

ER-TELECOM

CASE #3

Resource Provisioning / Fault & Performance Management

Project Scope

Major federal telecom service provider:

- Holds more than 11% of the market of broadband internet access in more than 560 cities in Russia.
- Nearly 3 mln. of active equipment
- More than a thousand of equipment types from different manufacturers.

- To decrease the risk of multicast storm;
- To eliminate unnecessary administration tools;
- To implement a «correct» snmp traps addressing and increase the reliability of accident events.

In complex with this solution we developed a toolkit that allows to view the current configuration of the device, save device's configuration, view all saved configuration files for this type of devices, compare two configuration files and restore the configuration file from CVS using the program's interface.

Key possibilities of Configuration Management module:

- Gathering of config information from network devices in a manual and automatic mode;
- Storing the history of configuration changes for every managed device;
- Visualization of configuration changes;
- Comparison of initial and configuration in performance;
- Given policies configuration accordance control
- Generation of equipment configuration file;
- Loading of the chosen configuration file to the device on the operator's request;
- Running the network device's configuration tasks in automatic and manual mode;
- Displaying of device list for which the tasks were successfully or unsuccessfully finished;
- Use of additionally developed scenarios for gathering and distribution of the configuration files of the

Challenge

Modern network infrastructure is usually multivendor. Unauthorized or incorrect actions towards any of its components can affect whole network infrastructure, which in turn can seriously affect business processes of the company, the quality of provided services or even create an emergency situation. The lack of equipment configuration policies management possibility is a serious problem for the telecom operator. It creates real risks for successful service provision. The effects of such faults are significant, and their complexity has a tendency to progress non-linearly. Because of that a process of incorrect network equipment settings analysis and elimination has been created.

Configuration parameter normalization allows:

- To use other abilities of Equipment Manager system, for example, the realization of reliable network topology and its correlation with the use of LLDP settings;



The configuration management solution allowed our access network engineers to spend less time analyzing the problem caused by incorrect device settings – now this process is mostly automated, and if an accident occurs, its effects are minimized, and it can be solved in a few minutes time.

Isaev Victor,

Leading Engineer of the monitoring center
JSC "ER-Telecom Holding"

network equipment, nominal support of which is nonexistent in the management tools;

- Support of equipment from different suppliers: Cisco, Juniper, D-Link, Zyxel, Huawei, AddPac, Revolution, Microtic, Ubiquiti, Audiocodes.

Active equipment monitoring:

- Observation of the active equipment's state with the use of flexibly tuned monitoring parameters by any open protocol of information access (SNMP, SysLog, Telnet, ICMP, text etc.);
- Flexible tuning of event processing in the system;
- Visualization of equipment state on the network scheme;
- Registration and analytics of events that occur on the active equipment;
- Operative notification of the staff members about the network events according to their area of responsibility;
- Long-term storage of the events that allows operating unlimited amounts of monitoring data.

RESULTS

- Errors related to unauthorized changes or incorrect settings of device configuration are terminated.
- A possibility of automatic setting of standard configuration on the equipment was implemented. These processes can be performed by the staff members that do not have a high level of qualification.
- A high level of network device access security is created by storing all the passwords in the Equip-

ment Manager system. There is no need of telling the passwords to staff now. Access to the devices through the system is registered in the configuration management module.

- Any attempts of changing of the configuration of network devices are being registered by the system and notified to the staff on duty.
- Automatic recovery of standard configuration in case of failures or errors allows to solve the problem in short time.
- Reducing the time needed for an accident termination improves the SLA indicators of the network provider.

SOLUTION

To solve this problem a network configuration management module was created along with the mechanisms that allow gathering and storing of current configurations. This module allowed our client to work with standard configurations for different types of equipment and network segments. During the periodical polling of the network devices device's configuration is compared to the standard one, and if there are any faults, the system automatically notifies the duty personnel by generating an event in the Fault Management module.

A configuration validation process has been created: comparison of standard and current values on the equipment, for example: the version of firmware, configuration command and other. If any faults are detected, then an event is created in the Fault Management module. All the faults detected are being fixated by the event's attributes.