

# **PRIMERGY ServerView Suite**

## **PRIMERGY Glossary**

Edition September 2009

## **Comments... Suggestions... Corrections...**

The User Documentation Department would like to know your opinion of this manual. Your feedback helps us optimize our documentation to suit your individual needs.

Feel free to send us your comments by e-mail to [manuals@ts.fujitsu.com](mailto:manuals@ts.fujitsu.com).

## **Certified documentation according to DIN EN ISO 9001:2000**

To ensure a consistently high quality standard and user-friendliness, this documentation was created to meet the regulations of a quality management system which complies with the requirements of the standard DIN EN ISO 9001:2000.

cognitas. Gesellschaft für Technik-Dokumentation mbH

[www.cognitas.de](http://www.cognitas.de)

## **Copyright and trademarks**

Copyright © 2009 Fujitsu Technology Solutions GmbH.

All rights reserved.

Delivery subject to availability; right of technical modifications reserved.

All hardware and software names used are trademarks of their respective manufacturers.

---

# Glossary

## 1

### **19 inch Rack**

Cabinet for installing electronic devices (system components and servers) with a standardized width of 19 inches.

## 3

### **3rd-Party Rack**

Installation cabinet from a 3rd-party manufacturer.

## A

### **Active Directory**

Part of the Active Platform concept from Microsoft. AD is a scalable, hierarchical directory service for the central administration of all resources relevant for a network. These include user and group IDs as well as workstations, servers and printers. One or more administrators can manage the directory data and directory structure of the entire network and release or block the required network resources for network users. AD is based on DNS and is LDAP-capable.

### **Advanced Configuration and Power Interface**

Open industry standard for device configuration, hardware detection and power management in notebooks, PCs and servers. The ACPI specification transfers full control of the power management of the individual computer components to the operating system. This results in more finely-tuned and thus more effective power management.

### **Advanced Technology Attachment**

Name given by the ANSI group X3T10 to IDE interface standards which regulate the communication between computers and storage media.

### **Advanced Technology Attachment Packet Interface**

Standard interface between a computer and CD-ROM/tape drives. ATAPI allows the connection of these drives to an IDE controller.

### **Advanced Video Redirection**

A feature of the RSB/ RSB S2/ RSB S2 LP (3HU) that allows the remote administrator to work on their PC as if they were sitting in front of the managed server (graphical console redirection, control over keyboard and mouse of the managed server). See also Console redirection.

### **Alarm**

Whenever an agent detects an unusual operating state, it sends an alarm (trap) to the manager. Alarms are assigned to an alarm level (error class, severity), which is displayed in the user interface in a specific color. See also Trap.

### **Alarm action**

An alarm recipient can be configured such that an action is triggered if there is a change in status.

### **Alarm Configuration**

Component of the AlarmService of the PRIMERGY ServerView Suite. Used to define the settings for alarm handling.

### **Alarm Monitor**

Component of the AlarmService of the PRIMERGY ServerView Suite. Used to display and edit all alarms received.

### **Alarm Service**

Component of the PRIMERGY ServerView Suite. Consists of the components Alarm Monitor and Alarm Configuration. See also Alarm Monitor and Alarm Configuration.

### **Alternating Current**

International abbreviation which identifies an operating-voltage value (e. g. 220 V AC).

### **American Power Conversion**

Web-based product for network management. Uses several open standards such as Telnet, HTTP and SNMP to guarantee complete management of supported devices such as the current-protection solutions from APC.

### **Apache Web Server**

Freely available Web server software distributed under an Open Source license. Different versions of Apache are available to run on Linux, UNIX, NetWare® and Windows servers.

### **Application-Specific Integrated Circuit**

A component on the system board that is designed for a specific application (e. g. controlling and monitoring the fans).

### **Archive Manager**

Component of the Asset Management in the PRIMERGY ServerView Suite. Used to record and store system and operating data of PRIMERGY servers for monitoring and evaluation.

### **Asset Management**

Integrated management of the software and hardware inventory within IT application scenarios. Components available for Asset Management within the PRIMERGY ServerView Suite are Inventory View, Version Manager, Inventory Manager and Archive Manager. See also Inventory View, Inventory Manager and Archive Manager.

### **Attribute**

Property of an object or database entry. In connection with ServerView: part of an object type definition in a MIB module or a class definition in CIM. Refers to a property in an object type or a class.

### **Authentication**

Process which checks the identity of a user at logon. Authentication usually occurs via the user name and password. Process which uses a digital signature to check during data transfer via the Internet whether the specified data source is identical with the actual sender of the data. This averts active attacks on the network security whereby the attacker positions themselves between the two communication partners ("man-in-the-middle") and pretends to each to be the other.

### **Automated Deployment Service**

Deployment procedure from Microsoft for distributing MS Server operating systems over multiple servers of the same type. See also Deployment.

### **Automatic Server Reconfiguration and Restart**

ASR/R functions control the behavior of PRIMERGY servers when errors occur. With ASR/R, critical situations are recognized and shutdown is initiated. The system is then automatically restarted,

with any defective components being masked (e. g. faulty memory modules or - in multiprocessor systems - faulty processors).

## **B**

### **Baseboard Management Controller**

Additional separate processor on the system board of a PRIMERGY server which is connected to the main processor and the various components via IPMI. It monitors and reports the status of various components regardless of whether the main processor is functional or not.

### **Basic Input/Output System**

The BIOS is the first program to run after the computer is started. The functions it executes include: Initialize and test hardware. This process is called POST (Power-On Self-Test). Offer setup for modifying the system configuration. Load and start operating system. See also Power-On Self-Test.

### **Battery Backup Unit**

A battery installed in a device to back up data buffered in the cache. If the computer crashes, the data buffered in the cash is not lost. A BBU is required, for example, for secure operation of a RAID controller working with activated write-back cache. Not all RAID controllers can be fitted with a BBU.

### **Blade server**

Compact, modular server system that offers high performance using little space. A blade server system consists of a number of CPU boards, known as server blades, together with some switch blades, which are the I/O modules, and finally a redundantly configured pair of management blades, enabling the user to monitor and control the system as a whole. Storage capacity and I/O functions

are separated from the server blades. See also RemoteView management blade, Switch blade and

### **BladeFrame**

A compact, modular server, which provides high processing power in a small space and high flexibility through virtualized hardware. A BladeFrame consists of: - Multiple CPU modules, called processing blades; the storage capacity and I/O functions are implemented separately from the processing blades. - Switch blades, which serve as I/O modules between the individual blades. - Two redundantly configured control blades for network connection, monitoring and controlling of the BladeFrame.

### **BMC Manager**

Independent component within the RemoteView software which enables access to the BMC (Baseboard Management Controller) of a managed PRIMERGY server. The BMC Manager offers numerous actions and information for the managed server. It also allows up to 40 PRIMERGY servers (arranged in groups) to be managed remotely. The BMC Manager can be started locally on the server on which it is installed, via the Start menu, on a remote workstation via ServerView Operations Manager (provided the BMC Manager is installed on the remote workstation) or from any computer via a Web browser. See also RemoteView and ServerView Operations Manager.

### **Boot retry counter**

A setting in the BIOS (Basic Input Output System) which specifies the maximum number of attempts allowed to start the operating system.

## C

### Cache

Local fast buffer storage integrated in a processor (processor cache) or a hard disk (hard-disk cache). Contains a copy of frequently required information. The processor cache buffers frequently used instructions, thus reducing the number of main-memory accesses, which are 5–20 times slower. This results in higher processor performance. The hard-disk cache buffers the read and write accesses to the hard disk, thus bridging the latency during disk accesses. This results in a higher data transfer rate. As well as the above two types, there is also memory cache and software cache.

### Central Processing Unit

The main processor of a computer.

### Certificate Authority

In connection with public-key cryptography, a central, autonomous body (agency, company etc.) that issues digital certificates and signs them with the private key of the CA. A certificate signed in this way confirms that the public key it contains belongs to the person, organization etc. named in the certificate. The CA provides a legally binding guarantee of the proven identity of the certificate holder. Depending on the level of confidentiality, the CA requires a valid e-mail address, a valid host name or further proof of identity. See also Digital certificate, Private key and Public key.

### Character-separated values

File format for storing and exchanging simply structured data. The values stored in the file are separated from each other by a comma or another defined character.

### **chipDISK**

RemoteView storage medium with an IDE interface. Contains the test and diagnosis software for RemoteView (RTDS), which can be automatically loaded from the chipDISK in the event of an error and then executed.

### **Chipkill™**

Advanced Error Correcting Code (ECC) technology. Unlike ECC error correction, which can only correct 1-bit errors, the Chipkill™ function can correct up to 4-bit errors and recognize 8-bit errors. If errors accumulate in a memory module, this module can even be masked without requiring system shutdown. See also Error Correcting Code (ECC).

### **Cloning**

Copying the installation and configuration data from one system (reference system) onto several systems of the same type. This is done by saving a raw copy of the hard disk of the reference system in an image file. This image file then serves as the basis for the automatic installation and configuration of the systems. See also Image file and RemoteDeploy.

### **Cluster**

Two or more independent computers which are addressed and managed as a single system. Clustering is used, for example, to increase computing capacity or to guarantee failsafety.

### **Codepage**

Used to support character sets and keyboard layouts from different languages/countries. A codepage is a table that maps binary character codes used by programs to characters on the keyboard or the screen.

### **Command Line Interface**

Interface for controlling an operating system or a program. In a CLI the commands are written directly into the input area as a character string (command line) via the keyboard.

### **Command Line Protocol**

Text-based interface for entering commands (e. g. SQL commands).

### **Common Information Model**

Object-oriented data model standardized by the DMTF (Distributed Management Task Force). For Web-based enterprise management, CIM specifies a standardized representation of the managed components (devices, file systems etc.) as classes or objects. CIM features several levels, known as schemas, which are hierarchically arranged. The highest, the metaclass, contains the specification of CIM. Below it are the core schema, common schema and extension schema, in which the classes are defined. For automated processing, the class definitions are stored as MOF files. See also Web-Based Enterprise Management.

### **Community**

A group of systems (manager and agents) that communicate via SNMP. The group is uniquely identified via the community string. Only systems belonging to the same community can communicate with each other. A system can belong to more than one community. See also Community string.

### **Community string**

Name of a community. In SNMP-based communication between manager and agent, the community string has the role of a password: The agent needs the community string from the manager

before it provides the information about the agent system. See also Community and Agent.

### **Compact Disc**

Widely used storage medium/data volume. See also Compact Disc-Read Only Memory.

### **Compact Disc-Read Only Memory**

Data volume on which the stored data can only be read.

### **Complementary Metal Oxide Semiconductor**

Technology for manufacturing integrated circuits with low power consumption and high interference immunity. This technology is used, for example, in RAMs.

### **Component Object Model**

Standard for object-oriented program components (“COM controls”). The idea is that, when implementing applications, programmers can simply use existing functional modules, which may also come from other providers.

### **Computer Associates**

Provider of management software.

### **Console**

A control unit via which users communicate with a system. A console is usually perceived to consist of the output (display) and input (mouse and keyboard) functions of a system. See also Console redirection.

**Console menu**

In the PRIMERGY ServerView Suite: Remote-management interface which is called up in the RemoteView/ Web front-end or the RemoteView/LAN front-end when a RemoteView management blade is accessed. The console menu offers access to various information on the managed server as well as text-only console redirection. See also RemoteView/Web front-end, RemoteView/LAN front-end and RemoteView management blade.

**Console redirection**

Redirection of the console of a system (display and input functions) to a different system via a terminal or Web application. A distinction is made between text-only console redirection, which can only redirect screen output in text mode, and graphical console redirection, which can also redirect graphical screen output. Redirecting input functions is a particular challenge and is therefore implemented to varying extents, depending on the application: from redirecting keyboard input only, to additional redirection of mouse control, right through to the consideration of different keyboard layouts. See also Console and Advanced Video Redirection.

**Cylinder Head Sector**

Method of addressing a hard disk by specifying the cylinder, head and sector number. In this way, each sector can be clearly localized and addressed.

**D****DataCenter Rack**

Installation cabinet with additional cable-management facility for system components of the PRIMERGY server series.

### **Demilitarized zone**

Separate small computer network which implements a neutral, protected area between a confidential, internal network (e. g. intranet) and the public Internet. Firewalls on both sides of the DMZ shield the confidential network from accesses from the Internet. Running HTTP servers, DNS servers etc. in the DMZ enables the corresponding Internet services to be used in the confidential network without the risks associated with actually placing these services in that network. See also Firewall.

### **Deployment**

Method of installing and preconfiguring computers for immediate use. Deployment involves reference installation, image creation and cloning. See also Image.

### **Deployment server**

The deployment server is the central instance that prepares the servers and their environment for use over the LAN. The PXE boot service is installed on the deployment server. See also Local Area Network.

### **Desktop Management Interface**

Standard developed by the DMTF for central PC, notebook and server management. DMI will not be developed any further. Its successor standard is the Common Information Model (CIM).

### **Diagnostic LED**

Component of the LocalView concept of the PRIMERGY Server-View Suite. Consists of light-emitting diodes positioned alongside key components (main memory, CPU etc.) of a computer to make it easier to identify defective components. See also LocalView.

### **Digest**

Also called message digest or checksum. A digest is a fixed-length character string which is generated from the plain text of a document using a mathematical function (cryptographic hash function) and is assigned to this document one-to-one as a digital signature. Digests guarantee the data integrity of the documents they identify during transport over a TCP/IP network.

### **Digital certificate**

In connection with public-key cryptography, a document issued by a Certificate Authority (CA). The certificate is signed with the CA's private key, which means that the CA vouches for the identity of the certificate owner. See also Certificate Authority.

### **Digital Video Disc**

Optical storage medium, similar to a CD but with much higher storage capacity.

### **Direct Current**

International abbreviation which identifies an operating-voltage value (e. g. 5 V DC).

### **Direct Memory Access**

Method of accessing the system memory without involving the microprocessor.

### **Directory service**

Central directory service for managing a network. The directory service manages, for example, user and group IDs, servers and printers.

### **Discovery**

In server management, managed objects can be detected in a network via the Discovery function.

### **Distributed Management Task Force**

Formerly Desktop Management Task Force. Consortium of manufacturers for developing new standards for system management. The most important DMTF standard is the Common Information Model.

### **Domain**

Logical subnetwork within a network.

### **Domain Name Service**

TCP/IP protocol of the application level which converts the symbolic computer names normally used in TCP/IP user programs (domain names) into IP addresses. DNS implements the network-wide assignment of computer names to IP addresses with the help of a distributed database, whose information is available to all interested parties in the network.

### **Download Manager**

Component of the Update Management of the PRIMERGY Server-View Suite. Used to automatic search and download update data for PRIMERGY servers in the support directory of the FSC Web server.

### **Dual Inline Memory Module**

Type of memory module in the main memory with a 64-bit data bus and contacts on both sides of the printed board.

### **Dual Inline Package switch**

Small switches, usually arranged in a row, which are used to configure electronic devices.

### **Dummy module**

A placeholder module for unoccupied slots/bays in a computer. All unoccupied slots must be fitted with a dummy module for cooling purposes, to comply with EMC regulations, and for fire protection.

### **Duplex Data Manager**

Software solution for PRIMERGY servers which allows the mirroring of data onto the redundantly configured storage subsystems over large distances. DDM consists of the components DuplexWrite and MultiPath. See also DuplexWrite and MultiPath.

### **DuplexWrite**

DuplexWrite is a component of Duplex Data Manager. DuplexWrite mirrors data onto another, remote storage subsystem.

### **DuplexWrite group**

A group of two redundant hard disks configured with DuplexWrite. Both elements (DuplexWrite hard disks) of a DuplexWrite group contain identical (user) data. From the point of view of the operating system, the DuplexWrite group is a single hard disk. Every DuplexWrite group has a preferred hard disk (by default this is the first hard disk) from which the data is read.

### **Dynamic Host Configuration Protocol**

TCP/IP protocol for central, dynamic management of the TCP/IP configuration parameters of computers in a network: IP address, subnet mask, responsible router and any further parameters. A computer that wants to log on to the Internet (TCP/IP network) can ask

for these settings from a DHCP server. Thus the DHCP server automatically assigns a free IP address to a DHCP client computer when it logs on to a TCP/IP network.

## E

### **Electrically Erasable Programmable Read-Only Memory**

Memory module whose contents can be deleted and rewritten ("flashed") with the help of an electrical signal.

### **Electromagnetic compatibility**

Since the end of 1992 the law on EMC has made it compulsory for every manufacturer of electronic products to prove and guarantee the electromagnetic compatibility of their products. The aim is to prevent the emission of unacceptably high interfering radiation from the device or system. Furthermore, products must not be susceptible to externally produced electromagnetic fields.

### **Electrostatic discharge**

Component that can be damaged or destroyed by electrostatic discharge. Electrostatic charge can e.g. result from friction. ESDs must be handled with the necessary precautions to prevent static charge!

### **Emergency Management Port**

Interface on Intel LAN chips for remote maintenance, which allows remote maintenance even after a server failure.

### **End User License Agreement**

Agreement between the software manufacturer and the software user. The EULA is displayed during installation and the user must agree to it in order to proceed with the installation.

### **Erasable Programmable Read-Only Memory**

Memory module whose contents can be written with the aid of special devices.

### **Error Correcting Code (ECC)**

Method for detecting and correcting errors in data transmission. ECC is used, for example, in modern RAM memory modules.

### **Event**

Action or change of status to which a program can respond. In the PRIMERGY ServerView Suite: arrival of a particular message from an agent. In the definition of the event, the incoming message is specified more precisely by a character string that must appear in the message text. See also Agent.

### **Extended Capability Port**

Extended standard for the parallel interface, which allows the connection of multiple devices and a higher data rate.

### **Extensible Firmware Interface**

Central interface between the firmware, the individual components of a computer and the operating system.

### **Extensible Markup Language**

Open standard defined by the World Wide Web Consortium (W3C) for creating machine- and human-readable documents in the form of a tree structure. XML defines the rules for the structure of such documents. For a concrete application ("XML application") the details of the respective documents must be specified. This concerns in particular the specification of the structural elements and their arrangement within the document tree. XML is thus a standard for the definition of any markup languages but which are closely related in

their basic structure. A language used to define other languages is called a metalanguage. XML is a simplified subset of SGML.

## **F**

### **Fast Management Link**

Connection from LAN to BMC.

### **Field-Replaceable Unit**

A component that can be replaced in the field.

### **File Transfer Protocol**

TCP/IP protocol for file transfer between computers in a network. The files can be exchanged between computers from any manufacturers, irrespective of the operating system used. FTP is based directly on TCP and can transfer files of any kind (e. g. text, graphics, sound, video or program files). File transfer with FTP is normally unencrypted.

### **Firewall**

Network component via which an internal, private enterprise network is connected to the Internet. The job of a firewall is to allow the users of the private network unhindered access to the Internet while simultaneously protecting them from external interference. This means that the firewall must be the only route through which the private network can access the Internet. A firewall normally consists of several hardware and software components, which can be individually configured according to the security requirements and the volume of Internet services used.

### **Flash memory**

Digital memory used in areas where information has to be stored persistently, i.e. non-volatile, in the smallest possible space. In most

computers, for example, the BIOS is stored in flash memory. Other application areas include USB sticks and device firmware. With flash memory, individual bytes can be addressed, read and written, but not deleted. Deletion is only possible in blocks, normally in units of a quarter, an eighth etc. of the total storage capacity.

### **Front Panel Controller**

Controller which controls the display and operating elements on the front of the server.

### **Front Side Bus**

Data line connecting the processor with the other internal components of the computer (RAM, chipset, PCI slots, etc.).

## **G**

### **Gateway**

A device that connects networks which use different communication protocols.

### **Global Array Manager**

A collection of RAID management tools from the company LSI/Mylex for configuring a RAID controller. With GAM you can, for example, select a RAID level and thus define the logical organization of the hard disks.

### **Global-error indicator**

An LED that lights up when critical events occur in the server system. Further details of the event can be looked up in the BIOS setup or in the operating-system event log and the System Event Log via ServerView.

### **Globally Unique Identifier**

Used by the operating system to identify components. A GUID is a 128-bit integer value (16 bytes) that is unique worldwide. It is comprised of a calculation which includes the current time and the unique MAC address of the network card.

### **Graphical User Interface**

Allows the user to control programs via graphical representations of the commands.

## **H**

### **Hard disk drive**

Drive with a magnetic storage medium (hard disk) for free storage of digital data.

### **Hard disk drive module**

An HDD module consists of a hard disk drive and carrier.

### **Hardware inventory**

In system management, hardware information about every device in a system, including the model, OS version, processor type, free RAM, RAM used, battery type and residual voltage.

### **Hot-plug**

Property of a component meaning that it can be replaced during operation.

### **Hot-spare memory technology**

Technology which enables the contents of a memory bank containing a potentially faulty memory module to be copied online to an additionally configured memory bank which is not used in normal

operation (hot-spare memory bank). This additional memory bank is only activated in the case of a hot spare.

### **Hot-swap**

Usually used synonymously with hot-plug. Sometimes, however, the following small distinction is made: With hot-plug the interfaces must be deactivated (automatically or manually) during the exchange, but with hot-swap this is not the case. See also Hot-plug.

### **HyperText Markup Language**

Standardized markup language and subset of the SGML standard (Standard Generalized Markup Language). HTML documents can be exchanged between any computer systems via the standardized communication protocol HTTP.

### **HyperText Transfer Protocol**

TCP/IP protocol of the application layer. HTTP is used to transport HTML files over the Internet and forms the backbone of the World Wide Web. Messages are exchanged between HTTP servers (Web servers) and HTTP clients (Web browsers) according to the client/server principle: The Web browser sends an HTTP request to the HTTP server, which then sends the desired HTML document to the client as an HTTP response.

### **Hypertext Transfer Protocol Secure**

Unlike the HTTP protocol, which transfers HTML files unencrypted, HTTPS encrypts the transferred HTML files via SSL (Secure Sockets Layer). As well as the encryption, HTTPS also guarantees the authenticity and integrity of the transferred files as well as the anonymity of the communication. See also Secure Sockets Layer.

### I

#### **ID button**

Button for activating the ID indicator.

#### **ID indicator**

Indicator (LED) which identifies a specific server.

#### **IDE storage medium**

Storage medium with an IDE interface. In connection with RemoteView: hard disk or chipDISK containing the RemoteView Test and Diagnosis System (RTDS).

#### **Image**

Copy of a reference system (e. g. a hard disk or hard-disk partition) with operating system, configuration and user data. See also Image file.

#### **Image file**

File containing an image. In PRIMERGY ServerView Suite, image files can be created, for example, with RemoteDeploy and used to clone systems. See also Image.

#### **In-band management**

A distinction is made between “in-band” management and “out-of-band” management. In-band management refers to the sum of the management options during a system status in which all installed management functions are available: The operating system of the managed PRIMERGY server and the ServerView Agents on this server are active. The hardware of the managed server works faultlessly and the entire installed management software is available. In this case the ServerView Agents communicate via the

communication channels of the standard operating system with the user interface, e. g. ServerView Operations Manager, Windows-based ServerView or BMC Manager. Furthermore, access to the managed server is also possible via LAN to the BMC or via the autonomous LAN/modem interfaces of the RSB/ RSB S2/ RSB S2 LP (3HU). See also Out-of-band management, ServerView Operations Manager and BMC Manager.

### **Installation Manager**

Component of the PRIMERGY ServerView Suite. Allows fast and convenient installation and configuration of the operating system and additional applications (e. g. the server management software).

### **Integrated Device Electronics**

Term coined by Western Digital for a special version of the ATA/ATAPI interface in which the controller is integrated in the drive (e. g. hard disk or CD-ROM drive).

### **Integrated Remote Management Controller**

Baseboard Management Controller (BMC) with a separate LAN connection and additional functionality that was previously provided by the RemoteView Service Board (RSB).

### **Intelligent Chassis Management Bus**

Internal bus for the exchange of information for platform management and controlling systems. ICMB is a subgroup of the IPMI specification.

### **Intelligent Platform Management Bus**

I2C-based (write-only) bus which establishes a connection between different modules in a cabinet. The IPMB can also be used as a standardized interface for remote-management modules.

### **Intelligent Platform Management Interface**

General interface for server-management hardware, via which the operating characteristics such as temperature, voltage or fan status can be monitored. See also Intelligent Platform Management Bus and Intelligent Chassis Management Bus.

### **Inter-Integrated Circuit**

Serial data bus for connecting integrated circuits.

### **Internet Assigned Numbers Authority**

Organization that controls the assignment of IP addresses, top-level domains and IP protocol numbers. Among other things, it assigns certain services to ports of the TCP/IP protocol, e. g. port 80 for the HTTP protocol.

### **Internet Information Server**

A group of Internet servers (including a Web or HTTP server and an FTP server) with additional capabilities for Microsoft server operating systems.

### **Internet Protocol**

Central protocol of the TCP/IP protocol family which, as a protocol of the network layer, defines the format of the transmitted data packets (datagrams) as well as the addressing schema. The Internet Protocol thus enables communication between different hosts and nodes in a heterogeneous network. The IP protocol exists in the variants IPv4 and IPv6: IPv4 supports 32-bit addressing. IPv6 supports 128-bit addressing as well as additional security mechanisms. See also IP address.

**Internet Protocol address**

32-bit address (IPv4) or 128-bit address (IPv6) which uniquely identifies an access point in the Internet.

**Internet Small Computer System Interface over IP**

Storage-over-IP procedure for storage networks. With this procedure, SCSI data is packed into TCP/IP packets and transported over IP networks. iSCSI is used to enable access to the storage network via a virtual end-to-end connection without separate storage facilities having to be set up.

**Interrupt request**

Signal from a peripheral device to the CPU reporting the need for computing power, whereupon the CPU interrupts its current tasks and processes the request from the peripheral device.

**Inventory Manager**

Component of the Asset Management of the PRIMERGY ServerView Suite. Exports data from ServerView (ServerView Operations Manager and Windows-based ServerView). This data can be stored in external media (e. g. file, database).

**Inventory View**

Component of the Asset Management of the PRIMERGY ServerView Suite. Allows you to identify and display the hardware-related and system-related software configuration of a PRIMERGY server.

**J****Java**

Object-oriented, platform-independent programming language that can perform memory management. Because Java was developed,

among other things, for use in the World Wide Web, security aspects were considered especially important. See also Java applet and Java Virtual Machine.

### **Java applet**

A Java class that can be started from an application that is already running (e. g. a Web browser). Java applets can be used to implement interactivity in websites. See also Java, Java Virtual Machine and Console redirection.

### **Java Virtual Machine**

Runtime environment and virtual system for the execution of Java programs. The core of the JVM is formed by the Java Interpreter, which translates the individual instructions of the so-called Java byte codes into machine code and then immediately executes them. See also Java and Java applet.

### **Job**

A specially defined request to carry out a task in a specific context, e.g. updating a server with components based on a specific inventory. Once executed, a job cannot be applied to another context. Jobs retain their status to help tracking. Typical actions on a job include "Create", "View" and "Delete".

## **K**

### **Keyboard Controller Style**

Interface defined in the IPMI standard for communication between a BMC and the system management software.

## L

### **LAN on Motherboard**

A motherboard with integrated circuits for the network functionality. This renders an additional network card superfluous.

### **Lightweight Directory Access Protocol**

Directory-service protocol which specifies a directory service that is executed via TCP/IP. An LDAP directory arranges entries in a hierarchical tree structure which reflects political, geographical and/or organizational boundaries.

### **Local Area Network**

Local computer network of multiple computers which are interlinked and communicate via protocols.

### **Local installation**

Installation and configuration of a computer in its immediate vicinity (unlike remote installation). A local installation can be performed with or without Installation Manager. See also Installation Manager and Remote installation.

### **LocalView**

Under the "LocalView" concept, the PRIMERGY ServerView Suite provides a series of functions which signal important information about the operating status of a system directly on that system, e. g. via display elements in the control panel (e. g. the global-error display), LEDs on the system board (see PRIMERGY diagnostic LED) or via the display of the LocalView module. See also Global-error indicator, Diagnostic LED and LocalView module.

### **LocalView module**

Compact module with an LCD showing important system messages directly on the PRIMERGY server. These system messages indicate the server status and warn of hardware faults. See also Liquid Crystal Display.

### **Log file**

File in which all or certain actions or events are logged automatically. Within the server management of the PRIMERGY ServerView Suite, the following log files play a key role: the event log of the operating system and the System Event Log (SEL) of the server. The event log of the operating system of a PRIMERGY server contains all events which are sent, for example, from the operating system or from drivers. These SEL entries can be transferred into the event log by the ServerView Agent. Event-log entries can be read out, for example, from other enterprise management systems such as Microsoft SMS or Tivoli and stored on a local management station. The SEL of a server contains all events concerning that server. These events can be evaluated with RemoteView, for example.

### **Logical Block Addressing**

Method of specifying the location of blocks of data on hard disk drives with the aid of 24-bit addresses.

### **Logical Unit Number**

Used to identify SCSI devices.

### **Low-Voltage Differential**

Special transmission method for the SCSI bus.

## M

### **Managed Object Format**

Standard format for textual definition of classes in CIM. MOF is based on the Interface Definition Language (IDL).

### **Managed Object Format file**

File created in MOF format.

### **Managed server**

A server, running the components of the server management software (e.g. ServerView Agents, ServerView Update Agents), which can be monitored, managed and updated.

### **Management Information Base**

A database of network management information about the configuration and status of nodes on a TCP/IP-based internetwork. MIB is used by the Common Management Information Protocol (CMIP) and the Simple Network Management Protocol (SNMP).

### **Management Information Base browser**

In server management with SNMP, this software allows the administrator to do the following: Display the hierarchy of the MIB objects or individual MIB branches as a tree structure. Issue SNMP requests to query or set values in MIB objects. Display traps.

### **Management server**

Central server (Intel-based computer with Windows or Linux operating system) on which the ServerView management software of the PRIMERGY ServerView Suite is installed (e. g. ServerView Operations Manager, Windows-based ServerView, Event Management).

### **Management station**

A Windows computer or a device with Internet connection and current Web browser, via which the server management software of the PRIMERGY ServerView Suite can be started.

### **Messaging Application Programming Interface**

Standardized interface for messaging systems. MAPI is contained, for example, in Microsoft Exchange.

### **MIB module**

A group of managed objects. See also MIB-I/II.

### **MIB objects**

Term encompassing object types and attributes in a MIB-I/II. See also MIB-I/II.

### **MIB-I/II**

Standard MIBs. These are standardized in the Request for Comments 1156 (MIB-I) and 1213 (MIB-II). MIB-II is an extension of MIB-I. The use of MIB-II is mandatory in the Internet. MIB-II offers an adequate data model for the management of devices. See also Request for Comments and MIB module.

### **Microsoft Operations Manager**

Comprehensive management solution for the management and performance-monitoring of Windows-based servers and applications. ServerView can be integrated in MOM via an integration module. The ServerView events are stored in the MOM database and displayed in the MOM management station. For detailed analysis, both ServerView Operations Manager and Windows-based ServerView can be called up from the MOM interface.

**Microsoft Windows Installer**

Microsoft® Windows® Installer is an installation and configuration service for application programs. It is a Windows 2000 component which simplifies the installation of application programs. Windows Installer organizes the installation and uninstallation of programs. During the installation process it applies a set of centrally defined rules. This set of rules defines the installation and configuration of the installed program. Windows Installer can also be used to modify, repair and uninstall an already installed program. The Windows Installer technology comprises the Windows Installer service for Windows operating systems and .msi packages. The .msi file extension identifies an installation package generated by Microsoft Windows Installer. Contains information on the program setup and installation. The .mst file extension identifies a Microsoft Windows Installer transform file. A transform file effects changes to an existing .msi package.

**Mirrored array**

See RAID 1.

**Modem**

MOdulator/DEModulator device for data transmission over telephone lines.

**Multicast**

Type of transmission from one point to a group (also called a multipoint connection). The advantage is that messages can be sent to multiple subscribers simultaneously or to a closed subscriber group. The packets to be delivered are copied to each new distributor (switch, router) and then forwarded. The server management of the PRIMERGY ServerView Suite uses the multicast method if, during cloning, the image file created on the reference system is to be dis-

tributed to multiple servers simultaneously. The individual servers are allocated an IP multicast address for this.

### **Multi-homed server**

A server with two or more network connections (i.e. a unique network address assigned to each of two or more network interface cards) to improve performance on the network. See also Network Interface Card.

### **MultiPath**

Component of Duplex Data Manager. MultiPath provides redundant data paths to the storage subsystem.

## **N**

### **Netmask**

Filter in a LAN which filters the network-internal part out of IP addresses so that only the part of the address that identifies the host within the relevant LAN remains. See also Local Area Network and Internet Protocol address.

### **Network Address Translation**

NAT assigns private IP addresses to public IP addresses in a LAN. Multiple private IP addresses can be assigned to an incoming public IP address. This means that several computers can share a single public IP address in a connection via remote data transmission, cable or DSL. NAT can also limit the access of hosts on the public network to resources on a private network.

### **Network Interface Card**

Also called a network adapter. Hardware component that is installed in a computer to enable it to communicate with a network.

**Network node**

In telecommunications, a general term for an interconnect point between more than two transmission paths of a message network. Depending on the type of message network, a node could be, for example, a telephone exchange, a multiplexer, a concentrator or a router.

**NMI button**

Button on the control panel of a server for generating an NMI which triggers a hardware reset. Depending on the operating system, this can cause a system restart. The NMI button can only be activated with a pointed object. As there is a risk that data may be lost, the NMI button should only be used by customer support. See also Non Maskable Interrupt.

**Non Maskable Interrupt**

Highest-priority interrupt, whose signal is triggered by a hardware module or peripheral device, usually by hardware errors. It is conveyed to the CPU via a special interrupt input, whereupon the CPU immediately executes a defined interrupt routine.

**O****Object Identifier**

Notation specifying the position of an object in a MIB tree. For example, 1.3.6.1.4.1.231.1.3.1 (iso.org.dod-.internet.private.enterprise.sni.1.3.1) could indicate an RM400 system (SINIX V5.43). There are also MIB names (symbolic names) for the OID (e. g. cisco for a Cisco router).

**Offline update**

In the PRIMERGY ServerView Suite, the updating of components from within a DOS environment. This method is used for

components if the update can only be performed from a DOS environment either because the system requires it or because the manufacturer does not offer a tool for online updates. Update Manager here only controls the boot process to DOS and back to the operating system. The offline update can be performed via the service partition of the PRIMERGY server or via a PXE server. See also Online update.

### **Online Update**

Update of components when managed server is online.

### **Out-of-band management**

Refers to the sum of the management options during a system status in which not all installed management functions are still available: The operating system of the managed server and the ServerView Agents on this server are no longer active. Status and inventory data of the server can no longer be accessed via ServerView. If the hardware of the managed server is still working, full control of the managed server is still possible remotely, even in this system status, via RemoteView. The tools of the RemoteView Test and Diagnosis System are available and it is also possible to access the managed server via LAN to the BMC or via the autonomous LAN/modem interfaces of the RSB/ RSB S2/ RSB S2 LP. Even if no CPU is still working in the managed server and therefore a connection to the server can no longer be established via system-dependent functions, remote management of the server is still possible on various levels. See also In-band management and RemoteView Test and Diagnosis System.

## P

### Pager

A miniaturized radio receiver with a fixed receiving frequency. The pager receives a radio signal from the provider of the pager service. Messages are, for example, shown on the display as a number or as text, or are relayed as an acoustic signal or a voice message.

### Performance Manager

ServerView component of the PRIMERGY ServerView Suite. Enables long-term monitoring of the utilization of specific server components and helps with early detection of resource bottlenecks and compliance with service levels. The report functions of Performance Manager offer a multitude of different options for graphical representation. The threshold management informs the user immediately if defined thresholds are reached or exceeded.

### Peripheral Component Interconnect bus

Bus system which enables the connection of up to ten PCI-compatible expansion cards.

### Ping

Computer program for checking the IP-level connectivity from one IP address to another.

### Platform Event Filtering

Offers a mechanism for configuring the BMC to react to event messages with selected actions. These actions can be operations such as system power-off, reset or the triggering of an alarm.

### **Platform Event Trap**

Special format of an SNMP trap that is used for alerting within server management. Platform event traps are generated by a system with ASF (Alert Standard Format) or an IPMI BMC.

### **Point-to-Point Protocol**

A data-link protocol for dial-up telephone connections, such as between a computer and the Internet.

### **Policy**

A set of rules according to which, for example, the event handling during ServerView integration in HP OpenView Operations occurs (e. g. forwarding alarm reports).

### **Policy group**

A combination of several policies (sets of rules). See also Policy.

### **Poll cycle**

Parameter which specifies the cycle in which information is retrieved. See also Polling.

### **Polling**

Cyclical request for information. Polling can be configured by the operator. See also Poll cycle.

### **Power Supply Unit**

Device or module for supplying electrical energy for devices or modules which require voltages and currents other than from the mains supply.

### **Power-On Self-Test**

First function performed by the BIOS. During the POST, the system hardware is initialized and tested.

### **Preboot Execution Environment**

Environment that is independent of mass storage available on the client side and in particular of operating systems, which enables a boot process from the network (netboot). PXE is an Intel specification that defines mechanisms and protocols that allow PXE-enabled devices to use their network interface cards (NICs) to find bootstrap programs located on network servers. The PXE environment is loaded from the BIOS on the NIC. Preboot Services uses PXE to discover if there is Preboot Services work specified for a device and to provide the device with the files necessary to execute the assigned work.

### **Prefailure Detection and Analysis**

Technology which monitors certain server functions, thus enabling early detection of potential faults in components (e. g. fans).

### **PRIMECENTER Rack**

Installation cabinet with additional cable-management facility for system components of the PRIMERGY, RM and BS2000 server series.

### **PRIMERGY Server**

The following servers are PRIMERGY servers: - Economy server - Tower server - Rack server - Blade server and BladeFrame

### **PRIMERGY ServerView Suite**

Server management concept from Fujitsu Technology Solutions for PRIMERGY industry-standard servers (Windows, Linux (Red Hat,

SuSE), VMware) with automatic installation, central administration, monitoring of assets and status, remote management and adaptive event management as well as integration with 3rd-party systems (e. g. Tivoli, SMS, CA Unicenter).

### **Private key**

In asymmetric cryptographic systems, the private key must only be known to the communication partner who is allowed to decrypt the message that was encrypted with a public key. See also Public key.

### **Promise Array Management**

Software from the company Promise for local set-up of an SATA RAID controller. With this utility you can select a RAID level and thus define the logical organization of the hard disks.

### **Property**

Part of a class definition in CIM. Refers to an attribute in a class.

### **Public key**

Used in public-key encryption. In asymmetric cryptographic systems, the public key is used by the communication partner to encrypt a message, which the recipient can then decrypt with their private key. See also Private key.

## **R**

### **Rack**

In a rack there are typically several components installed, which are thus combined to form one logistical unit. Racks are available in various models, which can differ both in width and in height.

### **RAID 0**

Redundant Array of Independent Disks, level 0, also known as “non-redundant striped array”. The data is broken down into blocks called stripes and distributed over several hard disk drives. This increases the data throughput and thus the access speed but without creating any redundant information. Therefore, data can be lost if a hard disk fails.

### **RAID 0+1**

Redundant Array of Independent Disks, level 0+1: a combination of mirroring (RAID 1) and striping (RAID 0). Here a RAID 1 array is formed from several RAID 0 arrays. This requires at least three hard disks. Through striping, RAID 0+1 offers fast access times, and in combination with mirroring it offers additional data security, although this is lower than with level 10.

### **RAID 1**

Redundant Array of Independent Disks, level 1, also known as “drive duplexing” or “mirrored array”. The data is duplicated on an additional hard disk drive. If a drive fails, the mirrored drive takes over all requests until a replacement drive is installed. While other fault-tolerant RAID configurations require at least three drives, the minimum number for RAID 1 is just two drives. RAID 1 offers full redundancy of the stored data, but the capacity of the array does not exceed that of the smallest hard disk involved.

### **RAID 10**

Redundant Array of Independent Disks, level 10: a combination of striping (RAID 0) and mirroring (RAID 1). Here a RAID 0 array is formed from at least two RAID 1 arrays, so at least four hard disks are required for implementation. Through striping and the omission of parity calculations, RAID 10 offers fast access times, and in combination with mirroring it offers additional data security.

### **RAID 5**

Redundant Array of Independent Disks, level 5, also known as “striped array with rotating parity”. The user data and its parity information is distributed over all drives of the disk array. This increases the speed with distributed read accesses but noticeably reduces it with write accesses because of the necessary calculation of the parity, and is therefore not recommended for use in write-intensive environments. The parity management - like the mirroring in RAID 0 and RAID 10 - ensures that the data can be restored, but requires much less disk capacity for this. Because the parity information is distributed over different drives, bottlenecks are avoided because of a special parity hard disk. A RAID 5 configuration requires at least three drives, offers redundancy despite relatively low costs, and is therefore the most popular RAID variant. Data integrity is only guaranteed if no more than one hard disk fails!

### **RAID 50**

Redundant Array of Independent Disks, level 50: a combination of RAID 0 with a striped version of RAID 5. Here a RAID 0 array is formed from at least two striped RAID 5 arrays, so at least six hard disks are required for implementation. A RAID 50 configuration offers both very high read/write performance, because the processing work can be distributed over two XOR units, and high data security. RAID 50 is therefore used in databases where redundancy and write performance are important.

### **RAID 60**

Redundant Array of Independent Disks, level 60: a combination of RAID 0 with the distributed double parity of RAID 6. That is, a RAID 0 array striped across RAID six elements. It requires at least eight disks. As it is based on RAID 6, two disks from each of the RAID 6 sets could fail without loss of data. Also failures while a single disk is rebuilding in one RAID 6 set will not lead to data loss. RAID 60

has improved fault tolerance, any two drives can fail without data loss and up to four total as long as it is only two from each RAID 6 sub-array.

### **RAID controller**

Hard disk controller with integrated management functions for configuring, controlling and managing hard disks in disk arrays (RAIDs). See also Redundant Array of Independent Disks.

### **RAID level**

Specifies the interaction of the hard disks and thus the performance features of a RAID system. The most common RAID levels are RAID 0, RAID 1, RAID 5 and combinations of these, such as RAID 0+1, RAID 10 and RAID 50. See also RAID, RAID 0, RAID 1, RAID 0+1, RAID 5, RAID 10 and RAID 50.

### **Read-Only Memory**

Digital read-only memory in which data is stored permanently and unchangeably and thus can only be accessed for reading. In a PC or server, critical programs such as the BIOS, for example, are stored in the ROM.

### **Redundant Array of Independent Disks**

Combination of two or more independent hard disks to form a logical unit (disk array) controlled by a RAID controller. A RAID system can store data so as to avoid data loss even if hard disks fail. It thus ensures that the operational readiness of the server is maintained. Often, RAID technology is also used to optimize access times. There are different RAID levels for different purposes. See also RAID controller and RAID level.

### **Reference system**

In a network, a server on which the first installation (reference installation) of the operating system and the applications is performed. A complete image of this reference installation is then stored as an image file on a deployment server in the network. With the help of this image file, the administrator can then install additional servers of the same type in the network (cloning). See also Image, Image file and Deployment server.

### **Remote deployment**

Server installation based on an image generated by a reference installation or on Installation Manager configuration files. See also Image and Installation Manager.

### **Remote installation**

Installation mode in Installation Manager comprising a preparation phase and a replication phase. Unlike the other installation modes, the subsequent replication is executed remotely on the target system via the PXE protocol. When the installation is complete, an image can be created. This image is used to duplicate multiple servers with the help of Remote-Deploy. See also Installation Manager, Image and RemoteDeploy.

### **Remote IPMI Manager**

In the PRIMERGY ServerView Suite, a remote-management interface which is called up in the RemoteView/LAN front-end when an IPMI-based BMC is accessed. The Remote IPMI Manager provides access to the power management for the managed server and allows secure text-only console redirection to be set up. See also Intelligent Platform Management Interface, RemoteView/LAN front-end, Baseboard Management Controller and Console redirection.

**Remote Management Controller**

Additional separate processor on the mainboard of a computer, whose functionality approximates that of RemoteView. See also RemoteView Service Board.

**Remote Manager**

RemoteView component in the PRIMERGY ServerView Suite. Telnet interface for remote management of an RSB, which is called up in the RemoteView/LAN front-end or the RemoteView/Web front-end. The Remote Manager user interface enables access to the power management and System Event Log of the managed server. See also RemoteView/LAN front-end, RemoteView/Web front-end, RemoteView and System Event Log.

**Remote storage**

RemoteView component in the PRIMERGY ServerView Suite. Provides the managed server with a "virtual" drive or image file. Physically, such a drive can be located at another point in the network, e. g. on an MSA (Management Server Application) server or on a remote workstation. Various storage media can be used as remote storage: hard disk, image file, IDE storage medium or CD-ROM. See also RemoteView, Image file, IDE storage medium and CD-ROM.

**RemoteDeploy**

RemoteDeploy is a chargeable component of the PRIMERGY ServerView Suite. RemoteDeploy enables the selective commissioning as well as the duplication or installation of individual servers. The remote installation or mass cloning of servers can be automated and scheduled from a central management station.

### **RemoteView**

Component of the PRIMERGY ServerView Suite. RemoteView® allows remote monitoring and maintenance of PRIMERGY servers as well as rapid restoration of their operational readiness when errors occur. RemoteView allows you to: Recognize system errors. Prepare for or, if applicable, initiate error recovery. Track down potential sources of errors. Configure the system. RemoteView can be operated both locally, i.e. directly on the server, and remotely, i.e. via LAN, Web or modem from a remote workstation. With the RemoteView Service Board (RSB) or a RemoteView management blade (in a blade server), remote control, including switching the system on and off, is possible in all operating states. See also RemoteView Test and Diagnosis System.

### **RemoteView console**

Window in the RemoteView/LAN front-end which is assigned to a server. Once a connection has been established, messages from the POST phase as well as the RemoteView Test and Diagnosis System (RTDS) are displayed in the RemoteView console. See also RemoteView/LAN front-end, POST and RemoteView Test and Diagnosis System.

### **RemoteView management blade**

Each PRIMERGY blade server has two RemoteView management blades integrated. These allow remote management (system monitoring) during the boot phase and while the system is running. See also Blade server.

### **RemoteView Service Board**

PCI board which uses its own operating system and power supply and runs completely independently of the managed server. Each RSB has its own Web server, its own SNMP agents, its own user administration and its own Event Manager for forwarding

messages. Thus each RSB in conjunction with the RTDS allows remote system configuration and remote restart - even if the operating system fails or hardware errors occur. The RSB S2/RSB S2 LP also offers powerful graphical console redirection (AVR), remote storage functionality, "headless" operation of the managed server, and comprehensive encryption functions. See also SNMP agent, RemoteView Test and Diagnosis System, Console redirection and Remote storage.

### **RemoteView Test and Diagnosis System**

The RemoteView testing and diagnostics software kept on an IDE storage medium in the server. See also Storage Extension Management Tool, IDE storage medium and RemoteView.

### **RemoteView/LAN front-end**

RemoteView component of the PRIMERGY ServerView Suite for controlling the RemoteView functionality via a LAN connection. The RemoteView/LAN front-end is installed on the remote workstation.

### **RemoteView/modem front-end**

RemoteView component of the PRIMERGY ServerView Suite for controlling the RemoteView functionality via a modem connection. The RemoteView/modem front-end is installed on the remote workstation. See also RemoteView.

### **RemoteView/Web front-end**

RemoteView component of the PRIMERGY ServerView Suite. Java application embedded in a Web interface, via which a Telnet connection to an RSB, a RemoteView management blade (in a blade server) or a BMC can be established. The RemoteView/Web front-end is started from the ServerView Operations Manager interface. It is installed on the remote workstation. See also RSB,

RemoteView management blade, Baseboard Management Controller, RemoteView and ServerView Operations Manager.

### **Request for Comments**

Series of documents describing the Internet protocols and related standards.

### **Riser card**

Slot expansion board, which is plugged into the system board and in turn offers slots for various modules. Modules which are plugged into the riser card are arranged parallel to the system board. This means that modules can also be installed in computers with a low overall height.

### **RomPilot**

BIOS extension which is used to establish a LAN connection to the administrator. This allows the server to be accessed during the POST phase. Then, depending on the setting, the server operating system or the RemoteView Test and Diagnostic System is booted. See also Power-On Self-Test and RemoteView Test and Diagnosis System.

## **S**

### **Secure Authenticated Channel**

In connection with symmetrical encryption procedures, a separate channel used exclusively to transfer keys between two mutually authenticated communication partners. The SAC exists independently of the channel on which the user data is transmitted. It must be guaranteed that the SAC is tap-proof and/or known only to the communication partners.

**Secure Sockets Layer**

Security protocol for secure data traffic over the Internet. Suitable for protecting any TCP/IP protocol above the transport layer (TCP). SSL allows the mutual authentication of two communicating applications and also guarantees the confidentiality and integrity of the application data exchanged. SSL thus prevents falsification of the sender address (message forgery, IP spoofing), eavesdropping and tampering.

**Self Monitoring and Reporting Technology**

Function of mass storage that enables early detection of defects. The drive electronics constantly compare target and actual values and determine whether, for example, with servo tracks or read/write heads, the values are outside the tolerance ranges. If so, S.M.A.R.T. reports this to the user.

**Serial Advanced Technology Attachment**

Standard based on Advanced Technology Attachment for a serial interface between the computer and mass-storage devices. SATA allows especially high transmission speeds. See also Integrated Device Electronics and Advanced Technology Attachment.

**Serial Attached SCSI**

New interface standard which replaces the previously parallel SCSI bus. Serial data transfer enables new functions and application possibilities.

**Server blade**

Component of a blade server with hot-swap capability, which combines all the core components of a conventional server. See also Blade server.

### **Server blade.**

Component of a blade server with hot-swap capability, which combines all the core components of a conventional server. See also Blade server.

### **Server Configuration Utility**

Utility for configuring all server components for subsequent installation of the operating system. Configuration parameters include the serial number of the server, the server model (PC type), the settings for pager operation and VT 100 / VT100+ operation, the error and event log, the operating-hours counter and the switch-on count. SCU also allows you to set or change the relevant BIOS settings for server management. The SCU is contained on the Installation Manager CD. See also Pager, VT100 / VT100+, Event and Installation Manager.

### **ServerView Agent**

Subprogram which is part of the central ServerView Suite and is installed on managed servers. The ServerView Agent allows a managed server to be monitored and managed remotely

### **ServerView integration**

ServerView can be easily integrated into other enterprise management systems through the use of standardized protocols and interfaces. Integration packages are available for integrating ServerView into, for example, CA Unicenter, IBM Tivoli TME 10, IBM NetView and HP OpenView Network Node Manager, and Microsoft SMS.

### **ServerView Operations Manager**

Server management software for the central administration of PRIMERGY servers. The data of the managed servers can be accessed

via intranet and Internet. It can be viewed from any computer that has intranet or Internet access and a current standard Web browser.

### **Short Message Service**

Function of mobile communication services which enables short text messages to be sent to mobile phones. For example, the ServerView software uses this functionality to send error messages to the operator.

### **Simple Mail Transfer Protocol**

A TCP/IP protocol of the application layer for sending e-mail.

### **Simple Network Management Protocol**

Protocol used for server management. It is the standard protocol for management in TCP/IP networks. The name SNMP not only stands for the protocol itself but also for the entire management system based on SNMP. The term SNMP also refers to a special variant of a client/server architecture with the SNMP Manager as the client and the SNMP agents as servers. See also SNMP Manager and SNMP agent.

### **Small Computer System Interface**

Industry standard for a hardware interface which controls the communication between a computer and various peripherals (e. g. CD-ROM drives, hard disks, scanners or printers). SCSI was originally implemented as an 8-bit parallel I/O bus suitable for connecting up to 7 peripherals. Nowadays there are other SCSI variants, such as Wide SCSI-2 or SCSI-3, which, because of their greater bandwidth (16-bit and higher), achieve higher transmission rates and can accommodate up to 15 peripherals and more.

### **Small Computer System Interface Accessed Fault-Tolerance Enclosure**

Industry standard for the monitoring of SCSI devices.

### **Small Computer System Interface controller**

Enables the connection of peripherals. While IDE only allows two devices to be connected per channel, a SCSI controller can control up to 15 devices. See also Integrated Device Electronics.

### **Snapshot image**

Backup image of a system (hard disk) which can be used to restore the server following a crash. See also Image.

### **SNMP agent**

In connection with server management, a small program that runs on a managed component and communicates with the SNMP Manager via the MIB. On request from the SNMP Manager, the SNMP agent provides information on certain events or system states of the managed components or puts values in the MIB. In defined situations the SNMP agent sends traps (asynchronous messages) to the SNMP Manager without waiting for a request. See also Alarm, Event, SNMP Manager and Trap.

### **SNMP Manager**

In connection with server management, a program that runs on a central management station. The SNMP Manager allows servers to be monitored via SNMP by sending requests to the SNMP agents, then receiving the data ascertained by them and displaying it in graphical form. See also management station and SNMP agent.

### **Storage Area Network**

Mass-storage architecture based on Fibre Channel networks in which storage resources are uncoupled from the servers. From the point of view of the server, the storage resources are virtualized. Any server can access any resource. SANs have advantages above all for the backup, administration and security of data.

### **Storage Extension Management Tool**

Software component of the RemoteView Test and Diagnosis System which offers information on managed storage extension units. Can also be used to reboot a storage extension unit or install new firmware on it.

### **Storage Management Interface Specifications**

SMIS offers a range of APIs aimed at considerably simplifying the complexity of combining storage systems from different manufacturers to form SANs. SMIS uses CIM and the WBEM standard for error detection, monitoring and management of storage devices. See also Storage Area Network and Common Information Model.

### **Storage Networking Industry Association**

Consortium for the definition of standards for SANs. See also Storage Area Network.

### **Storage subsystem**

External storage system with a large number of storage media (e. g. hard disks).

### **Switch blade**

Component of a blade server with hot-swap capability. A switch blade offers high-speed LAN access via multiple Gigabit interfaces. These LAN connections provide the I/O functionality for the server blade. See also Server blade and Blade server.

### **System Event Log**

Non-volatile storage area (approx. 3-8 KB) for recording all hardware-related, critical events of a server such as voltage fluctuations, temperature overruns, failure of fans etc., which require immediate logging for a "post mortem" analysis. The SEL also

records all events which require a fast reaction from the system, e. g. switching on/off or shutdown. See also Event.

### **System Management BIOS**

The SMBIOS specification defines a manufacturer-independent standard format, which has been extended to x86 systems compared with the BIOS interface, for displaying management information relating to the system board and the operating system. Management applications can access this information via DMI, CIM or directly.

### **System Management Interrupt**

Interrupt used for the system-management bus.

### **System Management Server**

Microsoft product for inventorying, software distribution and system management. ServerView can be integrated into SMS.

## **T**

### **Task**

A predefined request for the management system, which can be executed at preset (scheduled) times or immediately. Unlike jobs, tasks are of a general nature, i.e. they do not have a specific context. Tasks also have no status, i.e. once they are completed the history is only visible in the corresponding log file. Typical actions on a task include "Schedule", "Start" and "Stop".

### **Telnet**

TCP/IP protocol of the application layer which enables a terminal session on a non-local computer in the network from a remote workstation. In RemoteView, for example, the Remote Manager supports a Telnet interface for the remote management of an RSB,

which is called up in the RemoteView/LAN front-end or the RemoteView/Web front-end. See also RemoteView, Remote Manager, RSB, RemoteView/LAN front-end and RemoteView/Web front-end.

**Telocator Alphanumeric Protocol**

ASCII-based half-duplex protocol for transmitting requests (numeric and alphanumeric messages) to a pager service. TAP is used for SMS with D1 and E-Plus.

**Threshold**

Monitored limit value. In connection with SNMP agents, a value defined by the administrator for a server parameter monitored by the SNMP agent. Depending on the configuration, if this value is exceeded or not reached, the SNMP agent sends a message (trap) to the SNMP Manager, which displays it on the management station. In the PRIMERGY ServerView Suite, thresholds are used, for example, by the Performance Manager and the AlarmService. See also SNMP agent, Trap, SNMP Manager and management station.

**Touchpoint**

On a device or component, a specially marked point (usually green) at which you can touch the component without damaging it. Touchpoints could include points at which a device can be handled for transport purposes, or buttons which, when pushed, open locks or release ejection levers.

**Transmission Control Protocol**

TCP/IP protocol of the transport layer that creates the data packets intended for transport via IP protocol. Unlike UDP, TCP is a connection-oriented protocol that establishes a connection to the communication partner before the data packets are transmitted.

### **Transmission Control Protocol over Internet Protocol**

Protocol family that defines how systems in heterogeneous networks communicate with each other. TCP/IP was originally developed by the Advanced Research Projects Agency (ARPA) and forms the basis for communication in the Internet.

### **Trap**

Asynchronous message from an SNMP agent, which the agent automatically sends to the recipient (e. g. management station) when it detects an unusual operating state (event). See also Alarm, SNMP agent, Event and management station.

### **Trivial File Transfer Protocol**

TCP/IP protocol of the application layer for file transfer between computers in a network. Unlike FTP, TFTP does not support any functions beyond simple file transfer. In the PRIMERGY Server-View Suite, the Open Source TFTP server and client PumpKIN is used to update the firmware of, for example, an RSB.

### **Trusted domain**

Domain that has set up a bidirectional, secure relationship with a second domain. Each domain saves user entries in the other one also. Users on a computer in one of the two domains can log on to the other domain. Each domain can avail itself of both the user entries as well as the resources of the other domain. See also Domain.

## **U**

### **Unicast**

Type of connection whereby a single sender is connected to a single receiver, unlike multicast and broadcast, in which a single sender is connected to multiple receivers. See also Multicast.

**Uninterruptible Power Supply**

Hardware which, in the event of a power failure, provides the server or system with power until a controlled shutdown (exiting all applications) can be performed. This is necessary to avoid data loss. Another job of a UPS is to filter voltage peaks.

**Universal Computer Protocol**

Protocol for transmission of requests to a pager service. UCP is used, for example, for SMS with D2.

**Universal Unique Identifier**

Numerical 128-bit identifier which excludes the possibility of two components having the same ID. The UUID is always unique worldwide.

**Update**

In the PRIMERGY ServerView Suite, the updating of server components with Update Manager controlled by the active operating system.

**Update Agent**

Subprogram which is part of the ServerView Update Management and is installed on managed servers. The Update Agent allows the components of a managed server to be updated remotely.

**Update Management**

Maintenance process which includes the analysis, download and installation of update files.

**Update Manager**

Component of the Update Management of the PRIMERGY ServerView Suite. Enables updating of BIOS, firmware, ServerView

Agents, ServerView Update Agents and Add-on products on PRIMERGY servers.

### **Update process**

The update process refers to the updating of a component and consists of up to three phases: 1. Transfer phase: The updates are transferred from the management server to the PRIMERGY servers. 2. Update phase: The components on the PRIMERGY servers are updated. 3. Boot phase: Some components require a reboot to activate the update.

### **Update repository**

Contains the relevant update data for hardware and software components to update the PRIMERGY servers. A typical application for an update repository is Update Management.

### **User Datagram Protocol**

TCP/IP protocol of the transport layer which creates the data packets (datagrams) intended for transport via the IP protocol. Unlike TCP, UDP is a connectionless protocol, which does not establish a connection to the communication partner before transmission of the data packets.

## **V**

### **Virtual LAN**

Logical network of devices (computers, printers, etc.) which can physically belong to different network segments but are configured in such a way that they can communicate with each other directly.

### **VMware ESX Server**

Allows the use of several virtual servers with different operating systems on a single computer.

**VT100 / VT100+**

Virtual Terminal100 / 100+: terminal type from the company DEC (Digital Equipment Corporation). For VT100 there is an established terminal emulation which allows you to access applications of a server from a PC under any operating system.

**W****Wake On LAN**

Technology developed by IBM and the Intel Advanced Manageability Alliance which allows the system board to be switched on and off via the network card. The use of Wake On LAN requires that the system board, operating system and network card all support the ACPI standard. In addition, the network card must be supplied with power via the standby component of the power supply unit.

**Web-Based Enterprise Management**

Management architecture specified by the DMTF for Web-oriented system management. WBEM uses CIM to logically describe the objects to be managed, XML for coding the information and HTTP for data transfer.

**Wide Area Network**

Network in which the participating computers are physically a long way away from each other and are accessed, for example, via a modem connection or the Internet.

**Windows Management Instrumentation**

Microsoft implementation of the Web-Based Enterprise Management architecture. WMI allows access to information on server management in an enterprise-wide network. See also Managed Object Format and Web-Based Enterprise Management.

### Z

#### **Zero-Channel RAID (ZCR) controller**

RAID controller (PCI expansion module) which can be installed in the server in addition to the existing onboard RAID controller on the system board to extend the RAID functionality of the onboard RAID controller. This requires a specially integrated logic on the system board. As well as RAID levels 0, 1 and 10, the ZCR controller offers the option of configuring a RAID 5 or RAID 50. See also RAID controller, Redundant Array of Independent Disks and RAID level.