SW Check: What's Happening In My Network?

Quality and reliability are key differentiators in the competitive network market and therefore, tools to improve this are critical. SW Check from WTL allows operators to monitor 1000s of performance indicators from 100s of multi-vendor devices.
Information is presented clearly and concisely so that problems are flagged and handled quickly. Based on the industry-standard open source Nagios & check_mk alarm monitoring software SW Check supports all WTL products and has been tailored to manage the wide range of applications that we offer.

SW Check at a glance:

- Configurable alarm tool
- Generates email warnings
- Manages multi-vendor equipment
- Monitors carriers, servers, line quality, call patterns etc
- Graphical display of performance over time
- Historical data available for comparison/analysis
- Open source base gives access to library of existing add-ons

Main Features

Running a telecoms network relies on accurate, up to date information. All relevant data must be displayed in easy to understand ways. SW Check from World Telecom Labs does this by monitoring the health and operation of any number of our switches, applications, servers and external devices.

- Graphical display of switches and trunks
- 'Zoomable' graphs allow drill down to period of interest
- Graph trends over days, weeks or months
- Simple colour coding to indicate alarms received
- Ability to view recent alarms
- Choose which switches to monitor and how frequently (default every minute)
- Instant view of total calls & ASR per switch and per carrier
- Emails sent if certain events occur
- Auto-learning of new services & hardware running on switch, no configuration needed
- Add new switches easily with a few clicks through the GUI

Sophisticated Email-based reporting supported

SW Check is designed for unattended operation. There is a highly configurable system of email-based reporting available managed through an easy to use graphical interface:

- Configurable limits before emails are sent ('Warning' & 'Critical' levels)
- Different action rules for day and night (so emails can be sent when engineers off-duty)
- Multiple engineers' email addresses can be included
- Different alarm levels trigger emails to different people (for example, send carrier alarms to switch engineer, account balance alarms to customer service department)
- Definable escalation policies

Specific Checks Available

WTL Switches

- CPU, memory & disk usage
- Ping times for IP of switch's management interface

All Trunks

- Trunk full status alarm
- Timeout alarms
- Capacity in use v. capacity available
- Out of Service indication (how many channels)

VoIP Trunks

- Packet loss per carrier. Ability to set thresholds for 'Warning' and 'Critical' level

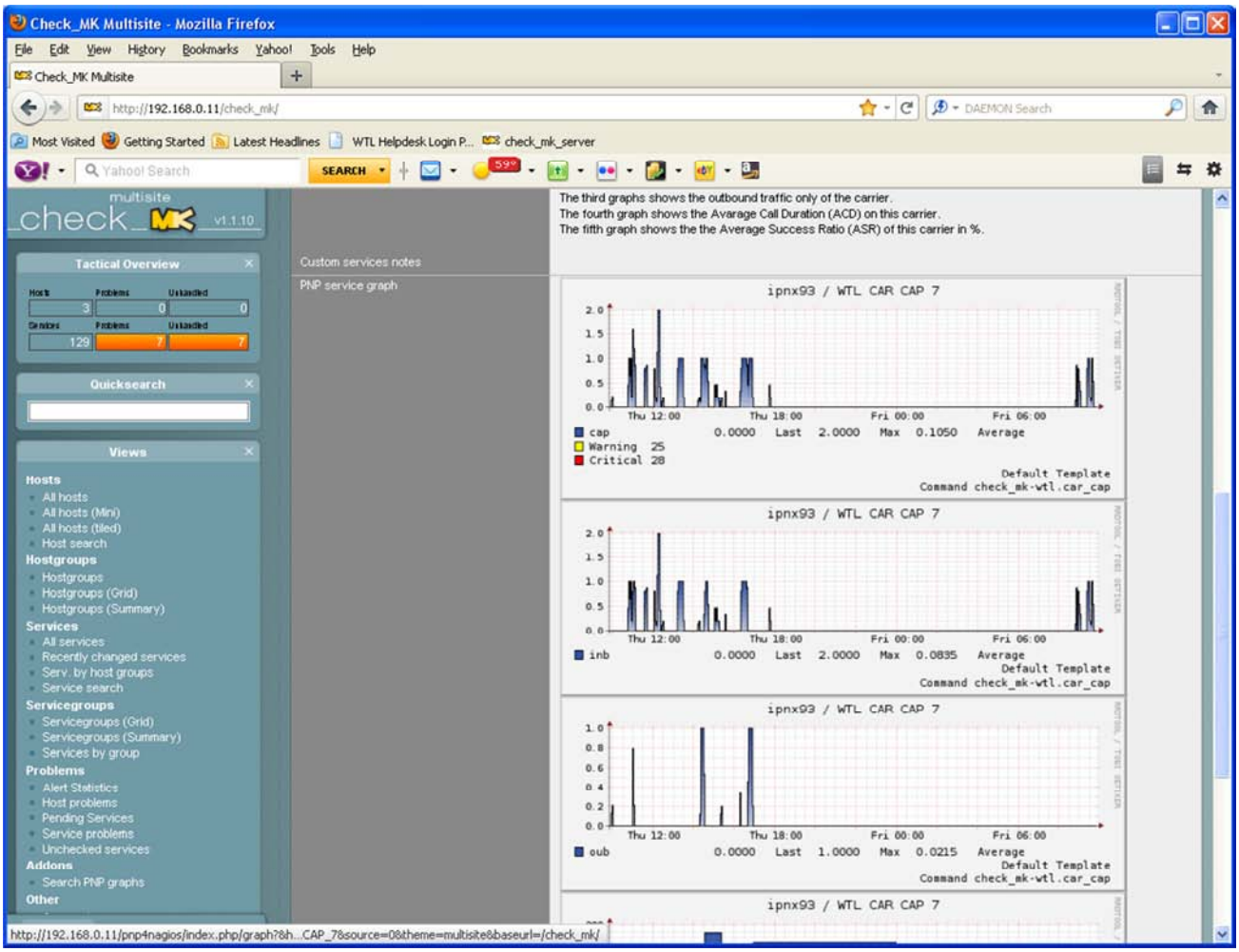

Figure 1: Carrier Traffic Overview Graphs

Application Alarms

- No calls detected for x time
- Bad PIN entered
- Excessive number of zero length calls
- Pre-Paid Account balance exhausted
- Maximum number of allowed daily minutes per account exceeded

SW Admin

- CPU, memory & disk usage
- Status of SQL, Call Data Import, Table Replicator (Running Y/N)

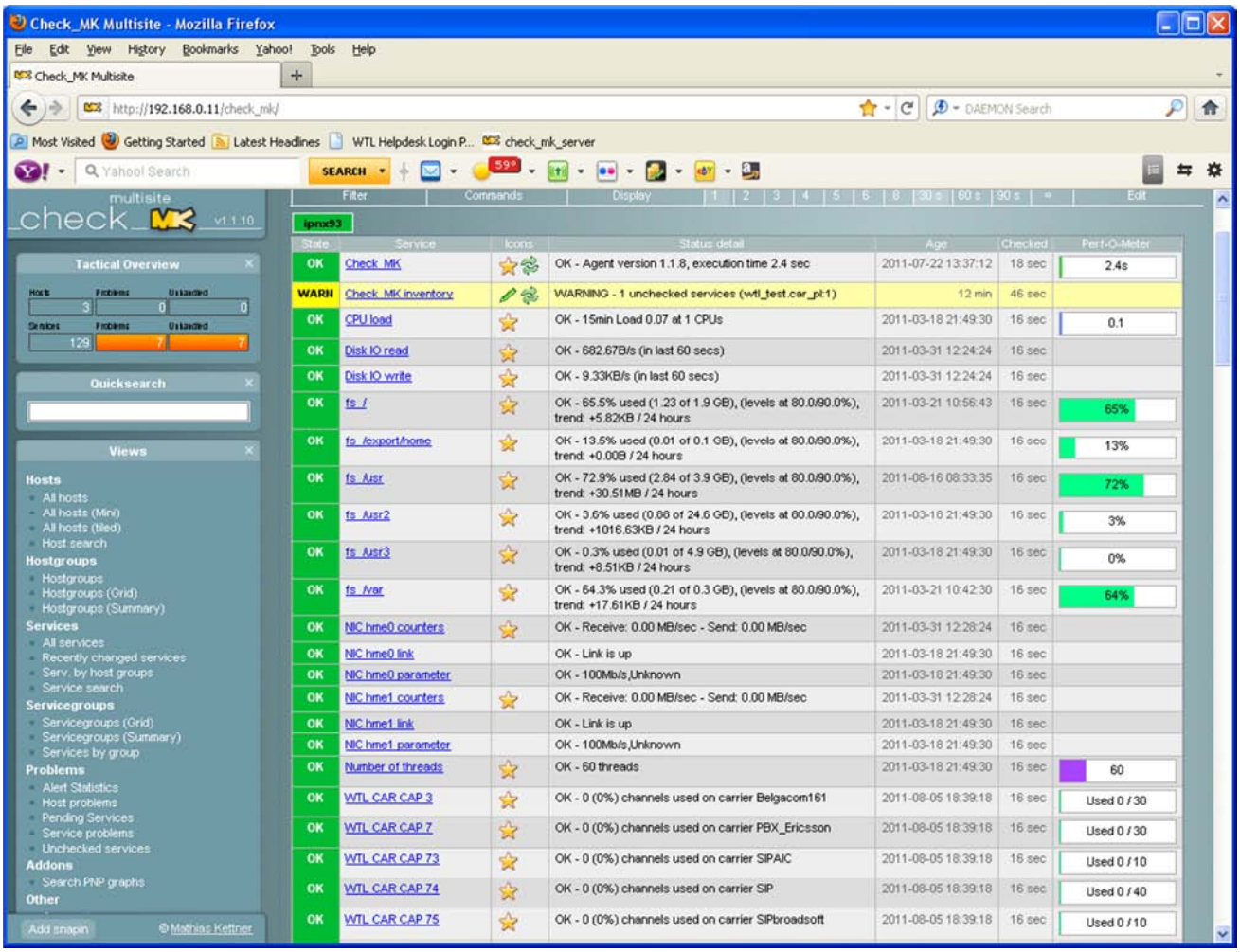

Figure 2: General Overview of all Configured Alarms

RADIUS

- Application running Y/N?
- Sessions rejected (%)
- Total data charged (in Kb)
- Message rate per min
- Resent messages (%)
- Average authorisation response time
- Average accounting response time

Alarms for RADIUS fault events include:

- missing mandatory parameters or format error
- error sending radius message
- configuration error/resource exhausted
- comp database error
- webconnect error
- webconnect request rejected by server
- MAP error
- Access-Request authentication error

- PIN database error
- CLI blocked
- Session database error
- Session peer database error
- Access-Request rating error
- Session identifcation error
- Radius client rejected

System Architecture & Deliverables

A dedicated SW Check server running Debian Linux has an IP connection to one of the WTL switches in the network. From here all interconnected WTL switches can be monitored – however, a management IP connection is required to every switch being monitored (this can be done using private IP addresses). wnmon is used to interrogate the local switch. It is then check_mk that contacts each switch on a timed basis to collect the full reports.

SW Check is delivered pre-installed on a WTL Linux-based Alarm Server. The product consists of a single module with support for all features described here. Customers are welcome to add checks for other vendors' products from the Open Source community. For security and reliability reasons however, we do not encourage customer-authored checks of the WTL switches.

As standard, WTL supply the application pre-installed on a server of the following specification:

Processor, Memory and Disk:
Intel® Atom™ Processor D510 (Dual Core, 1M Cache, 1.66 GHz)
1GB 128M x 64-Bit DDR2-800 CL 200-Pin SODIMM, 1x160GB SATA hard drive

About Nagios and check_mk

Nagios is a powerful, open-source based monitoring system that enables organizations to identify and resolve IT infrastructure problems before they affect critical business processes.

First launched in 1999, Nagios has grown to include thousands of projects developed by the worldwide Nagios community. Nagios is officially sponsored by Nagios Enterprises, which supports the community in a number of different ways through sales of its commercial products and services.

Nagios is capable of monitoring your entire IT infrastructure to ensure systems, applications, services, and business processes are functioning properly. In the event of a failure, Nagios can alert technical staff of the problem, allowing them to begin remediation processes before outages affect business processes, end-users, or customers.

The check and inventory system Check_mk is a general purpose Nagios plugin for retrieving data. It adopts a new approach for collecting data which features a significant reduction of CPU use on the Nagios host. It gives an automatic inventory of items to be checked, and is especially useful with larger Nagios installations. It is used in SW Check because it is very fast, and supports efficient distributed monitoring.