Distributed telecommunications network access using the TMOS IntraWeb Gateway

Magnus Ekhed, Peter Gundersen and Olav Queseth

In an increasingly competitive marketplace, network operator success depends more and more on network usage. In optimizing usage, operators invest in O&M systems, which control traffic and network quality. Next, in taking steps to uphold good service levels for customers, operators are finding that they must distribute information on network status and performance to all parts of the organization.

The TMOS IntraWeb Gateway from Ericsson Hewlett-Packard Telecommunications permits widespread access to network information through corporate IT networks, allowing persons outside an O&M center to access the network-related information they need.

The authors describe how the TMOS IntraWeb Gateway makes new functions and interfaces available anywhere in the corporate network, thereby improving internal work flow and enabling network operators to give their customers better service.

Traditionally, operations support systems (OSS) were created to meet the needs of the operation and maintenance (O&M) organization, whose job is to operate the telecommunications network. Consequently, personnel at O&M centers have a good picture of network status and performance. Direct access to network information has always been their privilege. Other departments have received network status reports distributed on paper, or in some cases, by electronic mail (e-mail).

As the market changes, network operators are refining their business processes to make their operatios more cost-effective, and to provide better service and shorter time to market. In doing so, they want to distribute information on network status and performance to new categories of users within their organizations. A typical example involves distributing reports on traffic performance measurements on a regular basis to different parts of the organization.

TMOS IntraWeb Gateway

The TMOS IntraWeb Gateway (TIG) concept, from Ericsson Hewlett-Packard Telecommunications (EHPT), applies Web technology to give managers, customer-care departments, marketing departments, and network planners direct access to user-specific information and reports from an operations support system. It does so by introducing a gateway – but without creating dependencies – between telecommunications management and operations support (TMOS) and the corporate information technology (IT) network. Thus, by using an ordinary Web browser, company personnel anywhere in the corporate IT network outside the operation and maintenance center (OMC) may access a subset of functions and information in TMOS and execute standard tasks in the telecommunications network.
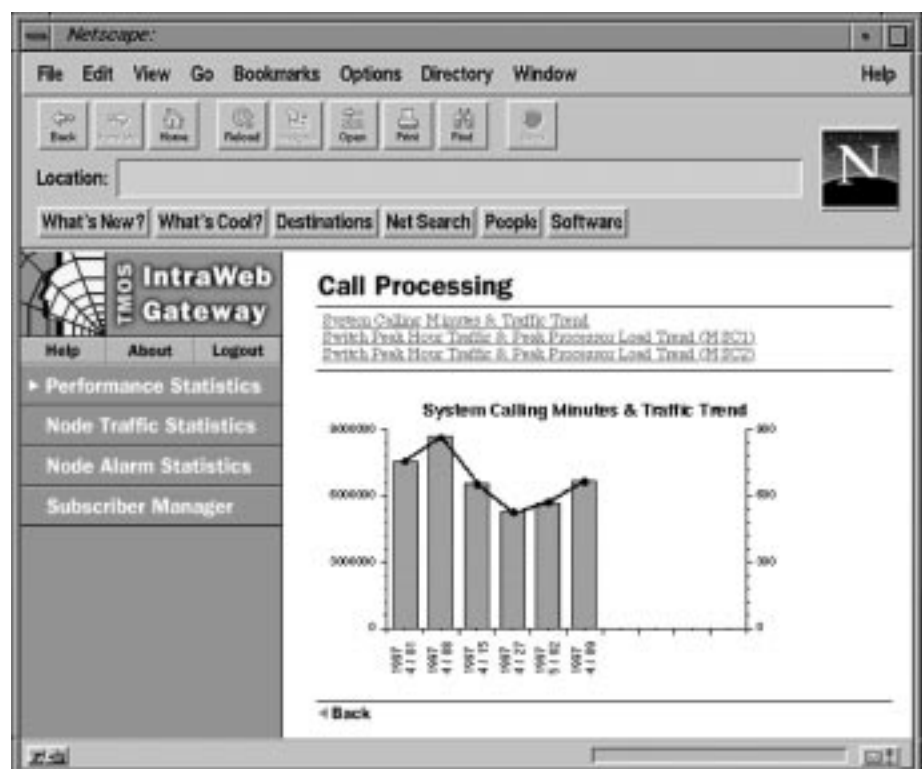

Figure 1
Information distribution – example of distributed traffic information from TMOS via TMOS IntraWeb Gateway.

The TMOS IntraWeb Gateway helps personnel at the operation and maintenance center to spread network information within the operator organization, and allows authorized persons outside the OMC to perform tasks that help customers. The internal work flow is improved, and customers get better service.

The TMOS IntraWeb Gateway, which is fully scaleable and easily customized, also helps network operators to get the most out of existing IT infrastructure. Web server hardware and customized software, along with tools and system interfaces, make up a controlled, secure, user-friendly link through which staff access TMOS information.

A Web-based solution allows standard Web-client software, such as the Netscape Navigator, to be used for browsing information. Thus information to and from operations support systems (such as the TMOS eXchange Manager), and from business support systems (such as TIMS) may be integrated into and displayed on existing clients. The TMOS IntraWeb Gateway may also be customized to access operations support systems (other than TMOS), seamlessly integrating operations support systems in multi-vendor environments into a single user interface.
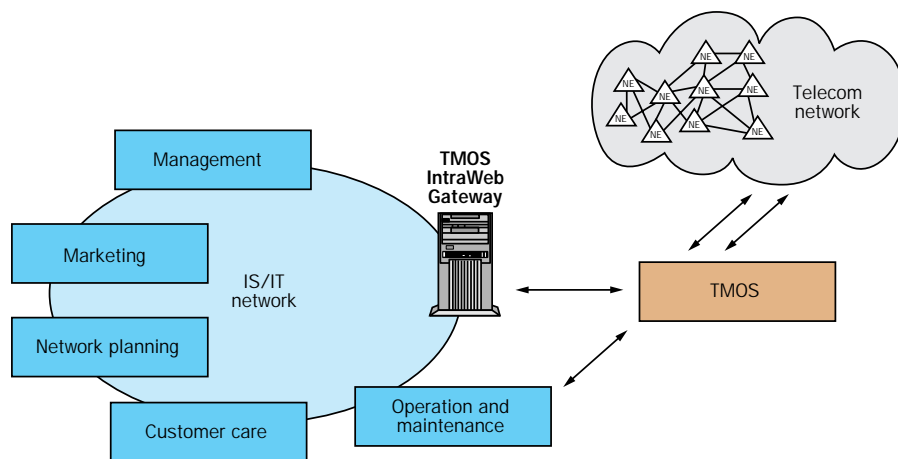
Fetching and transferring information

The TMOS IntraWeb Gateway enables employees to fetch information from TMOS as well as to transfer information to network elements that are accessed through TMOS by means of
- scheduled transfers from TMOS to the Web server;
- simple, controlled actions, which are activated from Web pages and sent from the Web server to TMOS.

Information distribution
In the past, when a marketing department needed performance measurement data for planning business activities, they usually had to order that data from the operation and maintenance center – which meant that they often had to wait for the data. Moreover, when the data arrived, the marketing department usually had to reformat it before they could use it.

The TMOS IntraWeb Gateway enables operators to schedule regular data transfers from TMOS to a Web server, which greatly improves quality and speeds up the dis-

tribution of information to end-users (Figure 2). Furthermore, by being able to schedule data transfer, operators can better regulate the impact of load on TMOS.

Software in the Web server transforms data into a variety of reports, which are published on the operator's corporate intranet. The format of the reports may vary from simple spreadsheets to automatically updated graphs. Thus, thanks to the TMOS IntraWeb Gateway, when someone at the marketing department wants to view an up-to-date report, he or she can find it on the Web server.

To better support customer processes, managers may also use the TMOS IntraWeb Gateway for creating and distributing customized presentations of TMOS data. Access restrictions guarantee that only authorized persons access the reports.
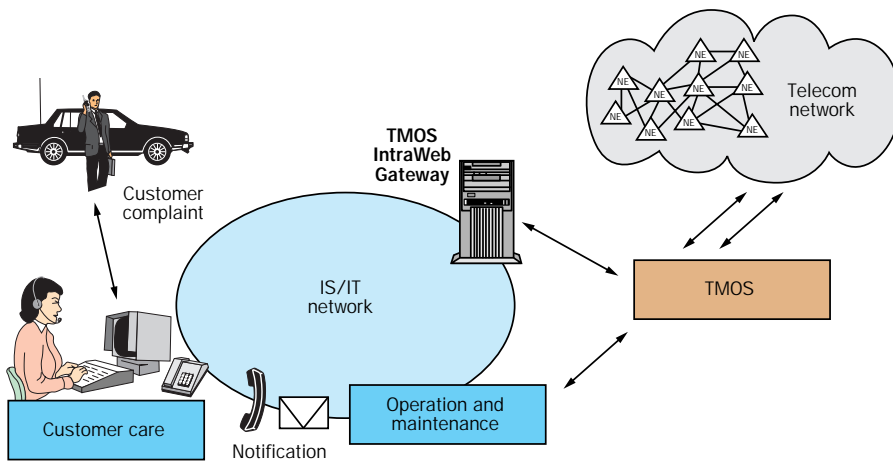
Furthermore, the TMOS IntraWeb Gateway enables end-users with little or no TMOS experience to obtain information from TMOS over the intranet.

Process automation
Previously, when a subscriber called to report that his or her voice-mail service was blocked, the customer-care department could do little more than submit a work order to the OMC, since their own administrative system did not provide a means of activating the subscription. The TMOS IntraWeb Gateway allows customer-care staff to perform such simple actions. They do so by filling in predefined forms displayed in their browser. A command sequence is then generated and sent through

Box A
Abbreviations

CLI   Command-line interface
EHPT   Ericsson Hewlett-Packard
         Telecommunications
IS/IT   Information systems and information technology
IT   Information technology
MML   Man-machine language
O&M   Operation and maintenance
OMC   Operation and maintenance center
OSS   Operations support system
SSL   Secure sockets layer
TCP/IP Transmission control protocol/Internet protocol
TIG   TMOS IntraWeb Gateway
TMOS   Telecommunications management and operations support

Figure 3
Process automation – the TMOS IntraWeb Gateway enables customer-care staff to perform simple O&M actions, such as restoring a customer's voice-mail service, if blocked.

the command-handling facilities in TMOS. The customer-care staff may observe changes in network status as the commands are executed. Using the TMOS IntraWeb Gateway concept, customer-care staff may actually restore certain kinds of customer service as the problem is being reported (Figure 3).

Product description

The TMOS IntraWeb Gateway is delivered as a basic package (Figure 4) with optional gateway customization consultancy service. The basic package contains software from EHPT that provides high-level interfaces to TMOS functions. The interfaces ensure that customer adaptations will run with any TMOS software.

The basic package also contains standard third-party hardware and software. Currently, these include an operating system (Windows NT), a Web server (Netscape Enterprise server), a Web-authoring tool (Netscape Navigator Gold), a programming language (Java), and optional firewall software (Firewall 1).

TMOS IntraWeb Gateway module
The functionality of the basic package may be divided into three categories:
• TMOS access blocks.
• The TIG toolbox.
• TIG applications.

TMOS access blocks
The TMOS access blocks – which consist of

a man-machine language (MML) access function block, a command-line interface (CLI) access function block, and a database access function block – add stable interfaces to TMOS functionality.

The man-machine language access function block enables TIG application programmers to connect to network elements that are linked to the TMOS system. The functionality allows users to send commands, and to choose between immediate or delayed responses.

The command-line interface access function block provides functions for accessing command-line interfaces to TMOS functions. Command-line interfaces are programs that are run from a command line. The program results, which are normally printed on the screen, may be used in the TIG application.

The database access function block gives operators access to databases located in TMOS servers. Data that is retrieved from the databases may either be processed in TIG applications, or displayed directly in the browser.

The TIG toolbox
The TIG toolbox, which is used for creating TIG functionality, contains functions for user and authorization handling, functions for logging and auditing applications, support for generating spreadsheets, and parsing tools.

The user- and authorization-handling function block provides functions for handling user information and some initial login data. The function block mainly handles user authentication by establishing the identity of TIG users. This is done either through secure sockets layer (SSL) certificates or by means of login and password combinations.

When users have been authenticated, the function block generates a list of the applications they are authorized to run. Obviously, the list may differ for different users.

A Web-based interface facilitates the administration of user profiles.

The spreadsheet generation function block helps TIG application programmers to generate output in the form of a spreadsheet directly in the TIG application. It also provides rules and guidelines that help TIG application programmers to program efficiently.

The logging and auditing function block gives TIG application developers a uniform way of logging events that occur within TIG applications. The function block also contains

functions that enable users to browse the logs generated by the applications.

Because most TIG applications need to parse input from HTML forms, *the parsing tools function block* contains functions that help TIG application programmers with this task. The function block also screens the input in order to improve security.

TIG applications
The basic package currently includes two applications: one for managing network performance and one for managing faults in the network.

The performance statistics application enables TIG users to view reports on the performance measurement statistics collected by TMOS. Predefined reports are distributed via the Web and displayed in the Web browser.

The alarm statistics application enables TIG users to view TMOS alarm logs. Users may retrieve historical data for a specified time interval by selecting the attributes of the alarms they want to see. The data generated from this application is displayed as a graph in HTML format, or in a spreadsheet (MS Excel).

TIG design environment

The design environment forms the basis for a certification program that will allow partners to develop TIG applications.

When used in combination, the TIG toolbox, style guides, templates, and specified design rules speed up the development of TIG applications and customer adaptations, and ensure that each application has the same look and feel. Adherence to the design rules also guarantees the security of TMOS, and keeps maintenance and upgrade costs down to a minimum.

Security

Because the TMOS IntraWeb Gateway allows users to access TMOS from the Web, security aspects must be considered very carefully. There are many ways in which an intruder can harm a computer system. For example, besides damaging hardware through theft or sabotage, intruders may try to attack a server in order to gain access to the super-user account. If they succeed in this, they can modify data, listen to traffic on the local area network, intercept data sent through the network, or even modify the telecommunications network. Thus, every hole through which a would-be intruder
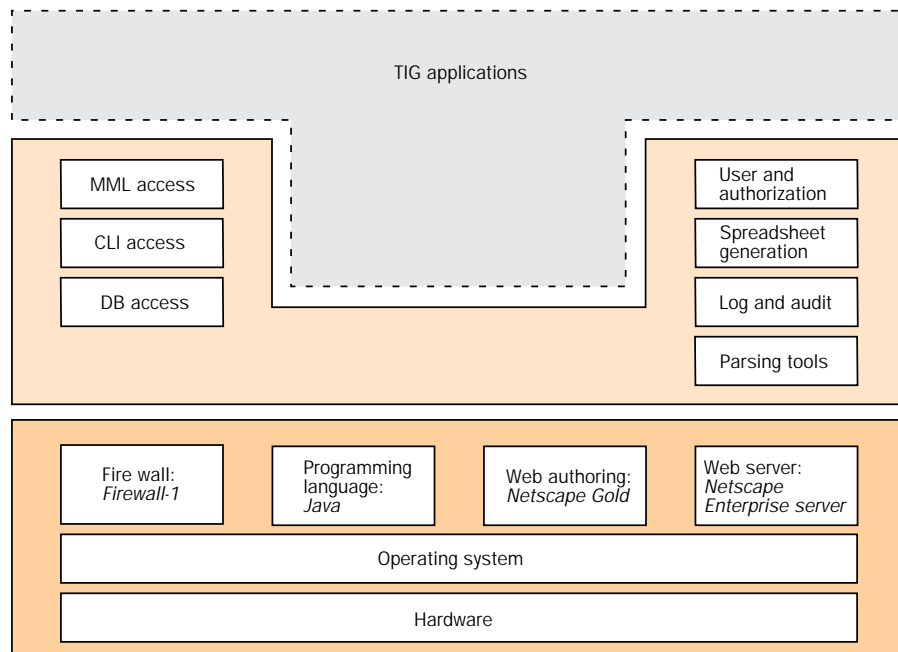
Figure 4
The TMOS IntraWeb Gateway consists of third-party products, access blocks to TMOS, the TIG toolbox, and the TIG applications.

might seek to gain access must be closed. To this end, measures (firewall, and screening of user input) have been taken to prevent intrusion, to control access (authentication and authorization procedures), and to shut out eavesdroppers (encryption).

The TMOS IntraWeb Gateway was designed with security in mind. Likewise, the selection of each accompanying third-party product has been based on compliance with the security framework. Firewalls, security levels, and encryption capabilities, which were developed in collaboration with Hewlett-Packard, have been designed to fulfill customer needs. Network and access security are embedded in the TMOS IntraWeb Gateway system.

Authentication
The login procedure, known as the user and authority handling function, screens each person who logs into the system with SSL certificates, or by querying them for a user name and password. This procedure ensures that only authorized personnel view or access data in TMOS.

Authorization
The most valuable part of TMOS is the data it contains – for example, traffic data and customer data are valuable to competitors.
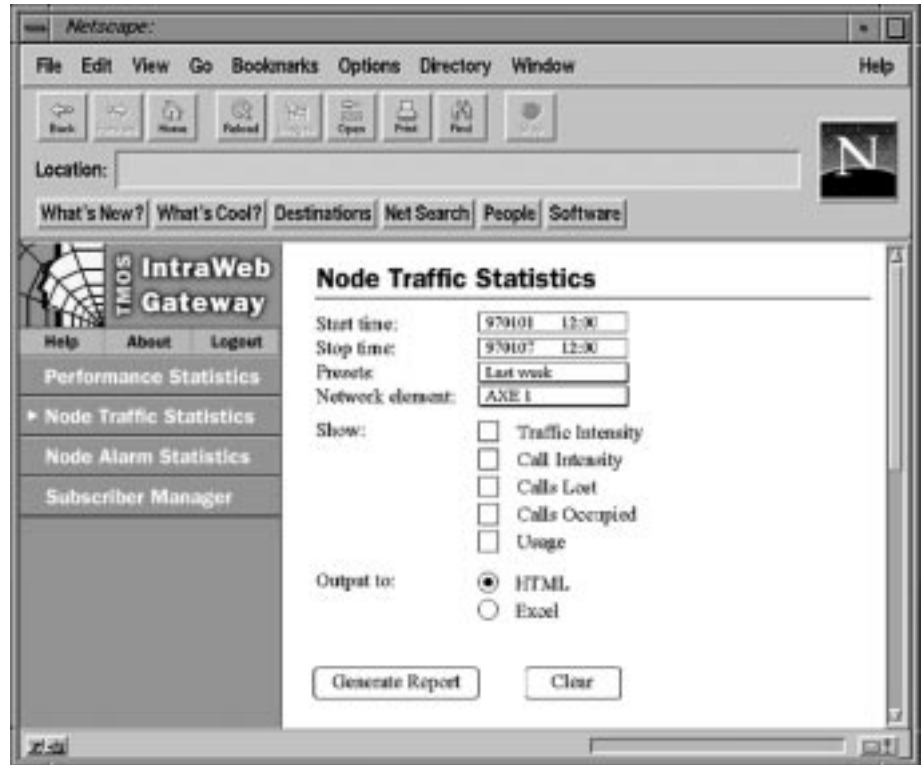
Figure 5
TMOS IntraWeb Gateway gives authorized users easy access to telecommunications network data anywhere in the corporate network.

Therefore, adequate measures must be taken to protect this data from harm. Only authorized persons must be able to access it. And then, only such categories of data as they need to access. The TMOS IntraWeb Gateway uses a built-in security system which ensures that no one but authorized users may view data, change data, or remove it from the system.

Encryption
An encryption technique is used to prevent information leaving the protected TMOS zone from being intercepted or replaced with false information. Encryption is implemented using the secure sockets layer standard and third-party products (Netscape).

Firewall
The TMOS IntraWeb Gateway has two separate network interface boards: one is connected to the corporate IT network, and the other one is connected to the TMOS network. Each unnecessary service is turned off and a Web server is installed on the gateway machine. In addition, firewall software is installed on the gateway machine – the software logs all server activities, generating alarms for unusual events, and filtering out unwanted TCP/IP packets.

Conclusion

The TMOS IntraWeb Gateway concept works with any version of TMOS, giving several user categories outside the operation and maintenance center access to the system. It permits operators to distribute high-quality real-time information to new user categories via a Web browser. It also enables OMC personnel to report on network status, and allows other departments to perform standard network operations. By integrating and automating work procedures, network operators can improve work flow and give customers better service.

Various security measures control information access.

The efficient transfer of information from the telecommunications network to different parts of the operator organization shortens lead time for customer services and makes better use of investments in TMOS. The TMOS IntraWeb Gateway concept also allows operators to extract more from existing IS/IT investments, without creating dependencies between TMOS and corporate IT networks.