activities, student guidance, data hosting, as well as special services such as cafeteria payments and transportation planning." [4]

This increased reliance on cloud services, coupled with limited IT staff and resources, makes it difficult to monitor and support, with traditional network management tools, a portfolio of offerings which are hosted outside the district's administrative domain and often spanning multiple administrative domains on the way to and from the district [5]. Also, network management systems must provide the IT administrative staff a means to manage the quality of service (QoS) and service level agreements (SLAs) they have with their internal customers [6]. For issues with these new services to be identified, isolated, and resolved, new methodologies and toolsets are required. By utilizing these new toolsets to collect and analyze these new metrics, network administrators will be able to identify the issue, the administrative domain in which the problem occurred, and will be able to verify the issue is resolved after the appropriate corrective action has been taken.

What to measure?

Traditional network management systems (NMS) rely on basic connectivity and latency tests to measure the performance of the devices within the local administrative domain. These systems typically do not measure application performance or User Experience (UX). In most IT organizations specific attention is paid to the performance of the network with less emphasis placed on the performance of the applications used on top of the network.

Focusing on User Experience or Application Performance Monitoring (APM), along with the traditional network performance metrics being measured, can provide IT staff with better insight into what their clients are experiencing and allow them to verify the existence of and resolve issues in a timelier manner. The most useful test that can be added with a UX or APM toolset is a synthetic transaction test. By simulating a user accessing a specific resource both within and outside the local administrative domain, administrators will get a view of the performance that the user is experiencing at that particular time. Many cloud-based applications are accessed through a standard web browser and are uniquely suited for UX and APM testing.

The data gathered by the UX and APM tests will show the time it takes for a specific cloud-based application to be accessed, the path that the transaction takes through the local administrative domain, and any other administrative domains it traverses, as well as round-trip latency. This monitor integrates some of the basic network latency functionality that traditional NMS use along with providing a detailed breakdown of the transaction. The metrics collected include each stage of the transaction between the end-user and the cloud-based application. This breakdown will record the time it takes for the following parts of the transaction: The Domain

Name Service (DNS) response, Connect, Secure Socket Layer (SSL) if it is used, Send, Wait, and Receive, for each of the resources on the target application that is monitored. Collecting this detailed data, along with the latency and path information provided by Ping and Traceroute, will give a comprehensive view of the application performance and will provide a higher fidelity indication of the user's experience.

Survey of existing tools

The move of resources from locally managed to cloud-based or hosted solutions creates a need for a new type of network management toolset. This toolset must allow network administrators to gather meaningful information about the resources their users' access. Meaningful data must be collected even when the resource is no longer part of their administrative domain. However, the monitoring tools often used today, such as Simple Network Management Protocol (SNMP), Ping, Traceroute, NetFlow, and Syslog, are often unable to cross administrative boundaries due to security policies and network configuration.

It is extremely rare for network administrators to monitor resources outside their administrative domain with these traditional tools. Once services move to the cloud, these methods are usually not available, with the possible exceptions of Ping and Traceroute, although, those tools could both potentially be administratively prohibited along the path to the resource. Table 1 lists conventional network monitoring system (NMS) tools and the scope of administrative domains they cover.

Table 1. Network monitoring system tools and scope of administrative domains

Existing NMS Tools	
Tool or Protocol	**Administrative Domains Covered**
SNMP	LOCAL
Ping	ALL (if not administratively prohibited)
Traceroute	ALL (if not administratively prohibited)
Netflow	LOCAL
SolarWinds (SNMP)	LOCAL
Cisco Prime Network	LOCAL
Syslog	LOCAL

Gathering metrics allowing network administrators to validate the performance of the cloud resources requires that additional tools be brought into the network management portfolio. For this research project, we chose ITSonar© as the tool used to measure the User Experience and Application Performance. ITSonar© is not intended to be a replacement for the existing network management tools being used, but rather as an additional tool that can provide a view of the user experience, baselining of resource performance, and fault isolation. This will provide an end-to-end picture of the user experience of the off-premise applications being used.

Figure 1 provides a breakdown of where each tool in Table 1 is most commonly used and where user experience monitoring software such as ITSonar© fits into the NMS toolset.

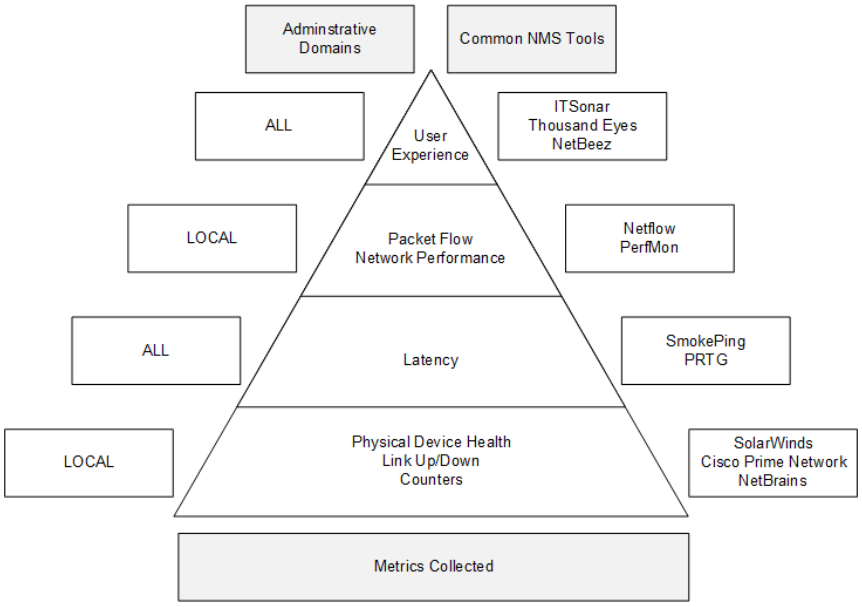

Figure 1. Network Monitoring Metrics Collected, Administrative Domains, and Examples.

Project description

This undergraduate student research project will be completed in three phases.

Phase I (Spring 2018):

As a pilot, a total of fourteen ITSonar© agents will be deployed at two locations in the school district's network. Four agents, all wired, will be placed at the school district central office and ten agents, some wired and some wireless, will be deployed at one of the district schools. This initial phase will allow for validation of the deployment design, as well as enable the district's network administrators to familiarize themselves with the ITSonar© configuration process and Dashboard.

Phase II (Summer 2018):

After completing the pilot during the initial phase of the project, additional agents will be deployed in a small number of other schools and at the school district's ISP. The additional agents and locations will give further insight into another of the administrative domains the user session must traverse when accessing the cloud resource. Also, data from all agents will be collected and analyzed to determine if any consistent issues are identified, and steps can be taken to remediate those issues.

Phase III: (Fall 2018):

After successful completion of the second phase, approximately 10-20 agents per school will be deployed in each school in the district. The number of agents implemented will be dependent on

the size of the school and the network that needs to be monitored. Data will be collected and analyzed for all the agents and analysis of the data will be used to resolve user complaints the schools received regarding accessing the cloud resources. After this phase, a comparison of help-desk ticket trends will be made to determine if using agents to monitor User Experience has a noticeable effect on the Mean Time to Resolution (MTTR) for those tickets opened concerning cloud services.

Project design and implementation

Collection of the new metrics requires that multiple ITSonar© agents be installed. These agents will be placed in the network at various locations throughout the school district. This will allow for Cloud Services statistics to be monitored by all agents and the data aggregated for collection and analysis. Each school will have multiple agents distributed on each floor and in various classrooms to provide a representative sample of cloud services performance from across that school's network.

For this experiment, hardware agents running the ITSonar© software agent will be running on either Raspberry Pi Zero W, for wireless agents or Raspberry Pi3 for wired agents. Agents will be installed at individual schools in the district. Agents will also be installed at the school district's central office and in the network of the school district's Internet Service Provider (ISP).

In the school district where the experiment is taking place, none of the individual schools connect directly to the public Internet. Instead, each school’s Wide Area Network (WAN) links connect to the school district central office where there is a high bandwidth connection to the district's ISP. Figure 2 shows a logical topology of the proposed agent locations within the school district network. Both wired and wireless agents will be used at the schools to provide a closer representation of how a user would access the network and the cloud resources. Having multiple types of agents, in various locations at a school, allows for higher fidelity measurements of user experience.

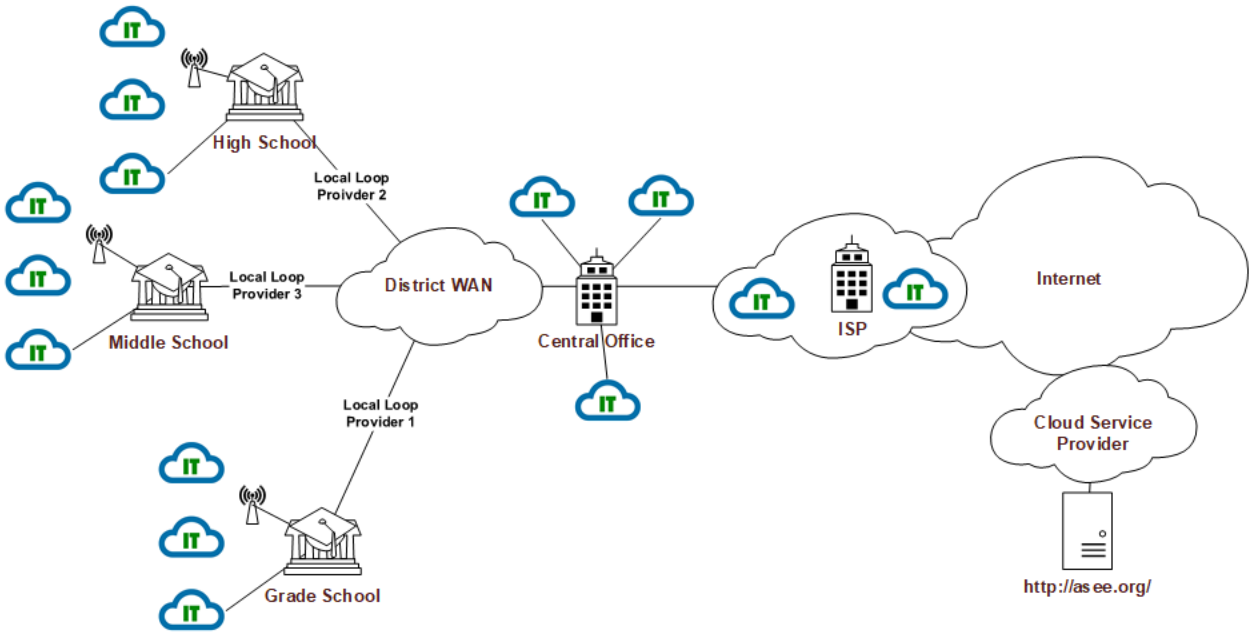

Figure 2. ITSonar© agent locations within the school district network.

Traditional NMS tools typically only collect data within a single administrative domain. With cloud services, sessions must transverse multiple administrative domains. If a problem occurs outside the local administrative domain, it is difficult to know where along the path, or in which of the other administrative domain the issue is located. The ITSonar© back-end systems look at the measurements from agents in all domains and perform initial fault isolation. This fault isolation can assist network administrators in troubleshooting the issue, getting the right support organizations involved earlier in the investigation, and providing faster Mean Time to Resolution. Figure 3 shows the administrative domains involved in this project.

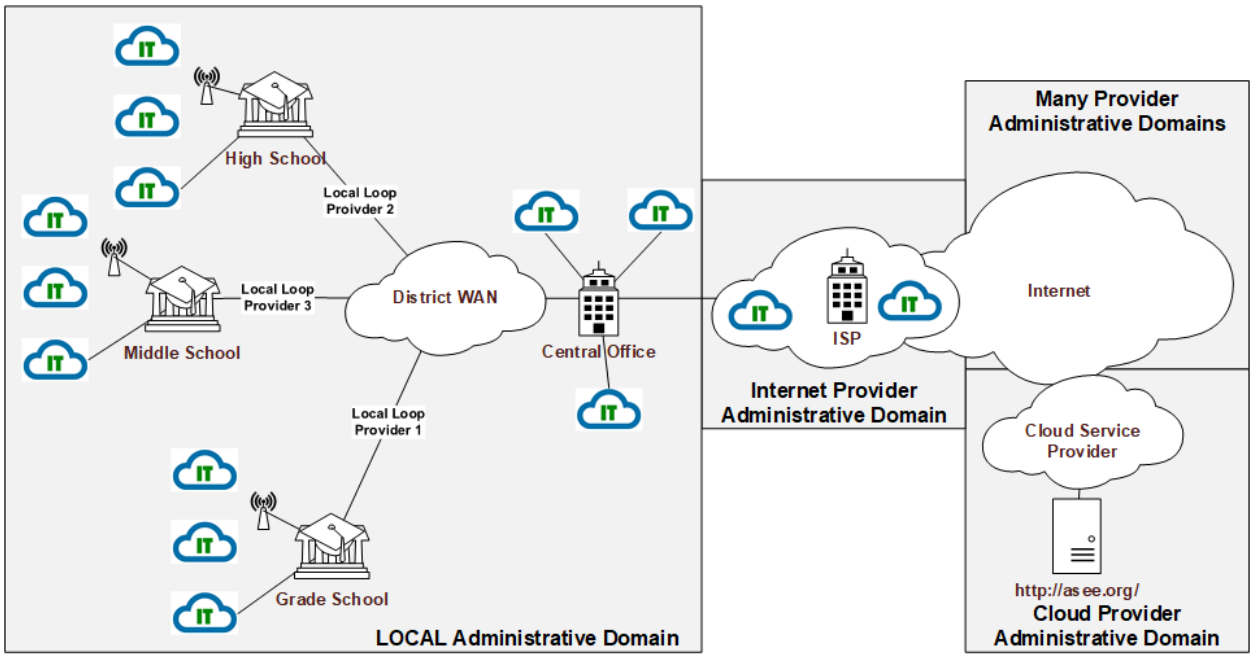

Figure 3. Administrative domain boundaries within the school district.

Once deployed in the appropriate domain, each agent is updated with the current version of the ITSonar© agent software from Nephos6© and will register with the Nephos6© back-end data collector.

An account for the school district and a unique user account for each of the Network Administrators was created on the ITSonar© website located at http://www.itsonar.com/. These accounts are used to manage the agents and to manage what measurements, or monitors, are applied to each agent. A monitor is a specific set of performance tests for a specified resource, for example, http://www.asee.org/. For each monitor multiple tests can be configured such as, HTTP Load Time, Ping, Traceroute, and Email (if supported on the monitored site). Also, a time interval defining how often the monitor will be executed can be configured.

The data that is collected for each monitor is stored and analyzed by backend servers maintained by Nephos6©. For each monitor, a performance baseline is automatically created. For data that is subsequently collected each, data point is compared to the previously computed baseline. The Network Administrators can generate alerts based on a percentage deviation from the baseline the newly taken measurements are. A single measurement outside the baseline will not cause an alert to be sent by default. The current threshold is configured so that three successive measurements outside the baseline must be received to generate an alert. This threshold can be configured by the network administrators.

Table 2 lists sites currently monitored by the school district as part of phase 1 of the study.

Table 2. Sites currently monitored by the school district and the number of ITSonar© agents configured to monitor each site

Monitors	
Cloud Services	**Number of Agents**
https://www.google.com/	4
http://www.powerschool.com/	4

Project summary and future work

Phase I of this project is currently underway and four of the initial fourteen ITSonar© agents are deployed at the school district central office. Data is currently being recorded about two cloud services that the district uses daily. The information is being collected and stored on ITSonar© backend servers. The school district network administrators have been given access to a dashboard that allows them to modify the configurations of the agents and other account details, review the collected data, and explore the details of individual measurements. Additionally, the administrators can launch on-demand tests from an individual agent or groups of agents for a specific cloud resource as necessary.

Future work will involve providing a mechanism for allowing the agents to authenticate with the school district's web-filtering service. This mechanism will allow for the experiment to have higher fidelity by allowing the synthetic transaction to follow the same path that is taken by the student's and teacher's sessions when accessing the cloud-based resource.

After the solution for the authentication of the web filtering application is verified, the agent deployment will be expanded to the additional schools, with the final goal of having multiple agents deployed at each school in the school district, the school district's central office and their Internet Service Provider.

References

[1] S. Stein, J. Ware, J. Laboy, H. E. Schaffer, “Improving K-12 pedagogy via a Cloud designed for education,” *International Journal of Information Management*, Vol. 33, Issue 1, pp. 235-241, February, 2013.

[2] G.L. Pierce, and P.F. Cleary, "The K-12 educational technology value chain,” *Education and Information Technologies*, vol. 21, no. 4, pp. 863-880, July 1, 2016.

[3] D. Kapuler, “Cloud collaboration tools: now or later?*” Tech & Learning,* vol. 35, no 9, pp. 26-28. March 26, 2015. [Online]. Available: https://www.techlearning.com/resources.

[4] J. Reidenberg, N. C. Russell, J. Kovnot, T.B. Norton, R. Cloutier, and D. Alvarado, "*Executive Summary*” in Privacy and cloud computing in public schools, New York: Fordham Center on Law and Information Policy, December 13, 2013.

[5] J. Panneerselvam, L. Liu, R. Hill, Y. Zhan, and W. Liu (2012), “An investigation of the effect of cloud computing on network management,” in *High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS),* Liverpool, U.K, June 25-27, 2012, pp. 1794-1799.

[6] S. Erfani, V. Lawrence, M. Malek, B. Sugla, “Network Management: Emerging Trends and Challenges,” *Bell Labs Technical Journal,* vol. 4, no. 4, pp. 3-22, October, 1999.