

Network Monitoring and Control

In recent years the data network has become an essential and key infrastructure tool necessary to maintaining the day-to-day activities of the business.

More services become increasingly dependent on the IP network infrastructure, whether those are basic E-Mail service, calendar sharing and collaboration services, web browsing, through telephony services, CRM, ERP, corporate accounting, that without them the business is literally paralyzed.

There are hardly any large organizations that can function properly nowadays without a properly working communications network, and the number of organizations that can't function at all without it is growing by the day.

A direct result is that the organizational communications network, and in many cases the internet connection itself, is the most important factor for the functioning of the organization, and the requirement is to have them available as close as possible to 100% of the time. It is obvious that 100% availability is unattainable, and as close to it as one can reach, malfunctions will still be inseparable, and therefore should be dealt with in the best possible way.

Every physician knows that diagnosis constitutes a large percentage, if not the majority, of the process of solving a symptom. An accurate and prompt diagnosis of a malfunction can lead to a resolution sometimes in timeframes of minutes or even seconds, instead of hours or days.

With tools for long-term monitoring it is possible, in most cases, to diagnose malfunction and analyze their root cause even before they happen, thus preventing them completely.

PurePeak specializes in network monitoring and control solutions, both remotely and by deploying a monitoring system in the customer's premises. Real-time Network Monitoring:

Provides ability to monitor devices up to scales of tens of thousands of different services, starting from availability checks of devices, through web services, and reaching to measurements of temperatures in different devices, RPMs of the fans, and connections or disconnections of devices from switches.

In fact, this service allows the monitoring of every piece of data that can be collected through SNMP, is reported using SNMP traps, and sampling of services over TCP and other common network services.

The monitoring system can be configured to react upon threshold crossing or upon many kinds of events, and can alert in real-time in Email, SMS or Instant Messages, or the relevant party in the organization, relying on predefined configuration of date and time, severity of the problem, the type of the device, and so forth. Long-term Systems Monitoring:

Graph-based systems monitoring for long term analysis.

The service allows measuring any numerical information that is available through SNMP can mathematical calculations thereof for the generation of long term graphs.

Long-term analysis is very beneficial for future predictions and planning, past events inquiries, and most of all – recognize a malfunctions while they form, before they become service degrading. Anomaly Behavioral Pattern Recognition:

Recognition of network behavioral anomalies and executing triggered actions.

The system receives flow information from the network access routers and based on analysis of the data from all routers it recognizes whether there are anomalies in behavior, for example in case one of the network computers is infected with a worm it will try to infect other computers around the world, and the system will recognize the unique behavior. When such cases are detected the system can issue active triggered actions to remove the threat, for example in case of a DoS attack the system can issue a blackhole mechanisms with the ISP, close a port in a switch, etc.

The system can be integrated with the real-time service in order to invoke real-time alters in Email, SMS or Instant Messages. Log Data Collection and Analysis:

A system that collects logs from devices in the network in the form of syslog messages, and stores them in a searchable

database for fast lookups and cross-reference analysis, for example to present all the logs received from a certain device, or all the logs that were received in a certain time of day, or all the logs that have some string that is common to all of them.

The system can be integrated with the real-time service in order to invoke real-time alerts in Email, SMS or Instant Messages. For further information please contact a sales representative and we'll gladly be at your service.
clifinar