Peak XV Networks

White Paper

Benefits of an Enhanced Network Operations Center for Service Providers

Phil Marasco
Manager, Peak XV Services Management Center

August 30, 2001

Introduction

As service providers seek to streamline their businesses within a challenging telecommunications marketplace, many firms must obtain flexible, scalable world-class infrastructure without major capital expenditures. At the heart of every service provider is a NOC (Network Operations Center) that is expensive to build, maintain and upgrade, yet which has a limited operational life span and must track to ever-changing market requirements.

Under these conditions, how is a service provider to design infrastructure that fulfills business objectives without making a major investment? In addition, how can service providers complement their existing NOCs with computing systems, applications and expertise that extends their capabilities seamlessly?

There is a new generation of infrastructure taking hold in the marketplace – the Enhanced Network Operations Center (ENOC) that is poised to change the way service providers operate their businesses and increase efficiency. This paper answers questions about the next generation of NOC management and offers service providers with a model of successful operations. In addition, this paper is designed to help service providers assess their infrastructure requirements and see how the landscape of the industry is shifting.

Tools of the trade

A growing service provider has multiple requirements to run their businesses successfully. These are frequently companies with resources located on a public accessible network (Internet) either offering or consuming IP (Internet Protocol – layer 3 and above) services. These services can be to or from one or many locations. Service providers have equipment that must be monitored for Internet access, applications, and operating system metrics. If the provider owns their network backbone, they have routers and switches that must also be monitored. Other possible devices that must be monitored include Managed Firewalls, Voice over IP solutions and Streaming Media. Service providers may also need version control services for code running within their infrastructure, which, although sounding simple, can be quite complex in today’s environment of tailored code distributions and undiscovered back doors. Many ISPs and smaller ILECs have multiple versions of code in deployment depending upon system and bandwidth requirements.

Finally, a number of firms need frontline support services as an alternative to purchasing support contracts from third-party vendors. For smaller ISPs and those just entering the broadband market, many organizations need a way to increase infrastructure deployment without growing their internal support personnel for this unique equipment.

With such complex requirements – and many others – most service providers continue to search for the optimal balance of resources. So what are the alternatives used by the savviest operators in the industry and what changes are evolving in the marketplace?

State of the Industry: Striving for responsive, efficient Network Management

Traditional NOC offerings to support service providers have typically relied upon a reactive approach to network support. Many service providers wait until a network condition violates a preset threshold, activating an alarm that prompts attention by an administrator. Traditional NOC monitoring scenarios are modeled upon this type of response, yet there are several hazards that come with it.

First, reactive tools only assist with the event triggering the alarm. They do not assist in predicting the next alarm. Reactive alarms also do not show events hovering near their threshold limits.

The second problem with traditional NOC implementations is that many polling methods used to determine network health can actually bring down an ailing server. If the polling request takes too much bandwidth or asks the processor to do too much, a server can crash. This situation occurs frequently since many routers and other web devices run close to peak tolerances during daily rush hour periods.

The third problem with traditional NOC implementations is that once data from an alarm is used it is usually discarded. There is no form of collective learning that occurs within the NOC to remedy future problems before they begin. While the alarm data is useful for each event, it is even more useful when combined with all alarms to show the bigger picture. By collecting the history of events, service providers can analyze network trends and identify infrastructure trouble spots. A single alarm, by itself, may not provide much for the long-term data analysis that many technical firms need. However if that alarm data is multiplied 10,000 times and across thousands of occurrences then the data collected turns into an action plan.

What it takes to build a NOC

To address these multiple challenges, many service providers have had no choice but to construct their own NOCs. This process is not only expensive and complex, but also time consuming and a never-ending responsibility. There are four main areas that must be addressed for any NOC project, whether if it is built from the ground up or acquired as a going concern: Facilities, Equipment/Applications, Staff, Processes & Procedures. Any service provider must take the following requirements into account as part of their operational plan.

Facilities

A physical location close to parking, highways, and Network Access Points (NAP's) is required. This location must have a secured infrastructure (secure logged entry, cameras, and secure connectivity). The facility must be able to provide well-conditioned power and telephony and have a climate control system capable of supporting the heat generated by a facility operating 24 hours a day. It must have a generator to provide back-up power. Connectivity is also considered to be part of the infrastructure and as such, must be fully redundant with multiple links through different Tier 1 providers.

The facility must be equipped with visual screens and speakers to ensure that all data will be noticed. For example, the NOC should be outfitted with wall mounted visual screens as well as mounted monitors to ensure that all personnel have a clear view of network activity. These visual alerts should also be accompanied by audible alerts announcing major status changes in monitored nodes and network status.

Equipment

NOC equipment must be chosen carefully due to its mission critical status. For this reason, proven equipment/operating systems should be used as frequently as possible. Redundant power supplies, network connections, and Redundant Arrays of Independent Disks (RAID) should all be a part of the network’s infrastructure. Spare independent disks should be on hand to prevent potential data loss. The network should fully utilize managed switches and hardware routers. Security should be multi-tiered with hardware firewalls used as the first line of defense. The phone system should be an enterprise level Private Branch Exchange (PBX) with battery backup, advanced call routing functions, and should utilize an advanced Automatic Call Distribution (ACD) system. The ACD will efficiently manage call queues and provide call statistics (i.e. Number of total calls, abandoned calls, average speed to answer, average length of call, individual statistics, etc.).

Applications

Information Systems - The NOC will need a trouble ticketing system to actively record, update, track and close monitored events.

Equipment Contact Database - An equipment and network contact database must be in place and updated regularly for accuracy. Such a database should contain the following:

Software, Firmware, Code Updates - A NOC should aggressively use enhanced database environments to track code problems discovered during performance analysis and lab testing.

Network Documentation - Documentation of the connections between all managed and monitored equipment is required. The diagrams must be updated as changes to the network are made.

Server Monitoring Configuration and Setup Systems- A NOC should provide monitoring of a server for "up/down" status as well as any applications via Simple Network Management Protocol (SNMP).

Staff

Reliable, experienced and educated staffing plays a pivotal role in quickly and effectively running a NOC, troubleshooting outages and upgrading/maintaining equipment. Constant training is required to ensure engineers are educated on new technologies. These skills are necessary to effectively pinpoint fault management and resolve issues.

Processes/Procedures

NOC Monitoring and Informational paths - A NOC must be staffed with qualified people 24 hours a day, 7 days a week. In addition, a NOC must have a reliable network monitoring and alarm system. Once an outage has been identified providers must have defined specific informational paths.

Trouble Tickets - A NOC needs to have a trouble ticketing system utilizing separate schemas to identify and track specific products or events.

Escalation - A NOC needs the ability to escalate trouble issues to facilitate resolution.

Performance Engineering - A key portion of a NOC's service is the ongoing analysis of data provided by threshold alarms and network reports.

Reports - The intent of the monthly report is to provide ongoing up-to-date information on the status of a network.

Equipment Maintenance - In order to optimize network availability, service providers must purchase maintenance on all managed equipment (routers, switches, hubs, and modems). Preferably, this will include on-site repair/replacement contacts for all hardware and software.

Backup Procedures - The NOC must be an integral part of back up and recovery planning. Immediate access to code backups can prevent major outages when faulty code needs to be replaced quickly.

Electrical Outage Drills - No emergency plan can be guaranteed for success and without the proper drills the chances for success decrease significantly.

In light of these various requirements, many service providers are looking for a solution that is faster to deploy, costs less (both to capitalize and operate) and provides the flexibility of service offerings required in today's fast-changing market.

The Smart Alternative to Infrastructure Development: The ENOC

The Enhanced Network Operations Center (ENOC) is an outsourced service that monitors, manages, troubleshoots, and tunes service providers' Internet backbone infrastructure. It also has the added bonus of gathering all network monitor data and processing it to show trends, pinpoint choke points, and make highly advanced analytical models. To ensure zero downtime, an ENOC service includes multiple data providers, a backup generator, a separately metered environment on a dedicated floor, proven chain of escalation for problem resolution, automated scripting installed to alert any and all outages, practice drills and more.

Peak XV (fifteen) Networks has already constructed the world’s first ENOC, called the Services Management Center (SMC). In addition to having the best equipment available in the market, the SMC includes the most complete, performance-tested applications, procedures and staff members to provide a seamless infrastructure service for ISPs, MSPs, Telcos, Enterprise networks and service providers of all types.

In addition to network status and trouble ticket management, the SMC provides the key benefit of reporting to identify and localize problem areas for resolution. Data, such as the top five outage locations, the top five reasons for outage, average meantime-to-restoration, and even SMC average speed-to-answer inbound support calls is available.

To address version control of system applications, Peak XV can patch/upload and configure new code to supported equipment during approved maintenance windows. Code versions in the field are constantly be crosschecked against the master list maintained by the customer.

The SMC also offers frontline support services for supported devices as an alternative to purchasing support contracts from vendors. This service enables service providers to attain maximum market flexibility to customers while keeping costs low.

All mission critical equipment at the SMC has guaranteed electrical power via a gas-powered generator. The facility’s Private Branch Exchange (PBX) and integrated Automatic Call Distributor (ACD) also have power backup. In the event of an outage, the SMC can reroute telephone lines in under five minutes to any other Peak XV facility. Any given machine will have two LAN connections and two switches to choose from in case of LAN or switch failure.

In addition to its equipment and applications, Peak XV’s SMC comes with a full complement of expert staff members. As part of its services, Peak XV will send engineers to a provider’s site to directly survey and assess conditions. Peak XV engineers will request information that will provide a view of what a provider envisions its Network Operation Strategy is and what it will need to grow to be. From that information Peak XV engineers will show how the target strategy can be implemented and its impact on resources while still addressing issues of scale.

As part of its SMC services Peak XV can assess current data processes and structures to recommend methods of integration and streamlining data flow. Service providers gain the benefits of quick dataflow to maximize returns on investment and leverage infrastructure against non-scalar growth.

Peak XV engineers can also recommend methods to resolve impediments to implementation such as re-training, policy positioning, or business model advocacy. Issues that affect subscriber retention, training, and employee empowerment are also addressed. Peak XV also assists with integration plans and processes while educating planners on the immediate vs. long-term needs for a successful project.

Peak XV engineers provide insights into how best to measure, tune, and mine all the data generated by a NOC. NOC data represents not only the health of a company's infrastructure at a given point in time. It also represents an opportunity to show where the next issue will surface and when.

The New Road Ahead: Flexible Service Offerings via Infrastructure Partnerships

The benefits of the ENOC approach are manifold. Now, service providers can enter new markets, expand offerings to match customer requirements, achieve new levels of operational efficiency and save capital, all by working with a partner such as Peak XV and its Services Management Center. This model of outsourced infrastructure is a new level of integration between service providers and represents a shift in the industry toward partnerships, not exclusive ownership of core facilities. As the industry continues to experience consolidation and the landscape transforms into a combination of large, monolithic operators and nimble niche providers, the outsourced infrastructure model will increase in popularity. Savvy operators will capture this opportunity now, opening new businesses and solidifying relationships with customers that will endure well into the future.