MONITORING OF NETWORKED MACHINES AND DEVICES IN MANUFACTURING NETWORKS

FABISIAK, B.

Abstract: *The monitoring of networked machines, devices and technology equipment in manufacturing networks is an important part of the production process. The methods presented here use the following standard protocols and software modules: a set of UNIX operating system commands and selected software tools available via the Internet on GNU license. To acquire the raw data representing the status of selected resources and production machines via a local manufacturing network, the presented methods use selected diagnostic software for the network devices. After obtaining the raw data-set, specific UNIX commands are used to provide the final data in a format appropriate for monitoring front-end software, and can be easily displayed using a regular web browser. The set of software modules combined makes a very useful and easy to utilize, flexible monitoring system, capable of being implemented in small, medium and large-size manufacturing systems.*

Key words: *manufacturing, machines, monitoring, network, technology equipment*

Author's data: Dr.-Eng. **Fabisiak**, B[oleslaw], West Pomeranian University of Technology, Faculty for Mechanical Engineering and Mechatronics, Institute for Mechanical Technology, Al. Piastow 19, PL-70-310, Szczecin, Poland,fabisiak@zut.edu.pl

This Publication has to be referred as: Fabisiak, B[oleslaw] (2010). Monitoring of Networked Machines and Devices in Manufacturing Networks, Chapter 14 in DAAAM International Scientific Book 2010, pp. 129-140, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-901509-74-2, ISSN 1726-9687, Vienna, Austria
DOI: 10.2507/daaam.scibook.2010.14

1. Introduction

Most modern manufacturing systems are composed of a set of machines, machine tools, work centers, robots and other technological devices such as: assembly, transportation and measurement devices, each controlled by different generations of numeric control units.

Control units of the newest production machines, robots and manufacturing devices mentioned usually have their own control unit with integrated, built-in or add-on NIC (network interface card) and therefore can be easy connected directly to a local manufacturing network. However, some older types of control units may still use previous generations of CNC (Computer Numerical Control) or DNC (Direct Numerical Control) unit sand may therefore be connected to a local manufacturing network with an intermediary of work cell computers -using classic industrial interfaces, like serial RS-232 interfaces and/or other machine specific interfaces.

Each such networked machine, robot or technology equipment has its own specific IP address, capable of being monitored via the manufacturing network, using standard TCP/IP protocol. On other hand, all network devices such as:

- servers, routers
- workstations, and work cell computers

use the same standard networking protocols and techniques to provide internal (LAN-related) and external (WAN-related) communication between all components of the manufacturing systems. This allows the use of the same monitoring tools and data acquisition methods for monitoring of all internal and external resources.

For proper internal communication within local manufacturing networks, especially for the data transfer between:

- Computer Aided Design (CAD) systems,
- Computer Aided Manufacturing (CAM) systems
- Computer Aided Production Planning (CAPP) systems
- workshop floor control and management systems
- networked machines, robots and other technological devices
- and other systems - like global MRPII/ERP systems

will require a reliable, secure and constantly monitored local network environment.

Additionally, an important part of the communication process is the external communication between manufacturing systems and other external subsystems (like: supervision, service, maintenance, external supply, distribution or wholesale subsystems). External communication is usually realized via the interconnection of manufacturing systems to WAN (Wide Area Networks) using telecommunication companies or local internet service providers. In these cases, the constant monitoring of WAN network connections is also required.

The basic concept for the monitoring method presented here is the use of standard informatics tools for constant monitoring of selected internal and external "check-points" within manufacturing networks, such as: UNIX system commands and software modules available as built-in scripts (as a part of UNIX systems) or available for download via the network for licensed use.

2. Network Traffic Monitoring

There are a number of software tools available, which can be used for the monitoring of network resources, most of them are listed on the NMT (Network Monitoring Tools) list, maintained and constantly updated by SLAC, Stanford University(Cottrell, 2010). This article discusses one of the software tools from this list, which is flexible and especially useful for monitoring manufacturing networks- it is MRTG - Multi Route Traffic Grapher (Oetiker, 2010).

The Multi Router Traffic Grapher (MRTG) is primary designed to monitor the traffic load on routers or network interfaces using SNTP (Simple Network Management Protocol).The primary aim for MRTG is to monitor the incoming and outgoing traffic. This software tool generates - in 5 minute intervals - HTML pages containing graphical PNG (Portable Network Graphics) images which provide a live, visual representation of monitored traffic. The monitoring results can be viewed and reviewed using regular web browsers. If the monitored interfaces are interfaces of the manufacturing network gateway– then it is possible to monitor traffic from/to local manufacturing network and represent monitoring results in daily, weekly, monthly and yearly graphs. The sample results achieved in manufacturing system live-traffic monitoring based on MRTG are shown in figure 1 and figure 2 below.

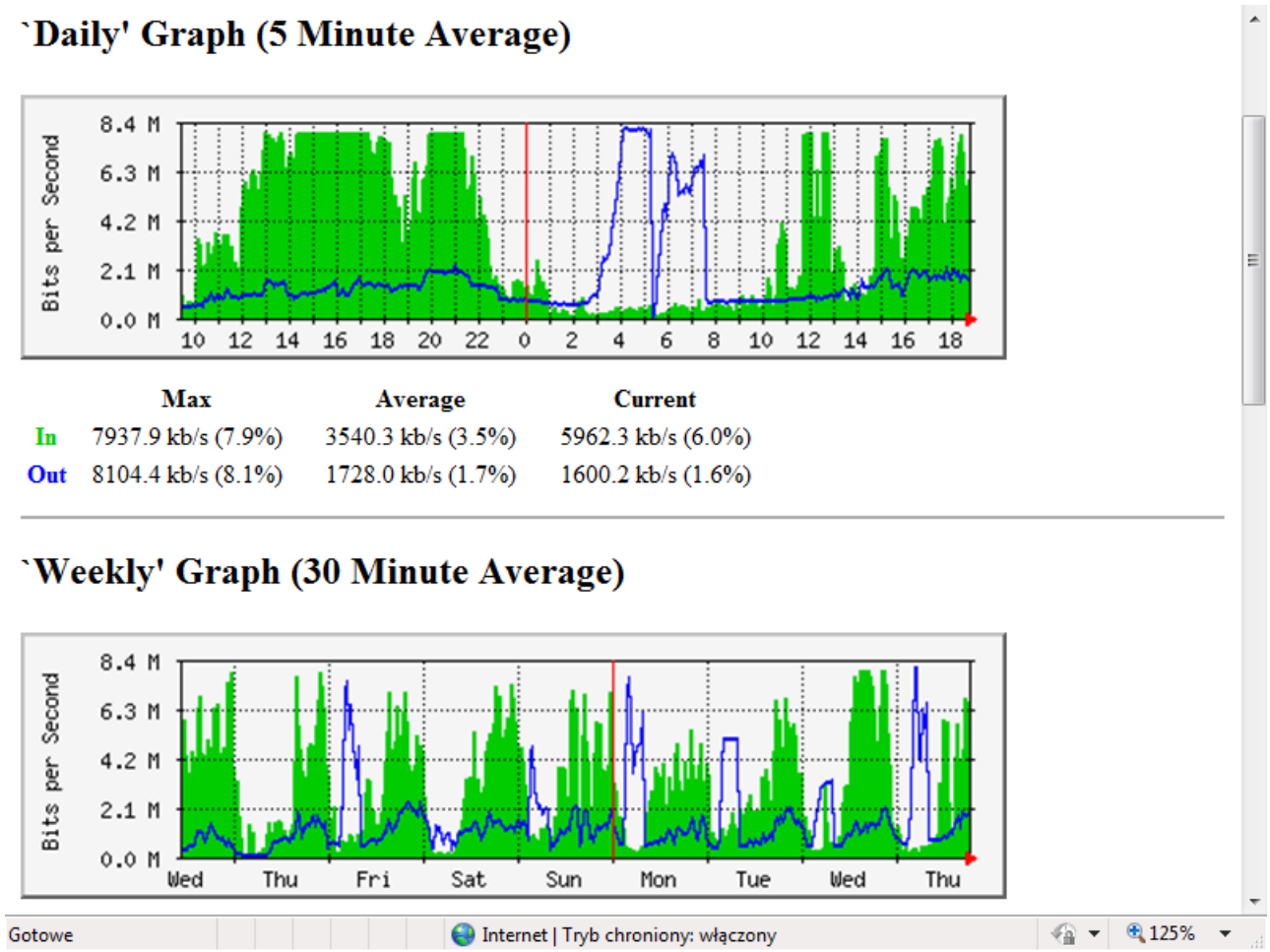

Fig. 1. Traffic load (incoming and outgoing traffic) - sample daily and weekly monitoring results (live graphics generated by MRTG)

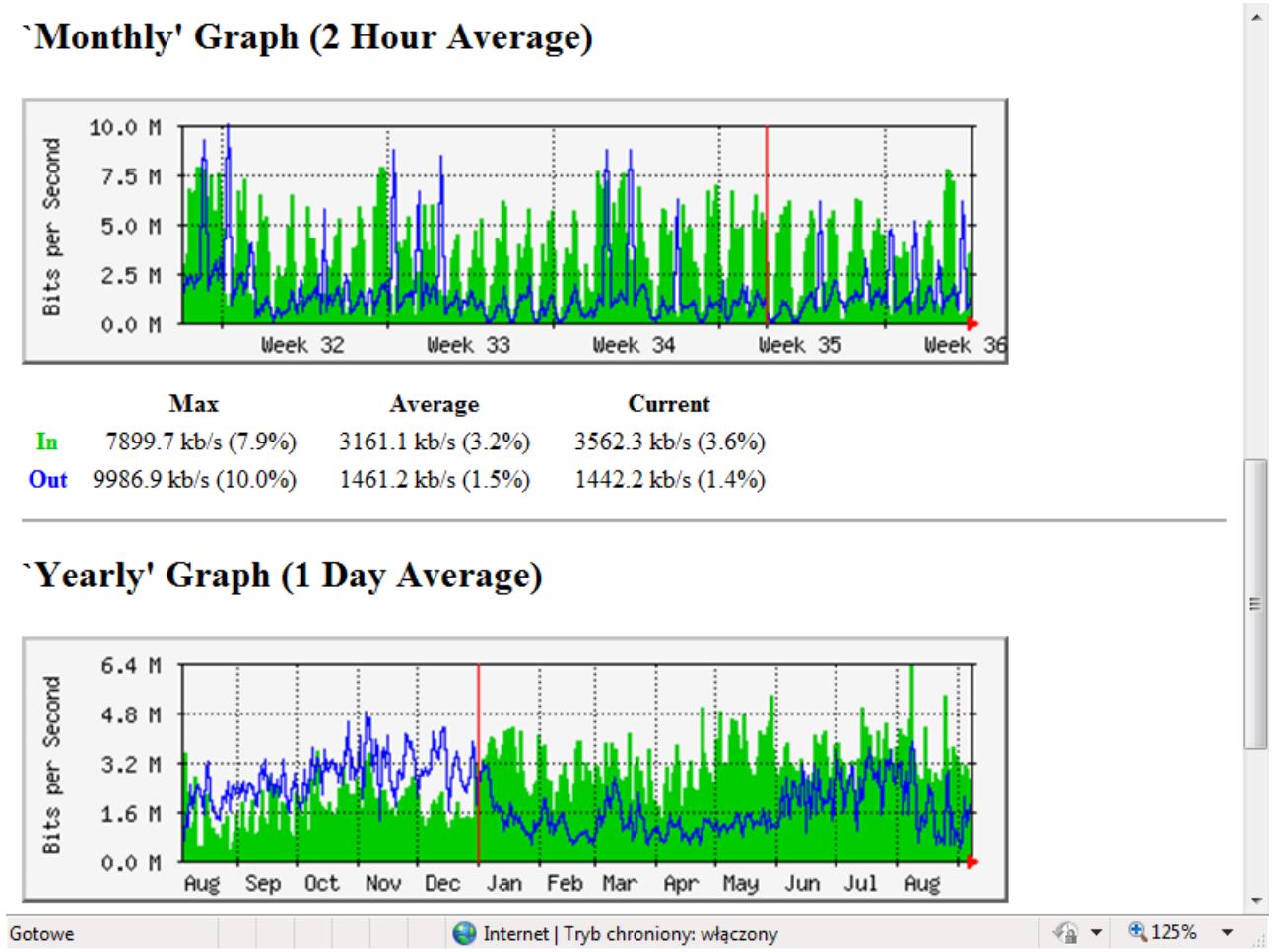

Fig. 2. Traffic load (incoming and outgoing traffic) - sample monthly and yearly results(live graphics generated by MRTG)

The Multi Router Traffic Grapher (MRTG) can be installed almost anywhere in the local manufacturing network, however the most reasonable and convenient location for MRTG installation is the main router - on the gateway to the local network.

Besides the basic ability to monitor incoming and outgoing traffic, the Multi Router Traffic Grapher provides:

- the ability to monitor and display any integer variables in graphical form
- a universal graphic presentation standard: HTML (Hyper Text Markup Language) pages, easily accessible via the HTTP (Hyper Text Transfer Protocol) using any type of web browser
- easy configuration and re-configuration, flexibility and scalability.

One additional important feature is that the Multi Router Traffic Grapheris available under the terms of GNU - General Public License (FSF, 2007), and can therefore be used free-of-charge for licensed use in non-commercial as well as commercial applications.

3. Monitoring of other variables

Because the Multi Router Traffic Grapher (MRTG) allows the monitoring of any variable expressed by an integer value, in addition to the monitoring of incoming and outgoing traffic, it can be also used as front-end software, for the monitoring of any other variables, which can be acquired from the manufacturing network (from servers, workstations, machines, robots and other manufacturing devices)for every defined time period (usually every 5 minutes) and represented as a numeric variable.

For example: the monitoring results of established TCP connections observed on the gateway to the networked manufacturing system are shown in figure 3 and figure 4 below.

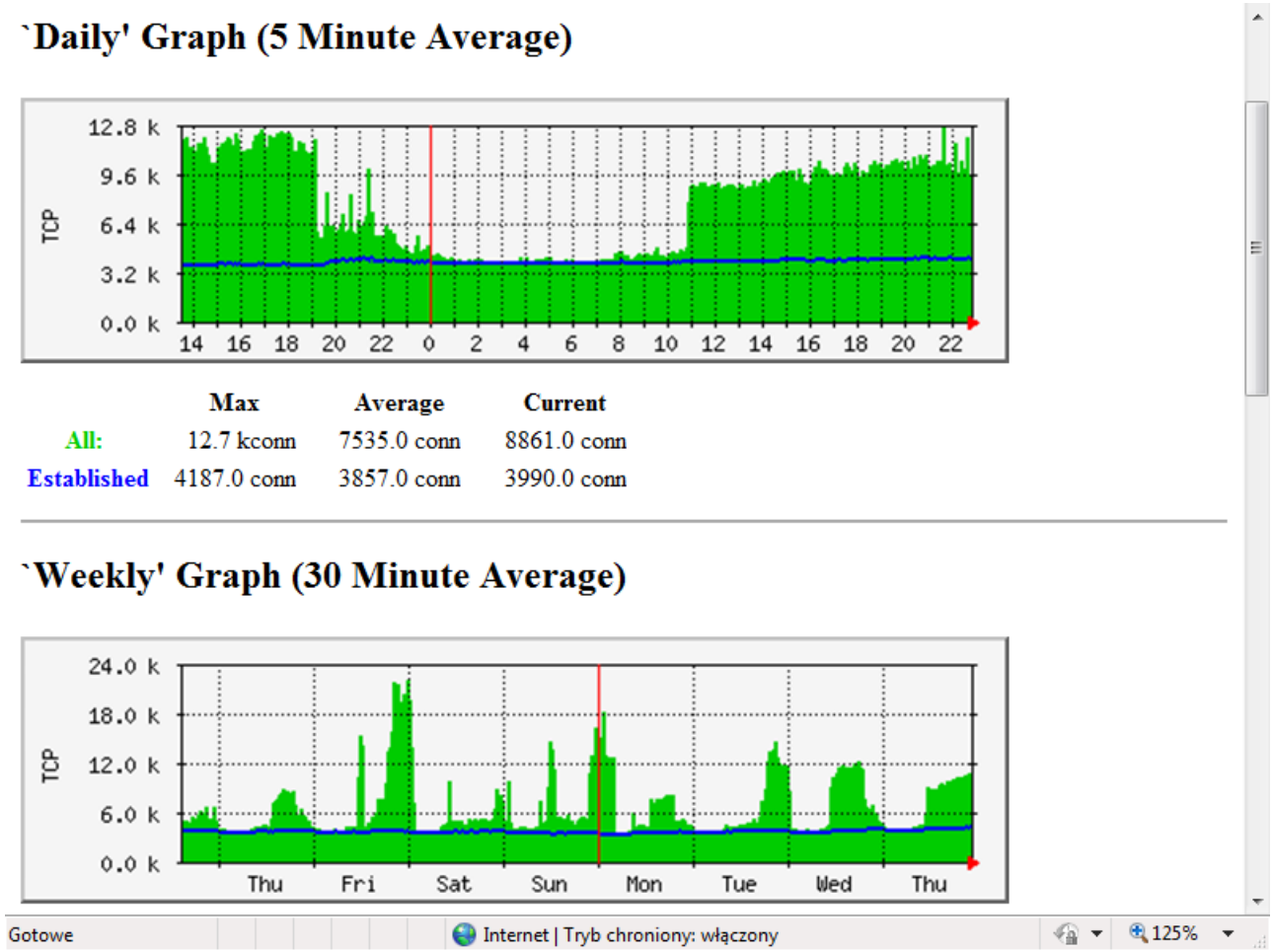

Fig. 3. Established TCP connections from/to manufacturing network - sample daily, weekly live graphics, generated by MRTG

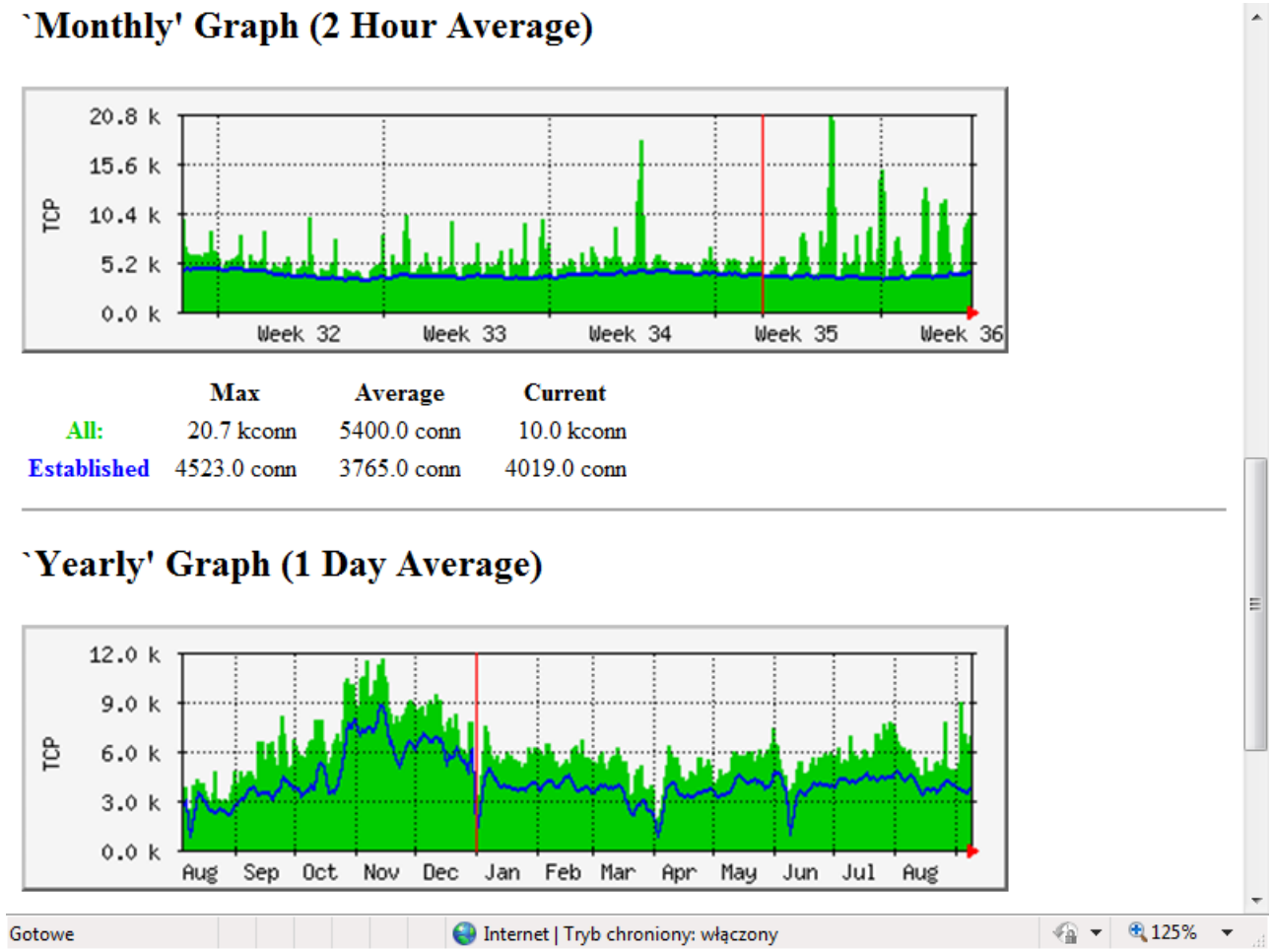

Fig. 4. Established TCP connections from/to manufacturing network -sample monthly and yearly live graphics, generated by MRTG

With this information the admin/ supervisor of a local manufacturing network can decide:

- which networked device, manufacturing machine or robot to choose for monitoring
- which parameter to monitor (i.e. which machine/ robot is up, how many manufacturing resources are logged into the manufacturing network, traffic load, etc.)
- how to acquire the data over the local manufacturing network
- how to transform the acquired data to the proper format, for logging and later graphical display/monitoring using MRTG

Data acquisition through the local network can be solved in a different way, depending on individual needs of the monitored manufacturing system

For monitoring of networked machines, the following software modules can be used:

- nmap - the Network Mapper and Security Scanner. This software module is usually included in UNIX operating systems as one of the software modules

included in the installation packet. The latest version can be downloaded from the author's web page (Lyon, 2010)
- regular commands available in UNIX operating systems – like ping, trace route, net stat and other commands or other vendor specific applications

Based on the results after running these test commands, the manufacturing network can deliver information valuable for monitoring, supervising and maintenance, such as:
- runtime/ uptime status of each machine, robot, etc.
- total number of selected resources (i.e. machines, robots, workstations) logged into the manufacturing network
- how continuous are the connections within the local manufacturing network
- how continuous are the connections from/to ISP (Internet Service Provider)
- traffic load on selected check points inside the local manufacturing network
- any other variable, which can be acquired from the local manufacturing system through the network

4. Monitoring examples

By using MRTG on the gateway to thelocal manufacturing network router (on any other single server/ workstation or work cell computer inside a manufacturing system), it is possible to monitor the uptime status of selected machines in the local manufacturing network.

4.1 Uptime of single manufacturing resource

An audit of a single manufacturing resource (machine, robot, etc.) connected to the local manufacturing network can be done by using the Network Mapper and Security Scanner (nmap) as follows:

/usr/bin/nmap -sP*(single IP address of resource)*

The main aim here is to test, if the selected machine is up. The sample command for such an audit:

/usr/bin/nmap –sP A.B.C.2

Sample results generated by nmap during such audit are as follows:

Starting Nmap 5.35 (http://insecure.org) at 2010-09-10 4:30 CEST

Host machine1.manufacturing.inpoland.com.pl (A.B.C.2) appears to be up.

Nmap run completed -- 1 IP address (1 host up) scanned in 0.350 seconds

These results can be converted to integer variables in the proper format for MRTG and then can be logged and processed by MRTG for monitoring (see figure 5).

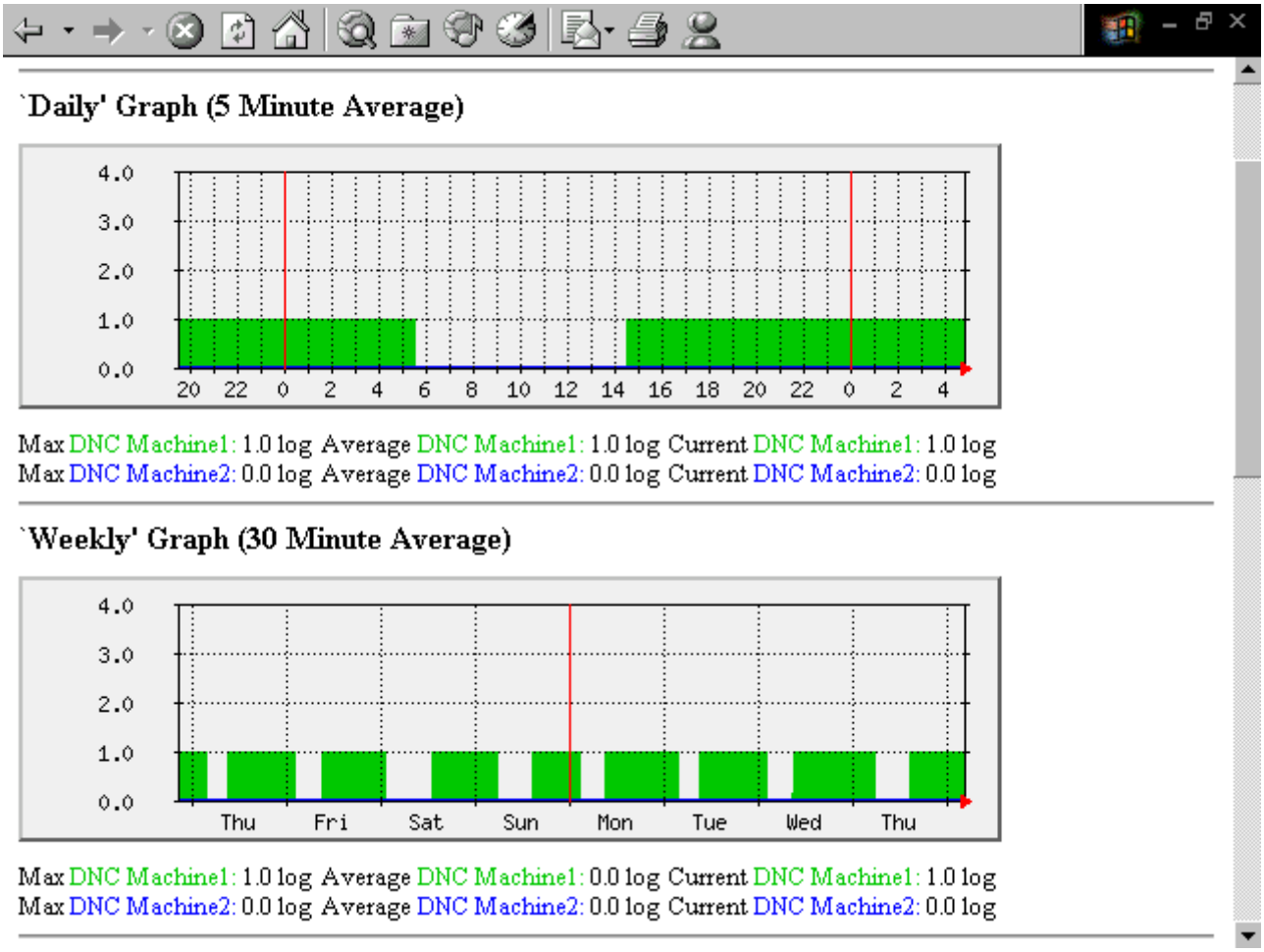

Fig. 5. Activity graph of a single manufacturing resource - DNC Machine
1 = resource online, 0 = resource turned off (no communication with the resource)

The same data for this manufacturing resource – DNC machine (and for any other machine, robotor manufacturing resource) can be also acquired by using the commands**cat, grep and wc** for the main audit file. Sample:

```
cat /etc/mrtg/stations.txt |grep A.B.C.3 |wc –l
```

This allows making just one audit, every defined time period, for all resources connected to local manufacturing network. Then, based on the results saved in the audit file, it is possible to monitor each manufacturing resource separately, making a separate graph for each manufacturing resource using MRTG.

4.2 Audit of Local Manufacturing Network

The aim for auditing the local manufacturing network is to testwhich networked machines, machine tools, robots, work cell computers and other technological devices and hosts presented in local manufacturing network are up.

The command for such an audit – using the NMAP Network Scanner is:

/usr/bin/nmap -sP*(IP address range)*

Sample:

/usr/bin/nmap –sP A.B.C.1-255

This audit gives as results following output (sample results):

Starting Nmap 5.35 (http://insecure.org) at 2010-09-1003:10 CEST

- Host router.manufacturing.inpoland.com.pl (A.B.C.1) appears to be up.
- Host machine2.manufacturing.inpoland.com.pl (A.B.C.2) appears to be up.
- (…)
- Host cad70.manufacturing.inpoland.com.pl (A.B.C.70) appears to be up.

Nmap run completed - 255 IP addresses (28 hosts up) scanned in 6 seconds

Using UNIX **crobtab** we can automatically repeat such audit every defined time period (usually: 5 minutes) and write results to a log file. Sample crontab command as follows:

```
1-55/5 * * * * root /usr/bin/nmap -sP A.B.C.1-255>/etc/mrtg/stations.txt
```

After the results of audit are saved in a file (/etc/mrtg/stations.txt), it is possible to analyze this file and forward the final results to MRTG. using **cat**,**grep**and **wc**commands.

Theaudit file can then be converted – using set of the Unix commands mentioned - to the format required by MRTG.

```
cat /etc/mrtg/stations.txt |grep appears |wc -l
```

After that operation - our monitoring system will have the result: **26**

The Multi Router Traffic Graphercan collect numeric results every 5 minutes, convert them to universal PNG graphs (Portable Network Graphics) and display graphical results as web page (sample daily, weekly, monthly and yearly graphs - see: figure6, figure 7).

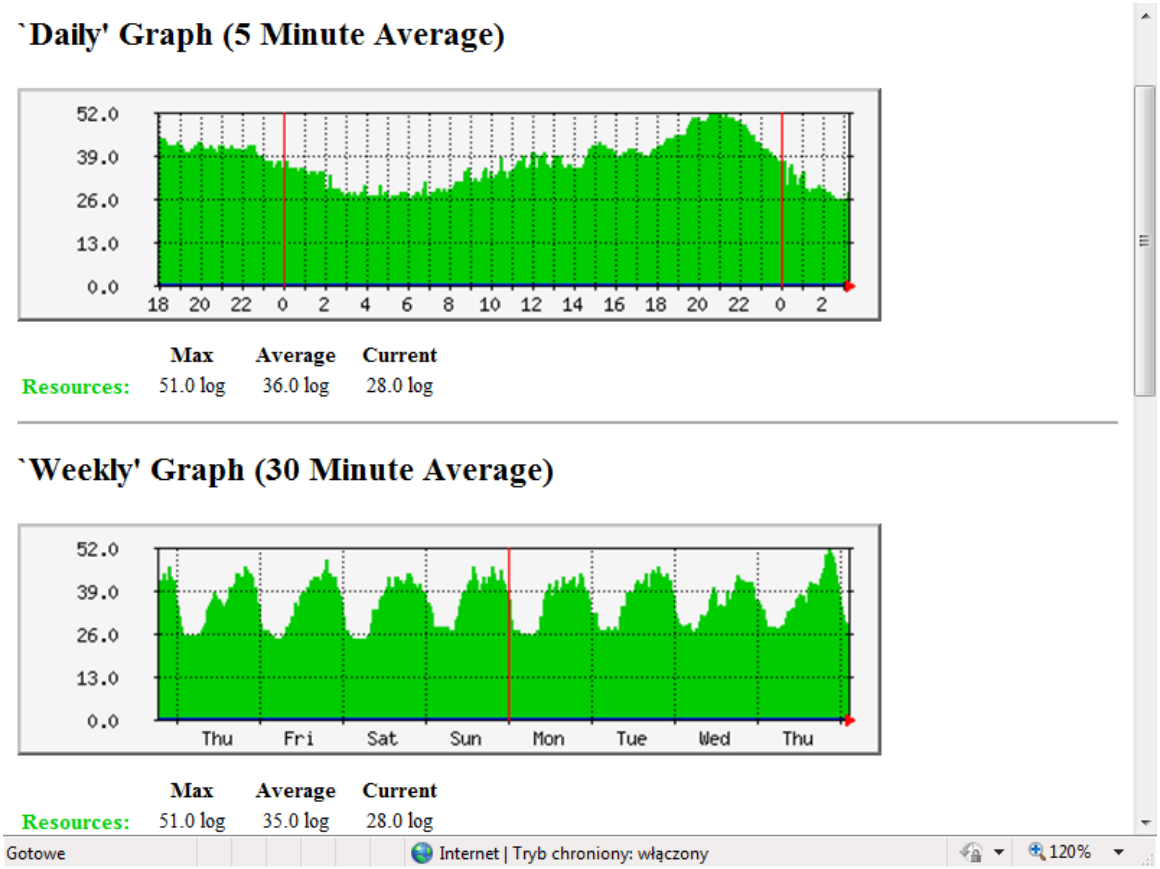

Fig. 6. Machines logged into the local network - sample daily/ weekly graph

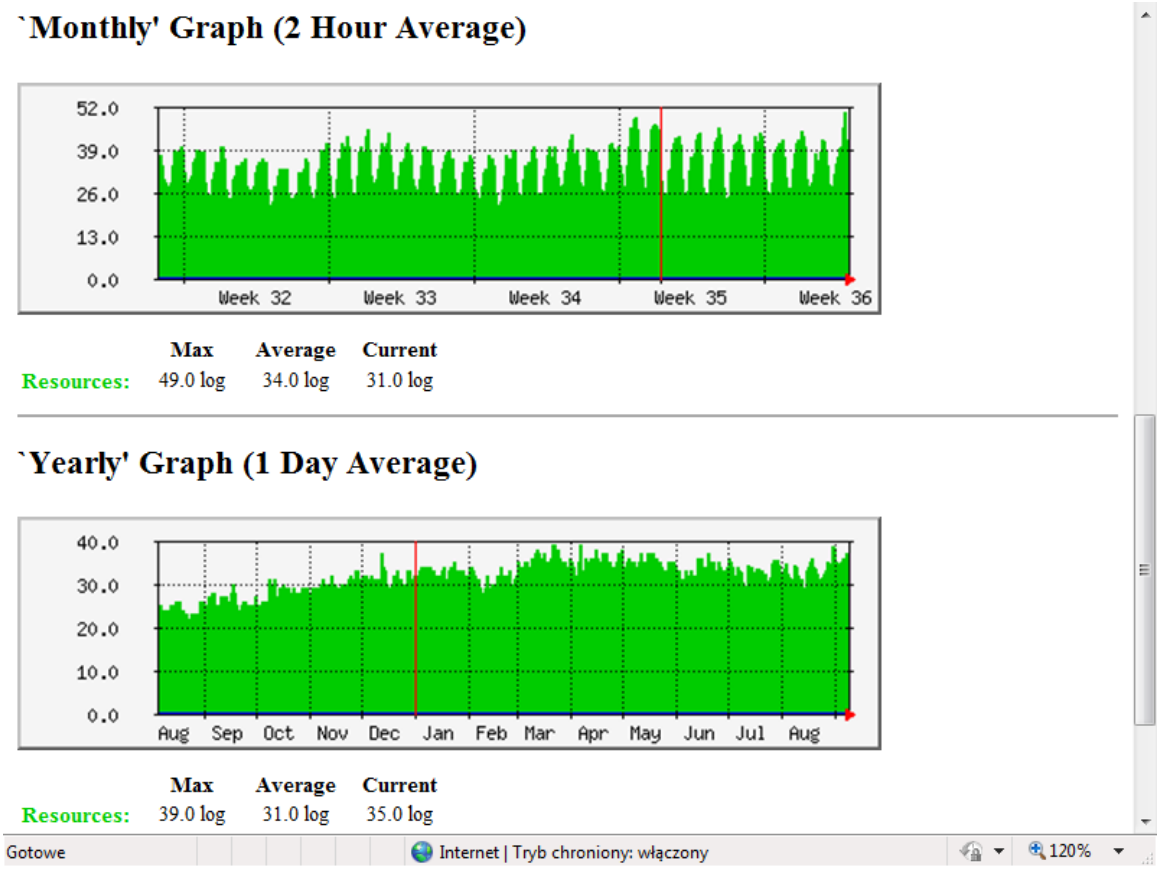

Fig. 7. Machines logged into the local network - sample monthly/ yearly graph

4.3 Audit how continuous is the network connection with WAN

The same monitoring method based on the Network Mapper and Security Scanner (mnap) scan and data logged to the Multi Router Traffic Grapher(MRTG) can be used for continuous monitoring the status of link to ISP (Internet Service Provider) or any other WAN links.

To test how continuousthe network connection is with the ISP, we can probe the Internet Service Provider gateway: router, access point (or any other check point located in WAN) every 5 minutes, andthen make the data format ready for MRTG. The sample results shown in figure 8.

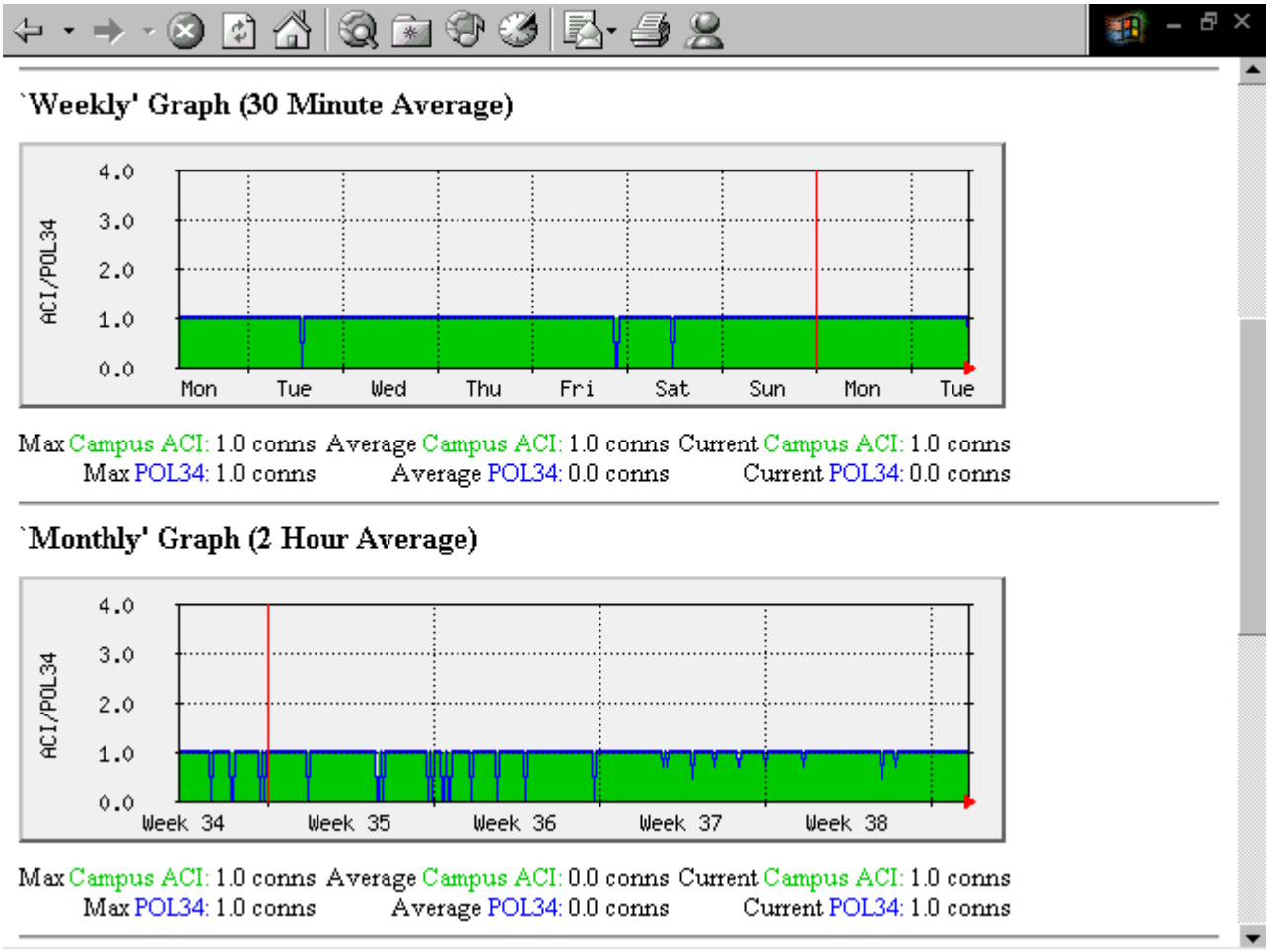

Fig. 8. MRTG graph presents how continuous the connection is to the ISP– sample weekly/ monthly graph

More detailed information on quality of connections such as: latency time and packets lost, can be obtained using “ping” command and after converting the results to a format readable for the Multi Router Traffic Grapher, will also be logged and monitored using MRTG (figure 9).

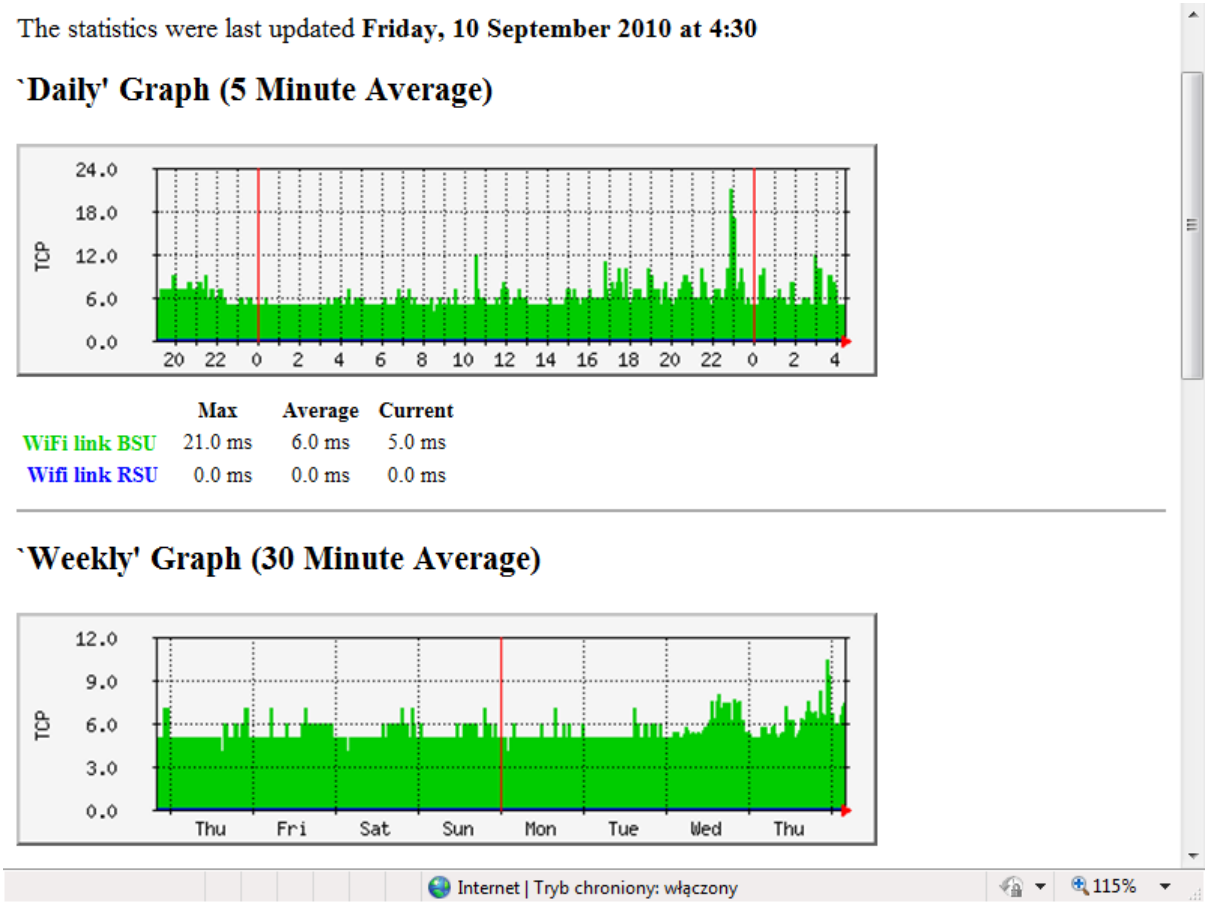

Fig. 9. Sample graph: monitoring of the WiFi connection (latency time) to the ISP

5. Conclusion

Using specific UNIX commands, nmap and MRTG software modules can yield an effective, scalable and free-of-charge method to monitor selected machines, robots and check points ina manufacturing network. This article presents sample, selected applications, however many other variables, specific for each selected manufacturing system can be monitored using MRTG. In the next step, for more complex monitoring, new software called: RDDtool (Oetiker, 2010) can be used.

6. References

Cottrell, L. (2010). Network Monitoring Tools, SLAC, Stanford University, http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html- *Accessed on:2010-09-09*

FSF Free Software Foundation, Inc. (2007). The GNU General Public License, http://www.gnu.org/copyleft/gpl.html -*Accessed on: 2010-09-09*

Lyon G. (2010) –NMAP Network Mapper and Security Scanner, http://www.insecure.org/nmap/ - *Accessed on:2010-09-09*

Oetiker T., Rand D. (2010). The Multi Router Traffic Grapher, http://www.mrtg.org - *Accessed on:2010-09-09*

Oetiker T. (2010).RDDtool Round Robin Database, http://oss.oetiker.ch/rrdtool/- *Accessed on:2010-09-09*