1 Preface

Enterprise-wide information processing today comprises a large number of systems and applications. These are often no longer concentrated in a computer center but distributed over a number of different sites.

While in the past the decentralized installation of servers meant that operational responsibilities were also distributed among various sites, centralization of these responsibilities can increasingly be observed today. This presupposes that the distributed systems and applications can be monitored and controlled via communication links, thereby largely replacing on-site support for the components. This task is being handled increasingly by central management stations which obtain current information about the components being monitored with the help of “agents”. An agent is the software which runs on the component being monitored and delivers the required information about this component. The management station and the agent communicate via a defined protocol. The SNMP protocol (Simple Network Management Protocol) has gained acceptance as the standard in this context. The SNMP standard facilitates the integration of an extremely heterogeneous IT inventory from different manufacturers into a standardized network management system.

With its BS2000/OSD products for SNMP management, Fujitsu Siemens Computers GmbH offers the prerequisites that also enable BS2000/OSD systems to be incorporated into the standardized network management concept. The following products are available:

- On the part of the SNMP agents:
  - SNMP-Basic-Agent BS2000 (SBA-BS2) with the basic agent
  - SNMP-Standard-Collection BS2000 (SSC-BS2), SSA-SM2 and SSA-UTM with extensions for the agent

- On the part of the management station:
  - The console monitor (CMBS2), performance monitor (PMBS2) and BCAM monitor (BMBS2) applications
  - The integration package (SMBS2) for integration of BS2000/OSD management into universal management stations such as Unicenter TNG, TransView and OpenView Network Node Manager.

Comprehensive information about these products may be found in the “SNMP Management for BS2000/OSD” manual.
As from July 1998, the product SNMP-LIGHT is supplied with the corrections package for BS2000 versions as from OSD V2.0 free of charge. SNMP-LIGHT allows you to familiarize yourself with the benefits of SNMP management without first having to buy the above-mentioned products. As from March 2001, Level 5 of SNMP management will be available as a Light version. This brochure provides you with information on how to install SNMP-LIGHT and a step-by-step guide to managing your BS2000/OSD system. Please follow the examples in the chapter “Monitoring with SNMP-LIGHT” (see page 17).

With reference to the SNMP-LIGHT agent, a special management integration package is available for the Unicenter TNG Framework management platform that you can download from the following URL over the internet:

http://www.fujitsu-siemens.com/servers/snmp/snmp_de/light_ag.htm

The emphasis in the present brochure lies in the description of selected application examples.

In addition to the SNMP interface, the SNMP agent for BS2000/OSD offers access via the World Wide Web as a further interface. This enables you to access BS2000/OSD management by means of a web browser. The present brochure provides a brief description of both means of access to the BS2000/OSD agent.

SNMP access enables you to integrate your BS2000/OSD into the complex management structure of a heterogeneous network involving equipment from different manufacturers. The prerequisite for this is appropriate management software. Such software is available to you for SNMP-LIGHT in the form of the aforementioned management applications and the SMBS2-LT package. Access to the web requires no special software. A web browser is sufficient.

This brochure provides you with information on the following individual topics:

● the general concept behind SNMP
● the concept behind SNMP management in BS2000/OSD
● how to install the “light” version of SNMP management in BS2000/OSD
● the functionality and features of the SNMP-LIGHT agents within the scope of SNMP management
● Web access with SNMP-LIGHT
Notes on using the brochure

You do not need to read through the entire brochure, section by section, from beginning to end. You should start with Chapters “2 Overview of SNMP” (see page 5) and “3 SNMP management in BS2000/OSD” (see page 11), which provide fundamental information about SNMP in general and also about the SNMP agent in BS2000/OSD. Chapter 4 describes how to install the necessary software.

There are two alternative ways in which you can now proceed:

– You can read the description of the SNMP functions in Chapter “5 Monitoring with SNMP-LIGHT” (see page 17). When doing so, you should first work through sections 5.1 and 5.2 because these describe the basic steps required to set up communication with the master agent. Sections 5.3 through 5.6 describe the functions and capabilities of individual subagents and also of the associated management applications; there is no need to work through them strictly in the order in which they appear.

– You can skip directly to Chapter “7 Web access to BS2000/OSD management” on page 55 to familiarize yourself with the web access functionality. When you follow this course of action, it is not necessary to install the management software for SNMP access.

Chapter “6 Other SNMP-LIGHT subagents” (see page 49) provides information about other subagents of SNMP-LIGHT.

The remaining Chapters “8 Problem diagnosis” (see page 67) and “9 Appendix” (see page 71) provide important additional information. The section “Configuring Unicenter TNG” in particular contains important information about working with the Framework of Unicenter TNG.

Your contact:

Erwin Fischer, tel. +49 (0)89/636-45780, fax +49 (0)89/636-41143
Fujitsu Siemens Computers GmbH EP BS
e-mail: erwin.fischer@fujitsu-siemens.com
Eine Dokuschablone von Frank Flachenecker
by f.f. 1992
2 Overview of SNMP

SNMP stands for **Simple Network Management Protocol** and was developed as a protocol for network management services in the TCP/IP internet. SNMP was originally intended for only monitoring and managing LAN components such as bridges, routers and hubs in heterogeneous networks with TCP/IP protocols. In the meantime, the application range of SNMP has been extended to include system and application management.

**Benefits of SNMP**

SNMP is no longer merely one management protocol among many, it is now *the* management protocol in TCP/IP networks. The reasons for this include:

- SNMP is a standard
- SNMP enjoys widespread popularity
- SNMP allows differentiated access
- SNMP is easy to implement

**SNMP as a special client/server architecture**

The name SNMP does refer to the protocol itself, but rather to the entire SNMP-based management system, in the same way the term TCP/IP designates the complete network rather than just the protocol as such. In addition, the term SNMP is also used to refer to a special variant of the client/server architecture with the management station as the client and the agent as server (see figure 1 on the next page).
SNMP manager

The SNMP manager is the software which generates the requests for the individual agents and sends them via SNMP to the agents involved.

SNMP managers receive two types of messages from the agents:

- responses to their requests
- so-called traps. Traps are asynchronous messages which the agent sends to the SNMP manager in defined situations, unsolicited by the SNMP manager.

The SNMP manager displays the information received from the agent and can react to this information with its own actions. The display options range from the output of the values in a simple table to a visual representation of the monitored systems and applications in a network map with event reporting and specific alarm management.

Figure 1: Communication between management station and agents via SNMP

MIB = Management Information Base
SNMP agent

An SNMP agent is the software which receives, executes and responds to the requests sent by the SNMP manager. The agent has direct access to the part of the system or the component being monitored. In defined situations, the SNMP agents also send unsolicited asynchronous messages (traps) to the manager.

Modern SNMP agents like the EMANATE agent used in BS2000/OSD are structured according to a master/subagent principle (see figure 2 on the next page). The functionality of the agent is distributed among one master agent and one or more subagents as follows:

- The master agent is responsible for performing basic tasks such as handling the SNMP protocol, performing security functions, distributing the workload, etc. centrally.

- Each subagent is only responsible for a certain part of the component being monitored. In this situation, the subagent does not communicate with the SNMP manager directly, but rather indirectly with the SNMP agent.

The subagents are independent units and can be started and terminated at any time. This provides best performance, reliability and scalability.
Figure 2: Master/subagent principle based on the example of the EMANATE agent

The agents shaded in violet in figure 2 are supported in SNMP-LIGHT.
Management Information Base (MIB)

The Management Information Base (MIB) describes the objects managed and their characteristics such as the object name, syntax, access rights and state. The MIB thus provides the basis for communication between the management station and an agent. Therefore the instance of the MIB used by the management station and the instance used by the agent must be identical.

SNMP protocol elements (SNMP operations)

SNMP sends the information over the network using just five protocol elements:

- **GetRequest**: Read request from the SNMP manager for an object defined precisely in the MIB.
- **GetNextRequest**: Read request from the SNMP manager for the next object defined in the MIB.
- **SetRequest**: Write request from the SNMP manager for an object defined precisely in the MIB.
- **GetResponse**: Reply from the agent to a GetRequest, Get NextRequest or SetRequest.
- **Trap**: Asynchronous message from an agent.

The manager and the agents address their messages using Internet addresses and port numbers. Port 161 is reserved for the request protocol elements and port 162 for traps.

Security mechanism

The authorization for a read or write access by the SNMP manager is controlled by a community name. The community name is included in each SNMP message and identifies the sender of the message as a member of a specific group, i.e. community. The manager and agents can only communicate with each other if they belong to the same community.

This relatively simple model is extended to produce a comprehensive security concept with SNMPv3. This enables you to utilize important SNMPv3 functions in the SNMP products for BS2000/OSD, even if you are using SNMPv1 as the protocol, functions such as

- selective allocation of access rights to MIB variables,
- definition of access rights for a group of management stations,
- detailed sending of traps.
3 SNMP management in BS2000/Osd

SNMP in BS2000/Osd is a step towards opening BS2000/Osd for management in heterogenous networks by linking it to the Internet standard.

The integration of SNMP in BS2000/Osd makes it possible to manage BS2000/Osd systems

- within large-scale, vendor-independent networks comprising computers and other devices,
- from a central site and in line with the other systems,
- using SNMP resources.

The management station offers the administration of monitoring and control functions on three levels:

- central monitoring of all the components in the network to determine whether they are functioning
- obtaining specific information (parameter values, utilization data, statistics)
- active manual or automatic system control based on the information received

BS2000/Osd is not bound to a specific platform through the use of the SNMP standard. This allows BS2000/Osd systems to be integrated in the comprehensive information and alarm management facilities provided by modern management stations.

Fujitsu Siemens Computers GmbH provides you with the integration package SMBS2-LT for the Unicenter TNG management station from Computer Associates International, Inc. free of charge. The Framework of Unicenter TNG is a prerequisite for installation of the package on a Windows NT system. The package extends the management station with special elements for BS2000/Osd management. The BS2000/Osd-specific MIBs, which are required for performing integration in other management platforms, are also available.
Fujitsu Siemens Computers also provides three management applications which have been tailored to fit for communication with individual subagents:

- For the Console Monitor subagent:
  CMBS2 (Reliant Unix and Windows NT) and SMAWcmbs2 (Solaris)

- For the Performance Monitor subagent:
  PMBS2 (Reliant UNIX and Windows NT) and SMAWpmbs2 (Solaris)

- For the MIB-II subagent and the BCAM subagent:
  BMBS2 (Reliant UNIX and Windows NT) and SMAWbmbs2 (Solaris)

These applications are supplied with the appropriate interpreter `tclset` (SMAWtcl); they can be integrated into the interface of Unicenter TNG but can also execute as “standalone” applications.
4 Installation and configuration (light version)

SNMP-LIGHT contains the “light” version of the following SNMP agents for BS2000/OSD:

- Master agent
- Console Monitor subagent
- Application Monitor subagent
- HTML subagent
- Performance Monitor subagent
- Host Resources subagent
- MIB-II subagent
- FT subagent
- Supervisor subagent

Although the light versions of the agents provide a restricted functionality compared with the full versions, they do however illustrate the basic way in which the agents work and the benefits to be gained from using the full versions.

You will find application examples for the master agent, and the Console Monitor, Application Monitor and Performance monitor subagents in the chapter "Monitoring with SNMP-LIGHT" (see page 17). The functionality of the other SNMP-LIGHT subagents is described in the chapter "Other SNMP-LIGHT subagents" (see page 49).

Since the agents use the standardized SNMP protocol under BS2000/OSD, they do not require a special management station. The agents can be controlled by any SNMP management system (CA-Unicenter TNG, HP OpenView, etc.). The systems vary, of course, with regard to performance and configuration.

For SNMP-LIGHT Fujitsu-Siemens Computers provides you with the special integration package SMBS2-LT for the Unicenter TNG management station. This package also configures the environment for the examples described in the chapter "Monitoring with SNMP-LIGHT" (see page 17).
4.1 Installing the SNMP manager

The individual management packages require the following software:

<table>
<thead>
<tr>
<th>Package</th>
<th>Software requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tclset</td>
<td>Windows NT Version 4</td>
</tr>
<tr>
<td>CMBS2</td>
<td>tclset (supplied with the product)</td>
</tr>
<tr>
<td>PMBS2</td>
<td>tclset (supplied with the product)</td>
</tr>
<tr>
<td>BMBS2</td>
<td>tclset (supplied with the product)</td>
</tr>
<tr>
<td>SMBS2-LT</td>
<td>Unicenter TNG Framework Version 2.2 and Windows NT Version 4</td>
</tr>
</tbody>
</table>

- First install the Framework (or the full version) of Unicenter TNG on a Windows NT V4.0 system.
- Then install the products listed above in the order specified. You should ensure that TCP/IP is installed as the network protocol and that SNMP is installed as the network service on the system. The master setup `snmp_lt_setup.exe` for all the packages ensures simple installation. The package installations perform all the configurations automatically. During the installations, you decide whether you wish to accept or modify the default settings.

Further information may be found in the readme files for the corresponding products. You can download the master setup for the aforementioned products from the internet at the following addresses:

http://www.fujitsu-siemens.com/servers/snmp/snmp_de/light_ag.htm

or


Following the installation, a few configuration steps are required before your BS2000/OSD system is integrated into the monitoring performed by the management station. The operations in the Unicenter TNG are described in detail in the appendix. Further information may be found in the readme files for the software packages.
4.2 Installing the SNMP-LIGHT agents

The product SNMP-LIGHT can be installed in any BS2000/OSD version $\geq$ V2.0. The individual agents require the following software:

<table>
<thead>
<tr>
<th>Agent / subagent</th>
<th>Software requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master agent</td>
<td>POSIX-BC $\geq$ V1.0 (included in BS2000/OSD-BC)</td>
</tr>
<tr>
<td></td>
<td>IMON $\geq$ V2.0 (included in BS2000/OSD)</td>
</tr>
<tr>
<td></td>
<td>SDF-P-BASYS V2.0B (included in BS2000/OSD-BC)</td>
</tr>
<tr>
<td>Application Monitor subagent</td>
<td>JV $\geq$ V11.2</td>
</tr>
<tr>
<td>Performance Monitor subagent</td>
<td>SM2 $\geq$ V11.2</td>
</tr>
<tr>
<td>FT subagent</td>
<td>FT-BS2000 V5.2 or openFT(BS2000) $\geq$ V6.0</td>
</tr>
<tr>
<td>other SNMP-LIGHT subagents</td>
<td>no special software requirements</td>
</tr>
</tbody>
</table>

Installation in the POSIX subsystem

The POSIX subsystem must be started. The executable agents and configuration files are located in the library SINLIB.SNMP-LIGHT.050. This library also contains the elements which must be installed in the UFS. Installation is performed under the user ID $TSOS$ using the POSIX installation tool:

/CALL-PROCEDURE *LIB(LIB=$TSOS.SINPRC.POSIX-BC.<version>,ELEMENT=POSINST)

Function: Install POSIX program package
- Product name: SNMP-LIGHT
- Product version: 050

You must uninstall the light version before you install the full SNMP version.

Deinstallation from the POSIX subsystem

You also deinstall SNMP-LIGHT under the user ID $TSOS$ using the POSIX installation tool:

/CALL-PROCEDURE *LIB(LIB=$TSOS.SINPRC.POSIX-BC.<version>,ELEMENT=POSINST)

Function: Deinstall POSIX program package
- Product name: SNMP-LIGHT
- Product version: 050
Eine Dokuschablone von Frank Flachenecker
by f.f. 1992
5 Monitoring with SNMP-LIGHT

This chapter provides you with a description of the two basic procedures used to monitor the most important BS2000/OSD components. Additionally, five typical monitoring activities are illustrated by examples:

– basic monitoring
– monitoring the console
– monitoring important applications
– monitoring system performance
– monitoring the subagents

Each example draws from activities illustrated in other examples. This means that, once you have installed SNMP-LIGHT, you will be able to perform basic monitoring of your system after performing a few tasks.

This chapter gives information on the objects supported by the subagents, as well. This will allow you to modify the examples and extend them to encompass other implementations, as well as to create your own monitoring configurations. It is also possible to obtain specific, more detailed information on parameters, utilization data, statistics, etc.

Information for using a management station other than Unicenter TNG can be found in the appendix in the sections “Trap structure“ (see page 75) and “MIBs of the subagents“ (see page 76).
5.1 Monitoring procedures polling and traps

There are two basic ways of monitoring the functioning and state of the central components in a network: polling and traps.

**Monitoring with polling**

When polling is performed, the management station queries the state of the systems being monitored at regular intervals. The manager takes the active role in the communication and controls the activities. The advantage of polling is its reliability: if an agent, the manager or the system fails temporarily, this does not impact the results once communication has been restored. Important is the definition of an appropriate polling rate, which should represent a reasonable compromise between the network load and the amount of time information is delayed.

**Monitoring with traps**

A trap is an asynchronous message sent by an agent which relates to a problem state. If monitoring is performed using traps, the agent overtakes the active role in communication whereby performance is highly important. The network load is reduced to a minimum and the message is unsolicited.

**Combination of polling and traps**

In practice, a combination of polling and traps is frequently used for monitoring: A trap sent to the management system activates polling or lowers a high polling rate.
Monitoring with SNMP-LIGHT

Monitoring procedures polling and traps

Figure 3: Monitoring with polling and traps
5.2 Basic monitoring with the master agent

The master agent is the interface between the subagents and the network, i.e. the management stations. It fulfills the following functions:

- handles the SNMP network protocol
- checks access authorizations
- forwards management station requests to the appropriate subagents

The master agent also supplies basic SNMP protocol data. This comprises information about

- system and SNMP group in the MIB-II,
- SNMP Framework MIB and
- other MIBs.

Configuring the master agent

The configuration file for the master agent is the file `snmpd.light`. It is located in the POSIX file system in the directory `/etc/snmp/agt`.

▶ Enter the IP address of your management station as the `<IP address>` in the `snmpTargetAddrEntry` specifications:

```
  snmpTargetAddrEntry myTarget snmpUDPDomain <IP-address>:0 0 0 Console
  vlExampleParams nonVolatile 255.255.255.255:0
```

This means that this management station is allowed to send queries to the agents. Please do not modify the entry apart from the IP address. This entry also ensures that your management station is entered as a recipient for traps.

Starting the master agent (in BS2000/OSD)

▶ Start the master agent with the command:

```
  /START–SNMP–MASTER–LT
```

▶ You can stop the master agent with the command:

```
  /STOP–SNMP–MASTER–LT
```
Initial tests

The SMBS2-LT package contains a program called snmpetest which enables you to test the functions of the SNMP agent. snmpetest has the following syntax for polling calls:

```
snmpetest [get|getnext|walk]
-<agent-address>
[-c <community>]
[-t <timeout>]
[-r <repeat>]
-o <oid1[,oid2, ...]>
```

You can find a detailed description of snmpetest in the readme file for the SMBS2-LT package.

▲ Enter the following command:

```
snmpetest get -i <IP-address> -o 1.3.6.1.2.1.1.1.0,1.3.6.1.2.1.1.2.0
```

You will receive the following response:

```
  system.sysDescr.0 =
  OCTET STRING - SNMP-Management LIGHT-Version
  system.sysObjectID.0 =
  OBJECT IDENTIFIER - .1.3.6.1.4.1.231.1.6
```

If your management system is located on a UNIX system, you can use the `getone` command on that system to query a single agent object.

▲ Enter the following command in the shell:

```
getone <IP address of the BS2000/OSD system> master sysDescr.0
```

If the test is successful, you will receive the following response:

```
  sysDescr.0=SNMP-Management LIGHT-Version
```

Please note that you can only perform queries from a management station whose IP address you have entered in the community specification in the agent’s configuration file `snmpd.light`. 
Performing basic monitoring

Your system is now “SNMP-capable”. Your system will be recognized and classified by the Discovery functions. If you have installed Unicenter TNG with the SMBS2-LT integration package, you can enter your BS2000/OSD system in the network map.

Use the following command to activate a Discovery for an individual object:

dscvorne -i <IP address of the BS2000 system> -s <subnet mask> -c master

After a short time a BS2000/OSD icon will be displayed in the network map. The Discovery has recognized the object in the network as BS2000/OSD through an SNMP request. If the Object was found in the network without an SNMP request providing more detailed information, then the icon for an unclassified_TCP object will be displayed. Figure 4 shows an extract from a network map showing the BS2000/OSD icon.

Figure 4: Network map for Unicenter TNG showing BS2000/OSD icon, Unispace icon and agent icons
► Now click on the BS2000/Osd icon with the right mouse button; this opens a popup menu, containing the Discover Subobjects entry.

► Click on the Discover Subobjects entry. The contents of the network map will change after a period of time.

► Double-click the BS2000/Osd icon to open a subwindow for BS2000/Osd.

This subwindow now also contains a Unispace icon in addition to the interface icons which may possibly already be present.

► Double-click the Unispace icon to open it.

In the new subwindow you will now see an icon for the master agent; this is coloured green, indicating that the master agent is active. Apart from the master agent, only the Supervisor subagent will also appear as an active agent as it is started automatically together with the master agent.

If you receive no response from the agent during these tests, please refer to the chapter "Problem diagnosis" (see page 67) for information on possible causes.

A further possible means of testing the agent is to query an object value by using a web browser. The associated procedure is described in the chapter "Web access to BS2000/Osd management" (see page 55).

If you need permanent control about your SNMP agent's work, you should configure your management station in such a way that it

– queries an object in the central system group at regular intervals (e.g. such as sysDescr.0 above) and

– receives traps from the agent.

Depending on the capabilities of your management system, you can initiate a visual or audible error indication as a reaction to the absence of a response or as a reaction to a trap which has been received. (It is not possible to set regular polls using the facilities offered by the Framework of Unicenter TNG. To do this, you require the agent technology from the full version.)

► Now stop the master agent in BS2000/Osd with the command:

```
/STOP–SNMP–MASTER–LT
```

If you carry out one of the aforementioned tests on the management system, you will no longer receive a response from the agent. You can also repeat the test using the Discover Subobjects function. After a short time, the BS2000/Osd icon turns black. The reason for this is that the underlying icon for the master agent has turned black. The master icon has switched to the "offline" state because no response has been issued to the SNMP request.
Start the master agent again with the command:

/START–SNMP–MASTER–LT

and click again on the Discover Subobjects entry.

After you have activated Discover Subobjects again, the icons change color back to green.

Request information on the MIB-II system and SNMP group

In its function as a SNMP protocol machine, the master agent supplies basic information on the SNMP protocol, which it makes available in the MIB-II system and SNMP group. The master agent provides, for example, the following information:

– runtime of the agent
– name and type of the system
– number of incoming and outgoing packages
– number of different protocol errors
– number of attempts made to query an agent using an incorrect community name

In Unicenter TNG, you can display this information as follows:

Select the Open Details or Object View entry in the popup menu for the BS2000/OSD icons:

– Open Details is described on page 25.
– Object View is described on page 26.
Open Details menu entry

Click on Open Details to open a folder which provides certain basic information on the system and on the object in the Unicenter TNG Repository. Figure 5 shows the first page of the folder, containing the values from the MIB-II system group.

![Managed Object Notebook for network map objects in Unicenter TNG](image)

Figure 5: Managed Object Notebook for network map objects in Unicenter TNG
Object View menu entry

The Object View menu entry offers another of requesting information on MIB objects. By clicking on Object View you open a window as shown in Figure 6. The tree in the lefthand pane shows you the MIB structure.

► In the lefthand pane, click on the SNMP entry. The values for SNMP are then displayed in the righthand pane.

Figure 6: Object View with SNMP values
5.3 Monitoring the console with the Console Monitor

The Console Monitor subagent is a universal agent and not associated with a particular product. It communicates with the BS2000/OSD console. You can use the Console Monitor subagent to collect messages, filter them according to certain criteria and send them to a management station as a trap. On the other hand, you can issue BS2000/OSD console commands at a management station and display the results of the command execution.

The Console Monitor subagent also provides the prerequisites for automatic responses. By utilizing the facilities of your management station, you can extract data from a message. This data can then be used in certain console commands and sent back to the BS2000/OSD system as a response.

Figure 7: Monitoring the BS2000/OSD console with the Console Monitor subagent
Configuring the Console Monitor subagent

You should perform the following preparatory steps in the specified order if you want the Console Monitor subagent to be able to access the BS2000/OSD system console:

- Set up the operator ID:
  
  /ADD-USER USER-ID=<name of operator ID>, 
  PROT-ATTR=*PAR(LOGON-PASS=<password>), 
  ACCOUNT-ATTR=*PAR(ACCOUNT=<account no.>)

- Create one or more operator roles:
  
  /CREATE-OPERATOR-ROLE OPER-ROLE=<name of operator role>, 
  ROUT-CODE=*ALL

- Assign the operator role(s) to the operator ID:
  
  /MODIFY-OPERATOR-ATTRIBUTES USER-ID=<name of operator ID>, 
  ADD-OPER-ROLE=(<name of an operator role> 
  [, <name of an operator role>] ...)

If SECOS is being used, you should also perform the following two steps:

- Grant the operator ID access authorization for $CONSOLE:
  
  /MODIFY-LOGON-PROTECTION 
  USER-ID=<name of operator ID>,OPER-ACC-PROG=*YES(PASSW-CHEC=*YES)

- Assign the operator ID granted access authorization the OPERATING privilege
  
  /SET-PRIVILEGE PRIV=OPERATING,USER-ID=<operator-id>

A message filter file with the name SNMP.CONSMON.LIGHT is located in the library SINLIB.SNMP-LIGHT.050. The following examples illustrate how this file is used.

In the light version, the generation of traps at the management station is restricted to

- one message number of your choice and
- one TYPE string SNMPLIGHT.

Whereas any console commands can be executed in the full version, the commands in the light version are restricted to STA MSG as an example.
Starting the Console Monitor subagent

- Now start the Console Monitor subagent with the command:
  
  ```bash
  /START-SNMP-CONSMON-LT
  OPERATOR-ID=<name of op. ID>, PASSWORD=<password>,
  OPERATOR-ROLE=(<name of an op. role>[, <name of an op. role>...]),
  MSG-FILTER=SNMP.CONSMON.LIGHT
  ```

- You can stop the Console Monitor subagent with the command:
  ```bash
  /STOP-SNMP-CONSMON-LT
  ```

Console Monitor application

The Console Monitor application CMBS2 allows you to trace the BS2000/OSD console messages transferred by the Console Monitor subagent and execute BS2000/OSD commands without detailed knowledge of SNMP. This management application is tailored to the functionality provided by the Console Monitor subagent.

![Console Monitor application](image)

Figure 8: Console Monitor application
You can start the Console Monitor application in two different ways:

- Select the following menu sequence in the Start menu:
  
  Start → Programs → SNMP Management Applications → Console Monitor

  or

- Activate the Console Monitor entry in the popup menu for the BS2000/Osd icon in the network map of Unicenter TNG.

A comprehensive help system provides you with information on the functionality and the handling of the application, if you have further questions.

Tests

- Start a program on your BS2000/Osd system, e.g. EDT:
  
  /START-PROGRAM FROM-FILE=EDT

  The following message is then displayed on the console:

  BLS0519 PROGRAM ... LOADED

  The following entry is defined in the message filter file SNMP.CONSMON.LIGHT:

  <BLS0519 001 SOURCE=SNMPLIGHT>

  It allows the subagent to forward messages with the message key BLS0519 to the management station as a trap. This trap is edited in the format defined for the object tccTrapString in the MIB sniTcc. This special format is interpreted by both the Console Monitor application and the Message Records in SMBS2-LT. Therefore, provided you have installed SMBS2-LT, you can also view the message on the Event Console of Unicenter TNG.

  The message displayed in the trap window of the Console Monitor application has the following format:

  - The name of the BS2000/Osd system is displayed in the column System.
  - The specification BS2-SNMPLIGHT (from the definition SOURCE=SNMPLIGHT to which the prefix “BS2-” has been added) is displayed in the column Source.
  - The actual console message is displayed in the column Message.

  Specifying SOURCE and DEVICE in the filter file in the full version makes it easier to classify the several hundred messages and to perform detailed filtering.
Monitoring the console (example: UTM0100)

The following example illustrates the monitoring of applications through the evaluation of console messages as a further possible use for the Console Monitor.

You want the following openUTM events to be reported to the management station:

– termination of an application
– loss of a connection
– violation of security breaches

To this end, openUTM must be represented as an icon in the Unicenter TNG network map. The various event classes are to be indicated by the different colors that can be applied to this icon.

The following actions are required in order to display the events:

– configuration of the Console Monitor subagent
– configuration of the openUTM application
– configuration in the Unicenter TNG network map

Configuring the Console Monitor subagent

In the filter file SNMP.CONSMON.LIGHT, change the entry

<BLS0519 001 SOURCE=SNMPLIGHT DEVICE=PROGRAM>

to

<UOM0100 001 SOURCE=UTM DEVICE=UTM>

Configuring the openUTM applications

Message destinations are defined in the openUTM connection module and can be modified with the utility routine KDCMOD. The modified message module must be linked with the subprograms of an application. See the openUTM manuals for more information.

This procedure ensures that the following openUTM messages are output on the BS2000/OSD system console:

End of application / end of task: K059 K060 K058 K056
Loss of a connection: K032 K036 K069
Violation of security breaches: K004 K005 K006 K031

The selection of the messages can be varied.
Configuring the network map for Unicenter TNG

The following is a checklist before configuring the network map for Unicenter TNG:

– The SMBS2-LT package must be installed.
– An object of the class Application having the name of the BS2000/OSD system, extended by the suffix ‘-UTM’, must be generated in the repository (network map). This object must be generated manually in network map Design mode. If possible, it should be placed in the Unispace of the BS2000/OSD system.

The detailed procedure of configuring Unicenter TNG is described in full in the section “Configuring Unicenter TNG: Example: UTM0100” on page 73 in the appendix.

The subagent forwards all the messages written to the console which have the message number UTM0100 to the management station. On the Event Console of Unicenter TNG, an instruction which causes a change in the status of the network map object is linked to the receipt of these special traps. The form of this instruction depends on the error number Knnn contained in the actual message. In this way, the open UTM icon assumes the color assigned to the event.

Figure 9: Unicenter TNG network map with open UTM object
Figure 10: Unicenter TNG Event Console with UTM0100 message
5.4 Monitoring critical applications with the Application Monitor

Like the Console Monitor subagent, the Application Monitor subagent is also a universal agent not associated with a particular product. The Application Monitor subagent monitors applications with the help of

- monitor job variables
- job variables
- log files

The Application Monitor subagent reports any change as a trap to a management station. On this basis, you are able to monitor user applications and tasks. Entries in a specific file can also be sent as traps.

The Application Monitor subagent also monitors subsystems. The Application Monitor subagent forwards status messages from the subsystems to a management station.

You can also query the status of the subsystems and user applications being monitored by sending polls to the Application Monitor subagent from the management station.

Both options, trap and poll, enable universal application monitoring to be incorporated in the alarm management of management stations.

Figure 11: Monitoring important applications with the Application Monitor subagent
Configuring the Application Monitor subagent

A message filter file with the name `SNMP.APPMON.LIGHT` is available and is located in the library `SINLIB.SNMP-LIGHT.050`. The following examples illustrate how this file is used.

In the light version, the monitoring and generation of traps on the management station is limited to

- one subsystem
- one monitor job variable
- one log file.

The contents of general job variables cannot be monitored in the light version.

Starting the Application Monitor subagent

- Start the Application Monitor subagent with the command:
  ```
  /START-SNMP-APPMON-LT FILE-NAME=SNMP.APPMON.LIGHT
  ```

- You can stop the agent with the command:
  ```
  /STOP-SNMP-APPMON-LT
  ```

Tests

Please note that you can only receive traps at a management station if you have entered its IP address in the trap community specification in the configuration file `snmpd.light` of the master agent.

Although the Application Monitor subagent does not have its own management application, you can choose to use the Console Monitor subagent’s management application or the Unicenter TNG Event Console in order to display the traps from the subagent. This is possible because the traps from the Application Monitor subagent and the Console Monitor subagent have the same structure.

- To display traps by using the Console Monitor application, start this application as described above (see page 28).

- Then start a program (e.g. EDT) on your BS2000/OSD system with the monitor job variable SNMP:
  ```
  /START-PROGRAM FROM-FILE=EDT,MONJV=SNMP
  ```
The following entry is defined in the configuration file `SNMP.APPMON.LIGHT`:

```
//ADD-APPLICATION-RECORD
// APPLICATION-NAME = SNMPLIGHT,
// TYPE = USER,
// JV-NAME = SNMP,
// TRAP-CONDITION = (A,R,T)
```

This allows the subagent to register any change to the monitor job variable SNMP. The monitor job variable is set to $R$ when the program is started. The Application Monitor subagent forwards the change in status of the monitor job variable to the management station as a trap.

The message is displayed in the trap window of the Console Monitor application:

- The name of the BS2000/OSD system is displayed in the column `System`.
- The name `SNMPLIGHT` (from the definition `APPLICATION-NAME=SNMPLIGHT` in the configuration file) is displayed in the column `Source`.
- An indication of the change in status of the monitor job variable is displayed in the column `Message`.
- In this example, the column `Object` is empty.

**Monitoring important applications (example: MONJV)**

You want to monitor certain applications which are especially important to you so that you are informed of any failures immediately.

As prerequisites for this example, Unicenter TNG must be installed on your management system together with the integration package SMBS2-LT.

For monitoring purposes, the applications are to be added as icons to the Unicenter TNG network map. Normally the icon is green. The termination of an application is indicated by color change. In the event of an error, the icon color changes to red, while on normal termination the color changes to black. This allows you to deal with problematic applications quickly and easily. In addition, the Event Console displays a message informing you of the name of the application and the system on which the application is running.

After the application has restarted, when the application is running normally again, the alarm indication is reset and the icon color changes back to green. At the same time, a message on the Event Console indicates that the application is running normally again.
The following steps are required in order to start the monitoring:

- Modify the `ADD-APPLICATION-RECORD` entry in the configuration file `SNMPAPPMON.LIGHT` as follows:

  ```
  //ADD-APPLICATION-RECORD
  //  APPLICATION-NAME = <application-name>,
  //  TYPE = *USER,
  //  JV-NAME = <jv-name>,
  //  TRAP-CONDITION=(A,T,R),
  ```

  Proceed as described in the following steps:

- Replace the name `SNMPLIGHT` in `APPLICATION-NAME=`... with the name `<application>` of your application.

- For `JV-NAME=...`, enter the name `<jv name>` of the monitor variable which you use to start the application.

- In the trap information, the name of your application is noted as the source. The parameter `TRAP-CONDITION` defines which status changes in the application are to be reported to the management station by means of a trap. The subagent forwards any change in the first positions of the monitor job variables to the management station if the value “$R...”, “$T...” or “$A...” is assumed.

- Stop the agent and restart it with the modified configuration file.

- In the popup menu for the BS2000/OSD icon, call the function *Discover Subobjects*. An icon for the monitored application is now also generated in the Unispace of the BS2000 system.

  The color of the icon indicates the status of the application:

  - If the application is running, the icon is green.
  - If the application has stopped, the icon is black.
  - Under error conditions, the icon is red.
  - If the application is in an unknown status, e.g. if the monitor JV is not found, the color of the icon changes to gray.

- Start the Unicenter service at the management station with the command `unicntrl start all` and open the Unicenter TNG Event Console by means of the command `caugui conlog`. 

If a trap now reports a change in the status of the application, you will see a message on the Event Console:

![Event Console Screenshot](image)

Figure 12: Unicenter TNG Event Console with a message reporting a status change for a BS2000/OSD-application and with BS2000/OSD console messages

... and a little later a color change of the application icon in the network map (see Figure 13 on page 39).
Figure 13: Monitoring important applications
Monitoring critical applications (example: polling)

As mentioned earlier, the monitoring of an agent based solely on asynchronous trap messages places a smaller load on the network. However, this benefit is achieved at the risk of not always being informed of the status changes for the monitor job variables (e.g. if the application fails).

Two principal causes are responsible for this situation:

- The state change took place *before* the management station or agent was switched on.
- As a result of a network error, the report of the state change does not reach the management station.

A greater level of security is provided by the concept of “trap confirmation” described in the manual “SNMP Management for BS2000/OSD”, which is based on the fact that the manager confirms receipt of the trap by setting a special MIB object.

A significantly greater level of security is provided by the polling method, i.e. where the status is queried explicitly at regular intervals by the management station. In this case, the SNMP manager can repeat the query if the response is not received.

Unfortunately, because no suitable functionality for regular polling is available with the Unicenter TNG Framework, the monitoring functions of SMBS2-LT are implemented in accordance with the following concept:

- Automatic status changes affecting the icons in the network maps are triggered only by traps. If no icon yet exists for the application being monitored, an icon will be generated.
- The popup menu for the BS2000/OSD icon contains the entry *Discover Subobjects*. The functionality associated with this entry not only generates icons for the monitored objects, it also determines the status of all objects. For already existing objects the status will be updated, enabling you to update the status display at any time with this function. After Unicenter TNG has been started and the network map opened, you should call this function in order to obtain a current status display.

If the network is interrupted in the given example, Unicenter TNG receives no response to its request (poll). As a result of this *NoResponse* information, the color of the icon for your BS2000/OSD system changes to blank (= offline) and thus indicates this error state.

Independent of the monitoring function, you can query the status and also further information on the critical applications at any time:
You can obtain the Information in Unicenter TNG as follows:

► Activate the entry Object View in the popup menu for the BS2000/OSD icon.

The new window initially displays the MIB-II values. In the subwindow ObjectView1, you can select a different MIB in a combo box at top center.

► Activate the MIB sniappmon.mib in the combo box.

The tree in the lefthand pane acquires an additional node bearing the designation Vendor Information.

► Double-click the node Vendor Information to display the structure of the Application Monitor MIB.

► Activate the node appMonUserApplEntry. You will then see the table of user applications displayed.

**Monitoring critical applications (example: log file)**

You will now use a log file to send information to the management station from selected applications. The information obtained in this way can be more informative than the status provided by the monitor job variables.

*Configuring the Application Monitor subagent*

The following entry is defined in the configuration file SNMP.APPMON LIGHT:

```
//ADD-LOG-FILE-RECORD  -
//   NAME = /tmp/SNMPLIGHT.LOG,  -
//   APPLICATION-NAME=SNMPLIGHT,  -
//   MONITORING=*YES
```

► Modify this entry by replacing the name SNMPLIGHT in APPLICATION-NAME=... with the name of your application.

► Stop the Application Monitor subagent and start it again with the modified configuration file.

The Application Monitor subagent forwards all the information written to the file /tmp/SNMPLIGHT.LOG to the management station as a trap. This trap has the same format as the trap from the Console Monitor subagent and is therefore displayed in identical form as a message on the Unicenter TNG Event Console.
Subsystem monitoring

In addition to the different types of applications, the Application Monitor subagent is also able to monitor subsystems. In the Light version, the monitoring is limited to a single subsystem. In principle, this kind of monitoring works in exactly the same way as the application monitoring.

This presupposes that the subsystem is entered in the configuration file for the agent. As with the applications, the entry defines which changes in status are to be reported to the management station by means of a trap. The function Discover Subobjects in the popup menu for the BS2000/OSD icons also generates icons subsystems and sets their color according to the status of the subsystem.
5.5 Subagent monitoring with the Supervisor subagent

The task of the Supervisor subagent is to monitor the other subagents. It checks at regular
intervals whether the other subagents are responsive.

The Supervisor subagent sends a trap to the management station in the following three
situations:

– A subagent logs in to the master agent.
– A subagent logs out from the master agent.
– A subagent is no longer responsive.

In addition, the Supervisor subagent provides information on all the subagents that have
logged in to the master agent.

On the one hand, this information includes general data, such as:

– number of active subagents,
– number of supported MIB objects,
– maximum possible number of active subagents,
– number of previously registered subagents.

On the other hand, the Supervisor provides information on the individual subagents, such
as:

– status of the subagent (active, disconnected, undefined),
– time of login,
– time of last communication,
– number of requests responded to,
– number of traps sent,
– smallest supported OID.

Starting the Supervisor subagent

The Supervisor subagent is always started or stopped in conjunction with the master agent.

Enter the following line in the configuration file `snmpd.light`:

```
subagent [:CATID:][$UID.]SYSLNK.SNMP-LIGHT.050 or
subagent [:CATID:][$UID.]SRMLNK.SNMP-LIGHT.050 (for RISC machines)
```

The entry causes the Supervisor subagent to be linked in to the master agent in order
to be started (or stopped) together with it.

No special configuration is required for the Supervisor. When this subagent is active, it
monitors all the subagents in the same manner.
Subagent monitoring in the Unicenter TNG network map

When your BS2000/OSD system is entered in the network map for Unicenter TNG, with Unicenter TNG and the integration package SMBS2-LT on your management system you can utilize the following functions for subagent monitoring:

– The function Discover Subobjects in the popup menu for the BS2000/OSD icon, mentioned several times previously, also generates icons for the subagents in the Unispace and colors them in accordance with the status of the subagents. Figure 12 on page 38 illustrates the contents of a Unispace for a BS2000/OSD, which also contains several subagent icons.

When you call the function Discover Subobjects, you generate a current status indication for the first time.

– Start, stop and failure of a subagent are indicated by means of messages on the Event Console.

– Similarly, a Supervisor trap also results in updating of the status indication for the subagent icons.

You can view the values in the subagent table by means of Object View, where you perform the following steps:

▶ Activate the entry Object View in the popup menu for a subagent icon.

▶ Using the tree on the lefthand side of the window, navigate via the entry Vendor information to the entry superVisSubagentEntry.

▶ You will find the general values under the node superVisGlobalDatas.

Figure 14 on page 45 gives an example of how the subagent table is displayed.
Figure 14: Subagent table displayed in the Unicenter TNG Object View
5.6 Monitoring system performance with the Performance Monitor

The SM2-based Performance Monitor subagent belongs to a group of subagents involved in system management. It supplies basic information on SM2 itself, i.e.

- subsystem status
- version
- measurement interval size
- sampling cycle

The complete set of values correspond to the familiar SM2 report groups and provide information on:

- CPU utilization and I/O activities
- main memory and virtual address space utilization
- main memory occupation by the four standard task categories
- input/output operations
- application-specific data from openUTM
- resource utilization values of individual tasks

Note:

In the light version, only the following CPU values are displayed:

- \textit{sm2TimeIOMachTabIdleTime} (idle time)
- \textit{sm2TimeIOMachTabSIHTime} (SIH time)
- \textit{sm2TimeIOMachTabStopTime} (stop time)

Starting the Performance Monitor subagent

If you want to start the Performance Monitor subagent, you must have already started the subsystem SM2. The subsystem is started implicitly with the SM2 user program.

- Start the SM2 user program with the command
  \[
  /\text{START-PROGRAM FROM-FILE=SM2}
  \]
- Now start the Performance Monitor subagent with the command
  \[
  /\text{START-SNMP-PERFMON-LT}
  \]
- You can stop the Performance Monitor subagent with the command
  \[
  /\text{STOP-SNMP-PERFMON-LT}
  \]
Suitable management application

You can use the performance monitor application PMBS2 to display the values returned by the agents in diagram or table form over time. The application has been tailored to the functionality of the Performance Monitor subagent.

![Performance Monitor: CPU / IO](image)

Figure 15: Display of CPU utilization values by the performance monitor application PMBS2

You can start the performance monitor application in two different ways:

- Activate the entry *Performance Monitor* in the popup menu for the BS2000/OSD icon
- Select the following menu sequence in the Start menu:

  *Start → Programs → SNMP Management Applications → Performance Monitor*

A comprehensive help system provides you with information on the functionality and handling of the application and about the values supported by the Performance Monitor subagent.
Test

Please perform the following steps:

► From the menu of the Performance Monitor application select the menu sequence *Options → Settings*.

► Enter the name and IP address of your BS2000/OSD system in the input fields on the tab card. Select the name *master* as the community name.

► Press the *Ok* button.

► In the main window, select your BS2000/OSD system from the list of objects and check the address and community name.

► Press the *Pmon-Test* button on the toolbar. If the value *alive* is displayed in the column *Agent*, the Performance Monitor subagent is available.

► Select *CPU/IO* under the diagrams and press *Start*.

The application queries the agent for the CPU values at two minute intervals (specified polling rate) and displays the values in diagram and table form.

**Querying the performance values in Unicenter TNG**

In addition to the monitoring, you can query the CPU utilization values manually at any time.

► To obtain a display of these values in Unicenter TNG, select the performance MIB in *Object View*. 
6 Other SNMP-LIGHT subagents

This chapter provides you with a description of the functional scope of the following subagents which SNMP-LIGHT supports:

– Host Resources subagent
– MIB-II subagent
– openFT(BS2000) subagent (FT subagent)
– HTML subagent

The information provided in this chapter allows you to

– modify the examples described in the chapter "Monitoring with SNMP-LIGHT",
– extend them to include other cases,
– create applications for your own particular monitoring needs.

It also makes it possible to obtain more comprehensive and specific information on parameters, utilization data and statistical values.
6.1 Host Resources subagent

The Host Resources subagent belongs to the group of subagents involved with system management. It uses the standardized MIB of the RFC1514 and provides information on, for example:

- devices
- pubsets
- POSIX file systems

In SNMP-LIGHT, only the following values from the storage table can be displayed:

- `hrStorageType` (storage type)
- `hrStorageDescr` (description)
- `hrStorageAllocationUnits` (unit)
- `hrStorageUsed` (storage used expressed as `hrStorageAllocationUnits`)

Starting the Host Resources subagent

You start the Host Resources subagent with the command:

```
/START-SNMP-HOSTRES-LT
```

You can stop the Host Resources subagent with the command:

```
/STOP-SNMP-HOSTRES-LT
```

Querying values

In Unicenter TNG, you can use the Object View to obtain a display of the values from the Host Resources MIB.

- In Object View, select the MIB file `host.mib`

  You will find the structure of the Host Resources MIB under the node `Vendor Information` in the navigation tree in the lefthand half of the window.

- In the Host Resources MIB, select the fields and/or MIB branches that you want to view.

  If you are using a different management station, you must incorporate the MIB from the above-mentioned RFC.
### 6.2 MIB-II subagent

The MIB-II subagent belongs to the group of subagents involved in network management. It supplies information on the standardized MIB-II in accordance with RFC1213. The MIB-II includes the following groups:

- interfaces group
- IP group
- ICMP group
- TCP group
- UDP group

In the light version, the display is limited to the following values of the interfaces group:

- *ifDescr* (interface description)
- *ifType* (interface type)
- *ifPhysAddress* (physical address of the interface)
- *ifAdminStatus* (desired interface status)
- *ifOperStatus* (current interface status)
- *ifLastChange* (system time of the last change in status)

**Starting the MIB-II subagent**

You start and stop the MIB-II subagent in Version 14 and up of BCAM with the commands:

```
/START-SNMP-MIB-MIB2-LT
/STOP-SNMP-MIB-MIB2-LT
```

and in Version 13 of BCAM with the commands:

```
/START-SNMP-BCAM-LT
/STOP-SNMP-BCAM-LT
```
Suitable management application

You can use the BCAM monitor application BMBS2 to display the values returned by the MIB-II subagent over time in diagram or table form. The application is tailored to the functionality of the MIB-II subagent and also the BCAM subagent.

You start the BMBS2 application in the same manner as the Console Monitor application and the Performance Monitor application:

► Start the BCAM Monitor application by activating the entry BCAM Monitor in the popup menu for the BS2000/OSD icon.

or

► Start the BCAM Monitor application directly via the Start menu by means of the menu sequence

    Start → Programs → SNMP Management Applications → BCAM Monitor

A comprehensive help system provides you with information on the functionality and handling of the application and on the values which the MIB-II subagent and BCAM subagent support.

Querying values

MIB-II support is provided by every SNMP management system. Therefore, the values of the interfaces group which are supported by the light version of the MIB-II subagent can be displayed on every management station.

In Unicenter TNG, you will immediately see a display in the Object View without the further selection of a MIB file.
6.3 *openFT(BS2000)* subagent

The *openFT(BS2000)* subagent, or FT subagent for short, belongs to the group of subagents involved in application management. It supplies information on FT system parameters and statistical data on current operation. The FT subagent also allows you to

- start and terminate file transfer
- diagnosis control
- change the public key for encryption

In the light version of the FT subagent, only the following two statistical values can be displayed:

- `ftStatWait` (requests with the status *WAIT*)
- `ftStatActive` (requests with the status *ACTIVE*)

**Starting the FT subagent**

You start the FT subagent with the command:

```
/START-SNMP-FT-LT
```

You can stop the FT subagent with the command:

```
/STOP-SNMP-FT-LT
```

**Querying values**

In Unicenter TNG, you can use the *Object View* to obtain a display of the values from the Filetransfer MIB.

- To this end, load the MIB file `sniFT.mib`.
  
  You will find the structure of the Filetransfer MIB under the node *Vendor Information* in the navigation tree in the lefthand half of the window.

- In the Filetransfer MIB, select the fields or MIB branches that you want to view.
6.4 HTML subagent

The HTML subagent is used for configuring and extending the web interface of the BS2000/OSD agent. Without a special configuration, the BS2000/OSD agent generates only standard HTML pages for the individual MIBs, where the structure of these pages is derived from the MIB definition.

The HTML subagent enables you to supplement these pages by means of special web pages (custom pages) which you can design in accordance with your wishes. These pages contain a selection of MIB objects. No restriction is imposed by the MIB structures with regard to the arrangement of the objects. The objects can originate from different MIBs. The means for accessing these customer-specific pages are described in the chapter "Web access to BS2000/OSD management" (see page 55).

The custom pages and their components are themselves MIB objects which are defined in a special MIB, the HTML MIB. The HTML MIB contains tables used for the definition of these pages. This means that you are to generate new, user-defined pages by means of new objects in these tables. The HTML subagent is required in order to provide support for customer pages. It is not, however, a prerequisite for web access.

SNMP-LIGHT contains the HTML subagent in its full functionality. It is therefore also possible to design user-defined HTML pages with SNMP-LIGHT. However, precise instructions for doing this do not fall within the scope of the present brochure. SNMP-LIGHT contains examples of customer pages which demonstrate the possibilities available to the designer of such pages. For detailed instructions on generating customer pages, refer to the manual “SNMP Management for BS2000/OSD".
# 7 Web access to BS2000/OSD management

In addition to the processing of SNMP requests, the master agent also enables access to the management information via the World Wide Web (WWW). The information provided by the subagents can thus be queried and modified both via an SNMP management station and also by using a web browser.

## 7.1 Two different types of requests

The master agent monitors the network for two different types of requests:

- **On the SNMP port (normally UDP 161), the master agent expects the SNMP Set and Get requests.**
  
  In response to the SNMP requests, the master agent sends SNMP GetResponse messages.

- **On the web-based management port (normally TCP 280), the master agent expects HTTP connection requests.**
  
  In response to an HTTP message, the master agent returns an HTML page to the browser. This HTML page can be a predefined, user-specific web page (custom page) or an automatically generated web page (subtree page).

The part of the master agent that is responsible for processing HTTP messages is called the HTTP engine.

HTTP requests are processed in the same manner as SNMP requests. After evaluating an SNMP or HTTP request, the master agent places the relevant components of the request in an internal queue and obtains the information from the subagents in the normal way. As soon as the master agent has received the information from the subagent, depending on the type of the request, the master agent generates an SNMP GetResponse message or an HTML page and returns this with the desired information to the sender of the original message. As far as the subagent is concerned, there is no difference between SNMP requests and requests from the web.

Figure 16 on page 56 shows the relationship between the SNMP interface and the web interface of the BS2000 agent:
Two different types of requests

Web access to BS2000/OSD management

Figure 16: Structure of the BS2000/OSD agent with SNMP and web access
7.2 Establishing connection to BS2000/OSD Web agent

To establish the connection to the BS2000/OSD Web agent (DR-Web-Entity), specify the network address and port number as follows using your web browser:

http://network-address:port-number

For example, http://D016ZE07:280 is the address of the Web agent on the system D016ZE07.

Entering user name and password

When the connection has been established, you are prompted to enter your user name and password using the browser. A dialog box is displayed (see Figure 17).

![Figure 17: Entering user name and password](image)

The user name and password must be configured on the agent. This is done by means of entries in the configuration file `snmpd.light` in the POSIX directory `/etc/snmp/agt`. The file `snmpd.light` also contains the SNMP configuration data. As supplied, the configuration is preset to accept “gast” as the valid input for the user name, and a blank entry for the password.

- Enter “gast” in the field for the user ID and leave the password field blank.
- Press the OK button.

Following a successful login, the Web agent presents the welcome screen on the browser.
BS2000/OSD Web agent welcome screen

Figure 18 shows the standard welcome screen containing hyperlinks to the subtree and custom page branches and to trap receipt.

![Figure 18: The Web agent welcome screen](image)

You can select from three links:

- **Subtree** takes you to the display of the standard pages which the master agent generates from the MIB definitions.
- **Custom** takes you to the user-specific pages which are defined with the aid of the HTML subagent and the HTML MIB.
- **Traps** opens a page for the trap display. For this purpose, a plug-in with a Java applet is downloaded which enables trap receipt.
7.3 Subtree functionality

When you click on the *Subtree* hyperlink in the DR-Web welcome screen, the subtree functionality which enables simple MIB browsing is available to you.

**Subtree page of Web agent (DR-Web-Subtree-Page)**

The subtree functionality is available via the subtree page of the Web agent. To see the subtree page displayed on the browser:

- click on the subtree hyperlink on the welcome screen or
- enter the following URL in the address field of your browser:
  
  http://IP_address:280/subtree/ .

![Image of DR-Web-Subtree-Page]

Figure 19: DR-Web-Subtree-Page
Through the hyperlinks to the subtree URLs, the subtree page offers fast access to all MIBs. When a MIB hyperlink is selected, the objects for the MIB in question are displayed.

The listing on this page corresponds to the maximum scope of the BS2000/OBD agent. However, the MIB objects can only be displayed on a subtree URL if the associated subagent has been started. So when only blank pages are displayed for some links when using SNMP-LIGHT, this is not an error condition.

By way of example, Figure 20 shows the contents of the Application Monitor MIB as supported in the light version.

Figure 20: Web page containing the objects of the Application Monitor MIB
For other, very extensive MIBs such as the MIB-II, you will see a page displayed containing further hyperlinks which allow you to select individual MIB branches.

If this display is excessively comprehensive for you, you can restrict the display to one branch in the MIB by specifying a MIB node in the URL. The URL http://<IP-address>:280/subtree/appMonSubsysTable, for example, displays only the contents of the subsystem table in the Application Monitor MIB. When the URL http://<IP-address>:280/row/appMonSubsysIndex.1 is specified, the display is restricted to the contents of the first table row.

**Auto-refresh function**

On every web page you will find an AutoRefresh button which enables you to activate the auto-refresh function. The auto-refresh function updates the contents of the page every 60 seconds.

**Set-request functionality**

In addition to querying MIB values (GetRequest), you can also modify the values for the MIB objects on the web interface by means of SetRequest operations. To display the web page required for this, containing the fields for modifying the MIB objects, click on the Set Box button which is located at top right on most web pages.

In the case of a modifiable object, the current value is displayed in an input field. For objects having a restricted value range, you may also find a radio button or an options menu. The check box to the right of the input field serves to specify whether the value is to be modified.

The value for a MIB object can only be modified under the following conditions:

– The MIB object is defined in the MIB as read-write or read-create and implemented in the agent as read-write or read-create.

– You have write authorization for the MIB object.

The current security configuration defined in the file snmp-light is taken into consideration during generation of the web page.
For every scalar MIB object displayed on your browser that you wish to modify, you need to perform the following four steps:

1. Log in with a user ID which has write authorization. The product is supplied with the user ID “admin” and the password “admin” available for this purpose.
2. Select the URL for the MIB page that contains the object to be modified.
3. Switch to Set mode.
4. Enter the desired value for the object.

When you have performed these steps for all the MIB objects, proceed as follows:

- Click on the Set button located beneath the MIB objects.

A similar procedure is employed when modifying table objects or adding new rows in tables. Relevant details may be found in the manual “SNMP Management for BS2000/OSD”.

Figure 21: MIB-II system group
7.4 Custom pages

If you use the HTML subagent on your system, the custom page functionality is also available to you through clicking on the Custom hyperlink on the DR Web welcome screen. This enables you to utilize the preconfigured web pages or to create your own web pages (custom pages). In addition to the HTML specifications concerning page design (text, graphics etc.), these pages also contain macros for accessing MIB objects. Custom pages give you the capability to group information according to suit your individual needs.

As already mentioned under the description of the HTML subagent (see page 54), the light version offers you the capability to design your own pages. The preconfigured customer pages included in the product as delivered give an impression of the capabilities on offer. The generation of custom pages is described in detail in the manual “SNMP Management for BS2000/OSD”.

To access a custom page, enter the keyword “custom” following the network address in the URL, i.e. use the following URL:

http://<IP-address>:280/custom/

Preconfigured custom pages

Preconfigured custom pages are available for the following task areas:

– SNMP management
– network management
– system management
– application management

The preconfigured custom pages are demonstration examples. Each page contains a time stamp, the most important information MIB-II system group, plus the following task-specific information:

● SNMP management
  – SNMP parameters
  – SNMP security information
  – SNMP web configuration

● Network management
  – ICMP statistical values
  – Interface tables
  – Routing tables and routing information
Custom pages

Web access to BS2000/OSD management

- **System management**
  - system resources
  - graphical display of CPU values

- **Application management**
  - subsystems
  - user applications and BCAM applications

![Custom page for displaying the CPU values](image)

Figure 22: Custom page for displaying the CPU values
7.5 Trap display in web browser

The web interface also allows you to open a web page displaying incoming traps in a table. To access this page, click on the Traps hyperlink in the DR-Web welcome screen. Alternatively, you can also specify the URL “http://<IP-address>:280/traps/”.

This table for displaying traps is implemented as a Java applet. As a result of the access restrictions that are demanded for the security of Java applets, only traps originating from the system from which the web page was loaded can be received.

Certain prerequisites are associated with the use of the trap recipient:

- Prerequisites applicable to the management station
  
  The following software must be available on the management station:
  
  - Java plugin-enabled browser, e.g. Netscape Communicator V4.5 or a later version
  - Java plugin x-java applet _ V1.2.2

  If this plugin is not present on the management station, a WWW address at which it is available will be displayed.

- Prerequisites applicable to configuration of the SNMP agent

  The IP addresses of the management stations must be configured as trap destinations with the port 9162 on SNMP agents whose traps are to be displayed by the web browser. The port can be changed, but it must not be privileged, i.e. the port number must be greater than 1024. Furthermore, the port number must match the parameter PORT in the file trap.html.

  You should insert the IP address of your management system in the following line of the file snmpd.light:

  ```
  snmpTargetAddrEntry myTarget1 snmpUDPDoman <IP-address>:9162 0 0
  Webtrap v1ExampleParams nonVolatile 255.255.255.255:0
  ```

  The web page for the trap display is shown in Figure 23 on page 66.
Figure 23: Trap display in the web browser
8 Problem diagnosis

This chapter describes how to diagnose problems in the event of errors
– in the program run
– when querying values (GetRequest)
– when setting values (SetRequest)
– when sending and receiving traps

GetRequests and SetRequests in the context of diagnostics should be performed via the function `snmptest` from the SMBS-LT package or the UNIX utility functions `getone`, `getmany` and `setany`. This prevents errors in the management application from being included. Traps can also be received with `snmptest` outside of management applications.

Please refer to the manual “SNMP Management for BS2000/OSE” for more detailed information on using traces.

8.1 Program run

- Check whether the agent has been started:
  
  /SHOW-JOB-STATUS JOB-ID=*JOB-NAME(SNMPDM)

  If you cannot start the agent, proceed as follows:
  1. Check whether this agent is already running. If this is the case, terminate this agent.
  2. Call the command program using the `-CLEAN` option in order to restore the runtime environment.

     /start-mastercmd-lt
     *CLEAN
8.2 GetRequest

In the case of an errored GetRequest, proceed as follows:

1. Check the connection via ICMP (ping).
2. Query `SysDescr.0` to check
   - the connection to the master agent and
   - read authorization of the community name used
   
   ```
   snmptest get -i <IP address of BS2000 system> -c <community-name> -o 1.3.6.1.2.1.1.1.0
   
   or
   
   getone <IP address of BS2000 system> <community-name> 1.3.6.1.2.1.1.1.0
   ```
3. Check the connection to the subagents by querying the subagent table of the Supervisor subagent:
   
   ```
   snmptest walk -i <IP address of BS2000 system> -c <community-name> -o 1.3.6.1.4.1.231.2.34.1.2.1
   
   or
   
   getmany <IP address of BS2000 system> <community-name> 1.3.6.1.4.1.231.2.34.1.2.1
   ```
4. Activate the traces by starting the agent with the parameter `TRACE=APALL`.

8.3 SetRequest

In the case of an errored SetRequest, proceed as follows:

1. First of all, always check communication via a GetRequest (see above).
2. Check the read authorization of the community name used by setting the object `SysContact.0`:
   
   ```
   snmptest set -i <IP address of BS2000 system> -c <community-name> -o 1.3.6.1.2.1.1.4.0 -s octetstring -v Test
   
   or
   
   setany <IP address of BS2000 system> <community-name> 1.3.6.1.2.1.1.4.0 -D "Test"
   ```
3. Activate the traces by starting the agent with the parameter `TRACE=APALL`. 
8.4 Trap

You diagnose suspected errors when sending traps as follows:

1. If no traps are being received, check communication via a GetRequest first of all (see above).

2. Check the connection to the master agent by
   - triggering a ColdStart trap (starting the master agent) or
   - triggering an Auth-Fail trap (submit a query using an illegal community name e.g. "error").

   Snmptest get -i <IP address of BS2000 system> -c error -o 1.3.6.1.2.1.1.1.0
   or

   getone <IP address of BS2000 system> error 1.3.6.1.2.1.1.1.0

3. Activate the traces by starting the agent with the parameter TRACE=APALL.
Eine Dokuschablone von Frank Flachenecker

by f.f. 1992
9 Appendix

In the appendix, you will find information on

– configuration of Unicenter TNG,
– trap structure,
– subagent MIBs.

9.1 Configuring Unicenter TNG

This section provides you with certain information on how to carry your own configuration of the environment required for the examples in the chapter "Monitoring with SNMP-LIGHT" (see page 17), including an explanation of the meaning of the individual configuration steps. More detailed information on the installation and use of the software package SMBS2-LT may also be found in the readme file contained in the package.

Configuring the network map

When it is installed, SMBS2-LT generates a new object class under the name FSCBS2000. This subclass of Host enables BS2000/OSD objects to be included in the repository and thus also allows the objects to be displayed in the network map each with their own icon.

You can add individual BS2000/OSD objects manually in design mode for the network map or by using automatic discovery. Individual BS2000/OSD systems can easily be included in the network map by means of the command dscvrone:

▶ dscvrone -n <name of BS2000 system> -s <subnet mask>
▶ dscvrone -i <IP address of BS2000 system> -s <subnet mask>
For manual insertion, proceed as follows:

1. Start the 2D network map of Unicenter TNG.
2. Switch to the subnetwork map into which you wish to insert the BS2000/OSD icon.
3. Switch the network map to design mode, either
   – by selecting the entry Design in the menu Modes or
   – by pressing the button for design mode in the toolbar.
4. Find the icon for the class FSCBS2000 in the toolbox containing the icons for all the managed objects. Left-click on the icon and, keeping the mouse button depressed, drag the icon to the desired position in the network map.
5. Release the left mouse button. A notebook is then opened in which you need to specify further details relating to the new object.
   ▶ Specify the object name.
   ▶ Set a label for the network map.
   ▶ Specify the IP address of the object.
6. Now switch back to run mode, either
   – by selecting the entry run in the menu Modes or
   – by pressing the button in the toolbar.

As soon as the new object has been entered in the network map, you can use the function Discover Subobjects in the popup menu for the icon to generate the subobjects.

**Configuring the receipt of traps**

In order to display trap messages on the Event Console and to automatically update the status of the icons in the network map, the management station must be in a position to receive traps.

The following prerequisites apply here:

- The TCP-IP protocol and the network service SNMP must be installed in Window NT.
- The SNMP Trap Server must be activated in Unicenter TNG.

  The SNMP Trap Server is activated in the *Settings* window which you can open in one of two ways:
  – from the Windows NT Start menu
  – from the DOS shell
Opening the Settings window from the Windows NT Start menu

- Select the following menu sequence in the Start menu

  Start → Programs → Unicenter TNG → Enterprise Management → Enterprise Managers

- In the window Enterprise Managers, click on the Windows NT icon.

  A window containing a number of icons is then displayed.

- Select the menu sequence Configuration → Settings

Opening the Settings window from the DOS shell

- In the DOS command shell, issue the command caugui settings.

Activating the SNMP Trap Server in the Settings window

The Settings window is displaying a notebook.

- In the notebook, select the card Client Preferences/Component Activation Flag.

- Locate the entry SNMP Server Activated and enter the value “YES” in the column Setting.

- Close the window.

To activate the new setting:

- Stop any active Unicenter TNG services with unicntrl stop all.

- Restart the Unicenter TNG service with unicntrl start all.

You can then check the display of traps: for example, provoke a trap by starting or stopping a subagent.

Example: UTM0100

To generate the openUTM icon, proceed in a similar fashion to that described on page 72 under “Configuring the receipt of traps” for manual generation of the BS2000/OSD icon:

- Start the 2D network map of Unicenter TNG.

- Switch to the subnetwork map in the Unispace for the BS2000/OSD icon.

  This subnetwork map contains the agent icons. If the BS2000/OSD icon does not contain a Unispace, the simplest way you can generate it is to use the function Discover Subobjects.
Switch the network map to design mode, either
- by selecting the entry Design in the menu Modes or
- by pressing the button for Design mode in the toolbar.

Find the icon for the class Application in the toolbox containing the icons for all the managed objects. It is located in the section Managed Objects.

Left-click on the icon for the class Application and, keeping the mouse button depressed, drag the icon to the desired position in the network map.

When the left mouse button is released, a notebook is opened in which you need to specify further details relating to the new object.

The following details are mandatory specifications:

- Object name
- IP address of the object
- Label for the network map

For the object name, enter the name of the BS2000/OSD node, plus the suffix “-UTM”. The name of the node is output in the message lines on the Event Console.

Enter the IP address of the object and the label for the network map. The label should match the object name.

Switch back to run mode,
- either by selecting the entry run in the menu Modes or
- or by pressing the button for Run mode in the toolbar.
9.2 Trap structure

You will require this information on trap structure if you are using a management station other than Unicenter TNG.

Console Monitor subagent

1. Community: <device> Specification of DEVICE from the message filter file
2. Enterprise: 1.3.6.4.1.231.2.14
3. Trap number: 6/1
4. Variable binding: 1.3.6.1.4.1.231.2.14.1.3 (OCTET STRING)
   "$DATE$:<date> $HOST$:<system> $SOURCE$: BS2-<source> $DEVICE$:<device>
   $MSG$:<msg>"

You should take <device> and <source> from the specifications DEVICE and SOURCE in the message filter file.

Application Monitor subagent

1. Community: <standard>
2. Enterprise: 1.3.6.1.4.1.231.2.14
3. Trap number: 6/1
4. Variable binding: 1.3.6.1.4.1.231.2.14.1.3 (OCTET STRING)
   "$DATE$:<date> $HOST$:<system> $SOURCE$: <appl-name> $DEVICE$: $MSG$: <Application has entered state: <jv-contents>>"

You should take <appl-name> from the specification APPLICATION-NAME in the configuration file.
9.3 MIBs of the subagents

You will find the proprietary MIBs used by the individual subagents under a link to the following Internet address:

http://www.fujitsu-siemens.com/servers/snmp/snmp_de/light_ag.htm

You will need this information on the MIBs of the subagents if you are using a management station other than Unicenter TNG.
## Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASN.1</td>
<td>Abstract Syntax Notation Number One</td>
</tr>
<tr>
<td>ATM</td>
<td>Asynchronous Transfer Mode</td>
</tr>
<tr>
<td>AVAS</td>
<td>Auftragsverwaltungs- und -abwicklungssystem</td>
</tr>
<tr>
<td>BCAM</td>
<td>Basic Communication Access Method</td>
</tr>
<tr>
<td>EMANATE</td>
<td>Enhanced MANagement Agent Through Extensions</td>
</tr>
<tr>
<td>FDDI</td>
<td>Fiber Distributed Data Interface</td>
</tr>
<tr>
<td>FT</td>
<td>File Transfer</td>
</tr>
<tr>
<td>HIPLEX</td>
<td>Highly Integrated System Complex</td>
</tr>
<tr>
<td>HIPLEX OP</td>
<td>HIPLEX Operations</td>
</tr>
<tr>
<td>HNC</td>
<td>High-Speed Net Connect</td>
</tr>
<tr>
<td>IAB</td>
<td>Internet Architecture Board</td>
</tr>
<tr>
<td>IANA</td>
<td>Internet Assigned Number Authority</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>INCA</td>
<td>Intelligent Network Communication Attachment</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>MIB</td>
<td>Management Information Base</td>
</tr>
<tr>
<td>NMCP</td>
<td>Network Management Communication Protocol</td>
</tr>
<tr>
<td>OID</td>
<td>Object Identifier</td>
</tr>
<tr>
<td>OSD</td>
<td>Open Server Dimension</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection</td>
</tr>
<tr>
<td>PDN</td>
<td>Programmsystem für Datenfernverarbeitung und Netzsteuerung</td>
</tr>
<tr>
<td>PDU</td>
<td>Protocol Data Unit</td>
</tr>
<tr>
<td>RDBMS</td>
<td>Relational Database Management System</td>
</tr>
<tr>
<td>RFC</td>
<td>Request for Comment</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>SMI</td>
<td>Structure of Management Information</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>SNMP-Version 3</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UPIC</td>
<td>Universal Programming Interface for Communication</td>
</tr>
<tr>
<td>UTM</td>
<td>Universeller Transaktionsmonitor / Universal Transaction Monitor</td>
</tr>
<tr>
<td>WWW</td>
<td>World Wide Web</td>
</tr>
</tbody>
</table>
Related publications

SNMP Management V5.0
SNMP Management for BS2000/OSD
User Guide

Target group
The manual addresses network administrators/operators and system administrators who wish to integrate a BS2000 system in SNMP-based management or operate such a system.

Contents
This manual describes how SBA-BS2, SSC-BS2, SSA-SM2-BS2 and SSA-OUTM-BS2 are embedded in BS2000/OSD, the installation and configuration procedures required to enable operation, and actual system operation. The Agents and their MIBs which are required for monitoring are dealt with in detail. Installation and configuration of the relevant management applications on the Unicenter TNG, TransView SNMP and HP OpenView management platforms are also described.
Further central topics of the manual are access to management information via the World Wide Web, and the Trap Server for Solaris and Reliant UNIX.

openUTM (BS2000/OSD)
Generating and Handling Applications
User Guide

Target group
This manual is intended for application planners, technical programmers, administrators and users of UTM applications.

Contents
The manual describes the generation of UTM applications with distributed processing, the tools available with openUTM for this purpose, and the UTM objects created in the course of generation. It also contains all the information necessary for structuring, operating and monitoring a productive UTM application.
Related publications

Other Publications

Douglas Steedman
Abstract Syntax Notation One (ASN.1): The Tutorial and Reference
Isleworth, 1990
(ISBN 1-871802-06-7)

Marshall T. Rose
The Simple Book: An Introduction to Management of TCP/IP-based Internets
Prentice-Hall

Ordering manuals

Please apply to your local office for ordering the manuals.
Index

A
access authorization (request)  9
agent see SNMP agent
alarm management  11, 34
application
  management  5
  monitoring  34
  monitoring (e.g.log file)  41
  monitoring (e.g.polling)  40
  monitoring (MONJV)  36
Application Monitor subagent  15, 34
  configuring  35
  starting  35
  testing  35
Auto-refresh function (Web agent)  61

B
basic monitoring
  performing  22
BMBS2  12
BS2000/OSD, SNMP integration  11

C
central management station  1
CMBS2  12
community name  9
configuring
  Application Monitor subagent  35
  Console Monitor subagent  28, 31
  light version  13
  master agent  18, 20
  openUTM application  31
  openUTM icon  73
  receipt of trap  72
configuring (continuation)
  Unicenter TNG  71
  Console Monitor subagent  12, 27
    configuring  28, 31
    example  31
    starting  29
    suitable management application  29
    testing  30
  console monitoring  27
  custom page (Web agent)  63

D
decentralized system  1
dehinstalling SNMP-LIGHT  15
DR-Web see web
DR-Web agent see Web agent

E
EMANATE agent  7
  entering user name  57
  entering password  57
Event Console (Unicenter TNG)  33, 38

F
FT subagent  15, 53
  light version  53
  querying values  53
  starting  53

G
GetNextRequest  9
GetRequest  9
  problem diagnosis  68
GetResponse  9
Stichwörter

H
Host Resources subagent
   light version  50
   querying values  50
   starting  50
HTML subagent  54
HTTP request  55

I
installing
   light version  13
   SNMP-LIGHT  15
Internet address  9

J
job variable  34
   monitor  34

L
light version  35
   FT subagent  53
   Host Resources subagent  50
   installing and configuring  13
   MIB-II subagent  51
   monitoring  35
   SNMP agent  8
log file  34, 41

M
management application
   BMBS2  2
   CMBS2  12
   for Console Monitor subagent  29
   MIB-II subagent  52
   Performance Monitor subagent  47
   PMBS2  12
   SMAWbmbs2  12
   SMAWcmbs2  12
   SMAWpmbs2  12
Management Information Base siehe MIB
management protocol  1
management station  1, 6
   central  1
   Unicenter TNG  11
manager see SNMP manager
master agent  15
   basic monitoring  20
   configuring  18, 20
   starting  20
   testing  21
master/subagent principle  7
master-setup snmp_lt_setup.exe  14
MIB  9
MIB-II
   SNMP group  24
   system group  24
MIB-II subagent  12, 51
   light version  51
   management application  52
   querying values  52
   starting  51
monitor job variable  34
monitoring  11
   application (e.g.log file)  41
   application (e.g.polling)  40
   application (MONJV)  36
   combined  18
   console  27
   console (UTM0100)  31
   critical applications  34
   in the light version  35
   procedures  18
   system performance  46
   with polling  18
   with SNMP-LIGHT  17
   with trap  18

O
Object Notebook (Unicenter TNG)
openFT(BS2000) subagent see FT subagent
openUTM application
   configuring for monitoring  31

P
password, entering  57
Performance Monitor subagent  12, 15, 46
   starting  46
   suitable management application  47
Performance Monitor subagent (continuation)
    testing 48
PMBS2 12
polling 18
    monitoring with 18
    rate 18
port number 9
preconfigured, custom page (Web agent) 63
problem diagnosis 67
program run, problem diagnosis 67
protocol element see SNMP protocol element
protocol, management 1

Q
querying
    values (FT subagent) 53
    values (Host Resources subagent) 50
    values (MIB-II subagent) 52

R
Request 55

S
security mechanism 9
SetRequest 9
    problem diagnosis 68
    functionality (Web agent) 61
Simple Network Management Protocol
    see SNMP
SMAWbmbs2 12
SMAWcmbs2 12
SMAWpmbs2 12
SMBS2-LT 11
SNMP 1
    C/S architecture 5
    integration in BS2000/OSD 11
SNMP agent 7, 9
    Application Monitor 15, 34
    EMANATE 7
    FT subagent 15, 53
    HTML subagent 54
    light version 8
    master agent 15
    MIB-II subagent 51

SNMP agent (continuation)
    Performance Monitor 15, 46
SNMP group (MIB-II), query information 24
SNMP manager 6, 9
    configuring 14
    installing 14
SNMP operation 9
SNMP protocol element 9
SNMP-LIGHT 8, 13
    deinstalling 15
    monitoring 17
    subagent 49
starting
    Application Monitor subagent 35
    Console Monitor subagent 29
    FT subagent 53
    Host Resources subagent 50
    master agent 20
    MIB-II subagent 51
    Performance Monitor subagent 46
subagent 49
    Application Monitor 15, 34
    Console Monitor 27
    FT subagent 15, 53
    MIB-II subagent 51
    Performance Monitor 15, 46
    subtree functionality (Web agent) 59
    supervisor subagent 43
subtree functionality (Web agent) 59
subtree page (Web agent) 59
supervisor subagent 43
starting 43
system group (MIB-II), query information 24
system management 5
system performance
    monitoring 46
    system, decentralized 1

T
Tclset 14
TCP/IP 5
testing
  Application Monitor subagent  35
  Console Monitor subagent  30
  master agent  21
  Performance Monitor subagent  48
trap  9, 18, 34
  generating in the light version  35
  monitoring with  18
  problem diagnosis  69

U
Unicenter TNG  13
  event console  33, 38
  configuring  71
  management station  11
  network map  22, 32
  Object Notebook  25
  Object View  26, 45
username, entering  57
vorkonfiguriert, Custom-Page (Web-Agent)  63

W
Web agent  57
  Auto-refresh function  61
  custom page  63
  SetRequest functionality  61
  Subtree functionality  59
web browser, trap display  65
Web access  55
Contents

1 Preface .......................................................... 1

2 Overview of SNMP .................................................. 5

3 SNMP management in BS2000/OSD ............................ 11

4 Installation and configuration (light version) .................. 13
   4.1 Installing the SNMP manager ..................................... 14
   4.2 Installing the SNMP-LIGHT agents .............................. 15

5 Monitoring with SNMP-LIGHT ..................................... 17
   5.1 Monitoring procedures polling and traps ......................... 18
   5.2 Basic monitoring with the master agent .......................... 20
   5.3 Monitoring the console with the Console Monitor ............... 27
   5.4 Monitoring critical applications with the Application Monitor 34
   5.5 Subagent monitoring with the Supervisor subagent ................ 43
   5.6 Monitoring system performance with the Performance Monitor 46

6 Other SNMP-LIGHT subagents .................................. 49
   6.1 Host Resources subagent ........................................... 50
   6.2 MIB-II subagent .................................................. 51
   6.3 openFT(BS2000) subagent ......................................... 53
   6.4 HTML subagent .................................................. 54

7 Web access to BS2000/OSD management ........................ 55
   7.1 Two different types of requests ................................ 55
   7.2 Establishing connection to BS2000/OSD Web agent ............. 57
   7.3 Subtree functionality ............................................. 59
   7.4 Custom pages ..................................................... 63
   7.5 Trap display in web browser ..................................... 65

8 Problem diagnosis ................................................ 67
   8.1 Program run ...................................................... 67
   8.2 GetRequest ....................................................... 68
   8.3 SetRequest ....................................................... 68
   8.4 Trap ............................................................. 69
## Contents

9 Appendix .......................................................... 71
  9.1 Configuring Unicenter TNG .................................................. 71
  9.2 Trap structure .......................................................... 75
  9.3 MIBs of the subagents .................................................. 76

Abbreviations .......................................................... 77

Related publications .................................................. 79

Index ................................................................. 81
SNMP-LIGHT V5.0 (BS2000/OSD)

SNMP management for BS2000/OSD

Brief Description

Target group
This brochure is intended for network administrators, network operators and system administrators of BS2000/OSD who wish to use the demp version SNMP-LIGHT to obtain information on the integration of BS2000/OSD in SNMP-based management.

Contents
After a brief introduction to the concept of SNMP and SNMP integration of BS2000/OSD, the brochure describes the installation of SNMP-LIGHT. Selected sample applications are then described to show users how they can manage their BS2000/OSD system step by step.

Edition: April 2001

File: snmp_lgt.pdf


All rights reserved.
Delivery subject to availability; right of technical modifications reserved.

All hardware and software names used are trademarks of their respective manufacturers.
Information on this document

On April 1, 2009, Fujitsu became the sole owner of Fujitsu Siemens Computers. This new subsidiary of Fujitsu has been renamed Fujitsu Technology Solutions.

This document from the document archive refers to a product version which was released a considerable time ago or which is no longer marketed.

Please note that all company references and copyrights in this document have been legally transferred to Fujitsu Technology Solutions.

Contact and support addresses will now be offered by Fujitsu Technology Solutions and have the format …@ts.fujitsu.com.

The Internet pages of Fujitsu Technology Solutions are available at http://ts.fujitsu.com/...


Copyright Fujitsu Technology Solutions, 2009

Hinweise zum vorliegenden Dokument


Das vorliegende Dokument aus dem Dokumentenarchiv bezieht sich auf eine bereits vor längerer Zeit freigegebene oder nicht mehr im Vertrieb befindliche Produktversion.

Bitte beachten Sie, dass alle Firmenbezüge und Copyrights im vorliegenden Dokument rechtlich auf Fujitsu Technology Solutions übergegangen sind.


Copyright Fujitsu Technology Solutions, 2009