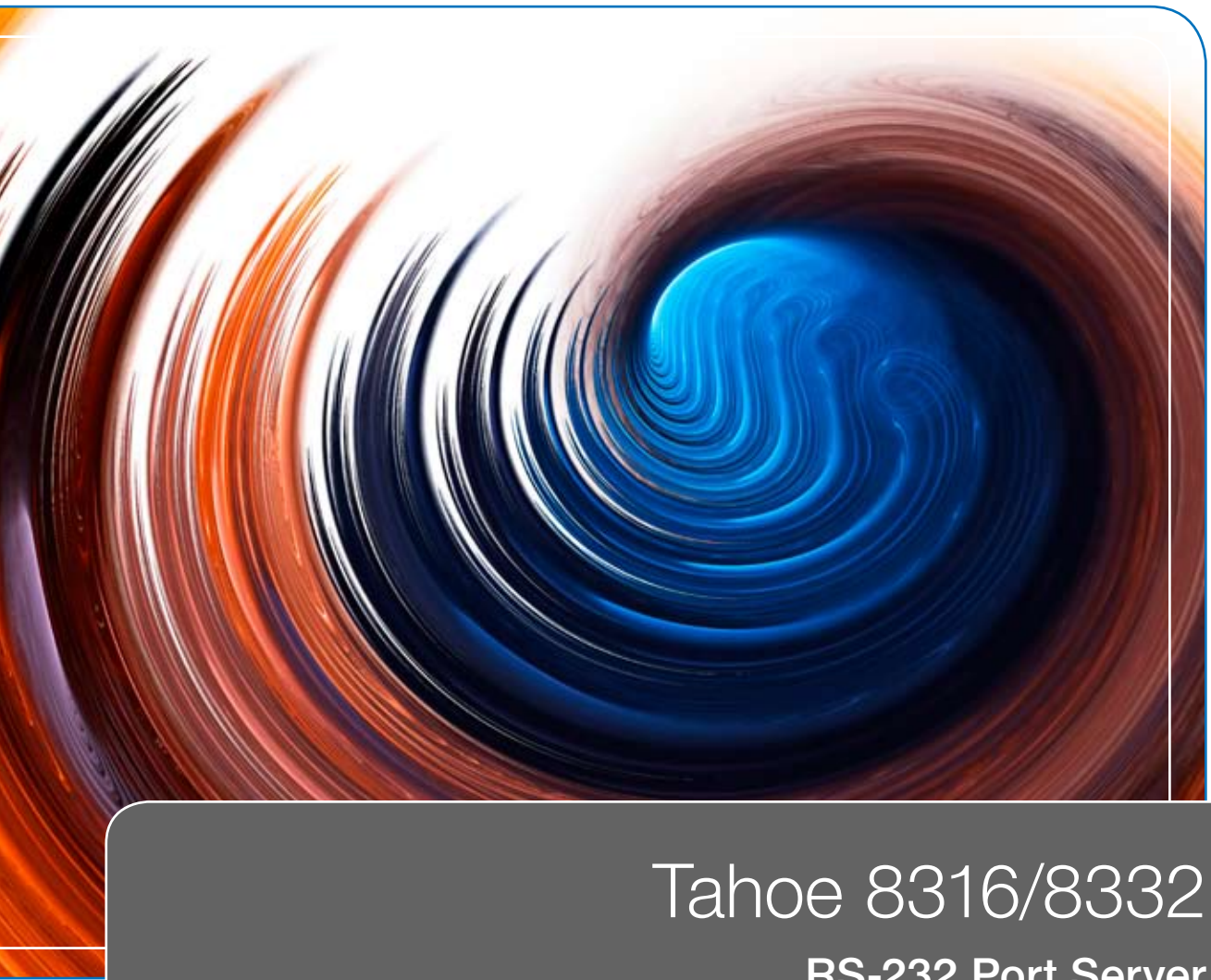
TAHOE®



Tahoe 8316/8332

RS-232 Port Server

User Manual

TAHOE®

Tahoe 8316/8332

RS-232 Port Server

User Manual

Tahoe RS-232 Port Server User Manual
Firmware version 1.4.1
Published August 2009

Contents

Preface

About this Manual

This manual contains following chapters:

Chapter 1, Introduction	An overview of the device and a short description of its features
Chapter 2, Interfaces and Cables	Description of device interfaces and wiring
Chapter 3, Device configuration	List of commands used to configure the device using the serial console or telnet connection
Appendix A, Short description of RS-232	Additional useful information – RS-232 in brief
Appendix B, Technical Specification	Parameters of the device
Appendix C, Safety Information	Important notices regarding safety of use
Appendix D, Declaration of Conformity	Information about compliance with European standards

Document Conventions

This manual uses following conventions:

boldface font	Commands and keywords
< >	Required arguments
[ ]	Optional arguments
{ a | b | c }	Alternative arguments
[a | b | c]	Alternative optional arguments
`typewriter font`	Information displayed during a serial or remote connection
`boldface typewriter font`	Information to be entered during a management session
LCD font.	Information displayed on the LCD
Note	Notes contain helpful suggestions that may be worth remembering
Caution	This symbol means a situation that requires you to be careful. Otherwise equipment damage or loss of data may occur.
Warning	This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry, and be familiar with standard practices for preventing accidents.

Introduction

The Tahoe 8316/8332 is a serial port server that allows access to serial devices via LAN or the Internet. Depending on the device model it provides up to 32 serial ports with several modes of transmission, and baud rates up to 300 kb/s per port. Connection to the port server can be made via telnet or ssh protocol. Thanks to that RS-232 range limit can be overcome and serial devices can be accessed securely from anywhere.

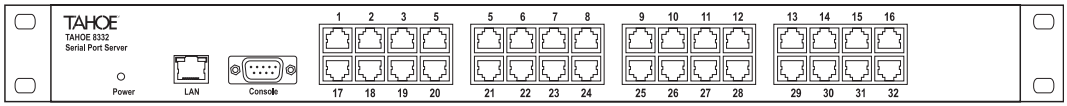
The idea behind the Tahoe 8316/8332 was to provide convenient access to manageable network equipment. Numerous network devices have a serial management console that provides access to them in any circumstances, even in the case of LAN interface misconfiguration. Having the Tahoe 8316/8332 connected to all network equipment in a server room the network administrator can recover unresponsive devices remotely.

Although the main field of use is network equipment management, the Tahoe 8316/8332 may be used to provide additional RS-232 ports in a PC. Compared to standard PC serial ports the Tahoe 8316/8332 offers two additional features:

- virtual connections between two Tahoe 8316/8332 ports – allows making interconnection between two serial devices remotely, without any changes in cable structure
- reporting of transmission errors (frame, parity, etc.) using syslog protocol

Interfaces and cables

The figure shows the front panel of the device:

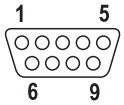


LAN

The Fast Ethernet interface is used to connect the port server to the Local Area Network (LAN). It may work at speeds of 10 Mbps (10Base-T) or 100 Mbps (100Base-Tx), in full-duplex or half-duplex mode. The mode of transmission is selected automatically, although a specific setting can be forced.

A feature called Auto MDI/MDIX automatically detects whether it is connected to a switch or to a DTE device like a PC or a router, so there's no need to use a crossed-over cable.

Management Console



The RS-232 serial console is used for modem management. It has a DB9/M connector and works as a DTE, i.e. a null-modem cable should be used to connect it to a PC. Three lines (in bold in the table below) are sufficient. Terminal settings are 9600 bps, 8 data bits, 1 stop bit, no parity, no handshaking.

Pin	Name	Description
1	DCD	carrier detect, transmission readiness signalling
2	**RXD**	data received from the PC
3	**TXD**	data sent by the modem to the PC
4	DTR	active, when the PC is switched on
5	**GND**	signal ground
6	DSR	active, when the modem is switched on
7	RTS	used by the PC to inform that is has data to send
8	CTS	used by the modem to permit data transmission
9	RI	ring indicator (signal used in telephone modems)

After connecting the console to the PC and running terminal software, the user has the same access to the port server functions as through a telnet connection.

Serial Ports

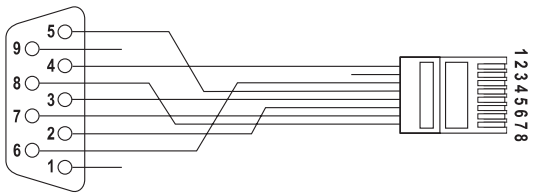
Every serial port uses an RJ-45 socket. Pin layout is described in the following table.

Pin	Name	Description
1	DSR	Data Set Ready - indicates that DCE* is powered on and is ready to receive commands or data for transmission
2	DCD	Data Carrier Detect – indicates that DCE has established connection with remote device
3	DTR	Data Terminal Ready - indicates that DTE* is ready to be connected
4	GND	Ground
5	RXD	Received data
6	TXD	Transmitted data
7	CTS	Clear To Send – acknowledge to RTS signal
8	RTS	Request To Send – indicates that DTE wants to send data

* DTE – Data Terminal Equipment – usually a PC or terminal
DCE – Data Communications Equipment – usually a modem

Cables

The figure shows DB9/F – RJ45/M interconnection in null modem (with full handshaking) configuration.



DB9/F		RJ45/M	
function	pin	pin	function
GND	5	4	GND
DTR	4	1	DSR
CTS	8	8	RTS
TXD	3	5	RXD
RTS	7	7	CTS
RXD	2	6	TXD
DSR	6	3	DTR

The presented wiring could be used in almost all kinds of serial manageable network devices. Nevertheless, some exceptions could exist, and you are strongly advised to check if the DB9/M socket pinout corresponds to the DB9/F connector shown above.

Device configuration using telnet or management console

Telnet Connection

To connect to the **Tahoe 8316/8332** the network interface on the PC has to be in the same IP subnet as the port server. By default the device's Ethernet interface is set to 10.0.0.1 address and 255.0.0.0 netmask, so the PC should have its IP address set to 10.0.0.2 and the same netmask.

If the device is already configured, a telnet connection to its IP address is possible from anywhere in the network.

After connecting, a password prompt will appear:

```
User Access Verification
Username:
Password:
```

The default user is "root" and the password is "Tahoe" (both are case sensitive). If the password entered is correct, a command prompt will appear:

```
Tahoe>
```

SSH Connection

As with the telnet connection a secure (encrypted) connection can be made using SSH protocol. The network settings should be the same, but before the connection can be made the SSH server has to be enabled using the "ssh on" command (entered during a telnet or serial console session).

Management Console

If the telnet connection is not possible (e.g. there's no telnet client available or the device's IP address is unknown), the device may be connected to the PC's serial port using a null-modem cable. After starting a terminal software (e.g. minicom under the Linux operating system, Hyperterm under Microsoft® Windows™) the user gets the same access as through the telnet connection. After pressing "Enter" the same command prompt appears:

```
Tahoe>
```

By default console access isn't password protected, but such protection may be enabled later using the "console password" command.

Command Summary

?	displays command list
arp	ARP table configuration
config	displays current configuration
console	console access settings
eepromdump	dumps EEPROM (configuration memory) contents
eraseconfig	erases EEPROM configuration
exit	closes connection with device
help	displays command list
ifconfig	interface configuration
kill	kills process
mem	memory usage
mii	MII (Ethernet) transceiver settings
netstat	TCP/IP connections list
ping	checks network device availability
prompt	changes command prompt
ps	displays process list
quit	closes connection with device
reboot	reboots device
route	routing table settings
sifcfg	serial port configuration
sitest	serial port tests
snmp	SNMP settings
ssh	ssh settings
syslog	sending logs to remote syslogd
tech	system information for tech support
telnet	telnet server settings
tcpdump	shows interface traffic
tftp	TFTP server settings
timeout	login and session timeout settings
uptime	shows router uptime

user	user management
ver	shows firmware version
vlan	VLAN bridging configuration
w	shows router uptime
write	writes settings to EEPROM

?

Shows a list of available commands.

arp

The arp command is used to configure the ARP table. The arp alone shows the list of bindings between the IP and hardware (MAC) addresses:

```
Tahoe> arp
IP address    Hardware address    Type         Expires
10.0.0.2      00:50:04:0D:70:31   dynamic      215s
Tahoe>
```

The "Type" can be "dynamic" (learnt from the network traffic), "static" (added manually) or "proxy" (a proxy ARP entry). The value in the "Expires" column denotes the time left until the ARP table entries' removal. ARP entries are removed when they are not used for 5 minutes.

ARP table entries can be deleted using the **arp del** command:

```
Tahoe> arp del 10.0.0.2
```

(insert the IP address to be deleted instead of "10.0.0.2").

A static ARP entry can be added using **arp add**:

```
Tahoe> arp add 10.0.0.3 00:50:13:E9:5C:01
```

A proxy ARP entry can also be added using **arp add**:

```
Tahoe> arp add 10.0.0.4 proxy
```

When a proxy ARP entry is added, the port server will respond with its own MAC address to the ARP requests asking for the specified IP address. Thanks to this function you may select an IP ad-

dress from the network connected to the Ethernet interface and assign it to the device on the other end of the WAN link. The port server will pretend to have that IP address, answer ARP requests and then forward received packets over the WAN link after an appropriate routing entry is added.

The dynamic hardware address resolution may be disabled using the **ifconfig** command. When disabled, only those stations whose IP and MAC addresses are entered statically into the ARP table using the **arp add** command are allowed to connect to the port server.

config

The **config** command displays the current configuration. The command output can be entered on another server to make an exact copy of the configuration.

console

This command is used to enable or disable password protection of the serial console. By default the console is unprotected and the user has full access to the port server. By entering:

```
Tahoe> console passwd on
```

the password requirement is enabled and the port server will ask for it in the same manner as during telnet connection. To disable password protection type:

```
Tahoe> console passwd off
```

eepromdump

This command displays the complete contents of the EEPROM (non-volatile) memory in hexadecimal form. It is used for debugging only.

eraseconfig

The **eraseconfig** command erases the whole configuration from the EEPROM. After rebooting the port server it will return to its factory defaults. Until the reboot it will continue to run with its current settings, which can be saved again using the **write** command.

exit

This command closes the configuration session and disconnects the user from the port server.

help

Shows a list of available commands.

ifconfig

This command allows configuration of the network interfaces. The following interface names are available:

- **eth0** - Ethernet interface
- **eth0.1**, **eth0.2**, etc. - VLAN networks (LAN networks separated from each other, although using the same cabling)
- **wan0**, **wan1**, etc. - G.shdsl bundle, the WAN interface

This command has similar syntax to the Linux ifconfig:

```
Tahoe> ifconfig <interface name> [<IP address>] [netmask <network mask>]
[bcast <broadcast address>] [ static | dynamic ] [bridge { on | off } ]
```

The **ifconfig** alone displays information about all active interfaces. Entering **ifconfig <interface name>** shows information about a specific interface. Information about the interface's IP address, number of packets and bytes sent and received, number of transmission errors and other important data are displayed.

You can assign an IP address to an interface, together with a subnet mask and broadcast address. You can also enable or disable dynamic Address Resolution Protocol (ARP, enabled by default).

kill

Kills a process that has stopped responding. The command requires one argument – process ID – which can be found by the **ps** command.

mem

Mem shows memory usage statistics. The **free** entry shows how much free memory is left, and the **free bufs** provides information about the amount of free memory destined for a network packet.

mii

The mii command allows access to the Ethernet transceiver. The following options are available:

- **`status`** – displays Ethernet port status (link state, negotiated speed, etc.)
- **`reset`** – resets the transceiver to the default settings
- **`auto`** – enables Ethernet auto-negotiation (default)
- **`adv { mode [, mode,...] }`** – sets a list of modes used during auto-negotiation. The modes may be selected from the following values: **100BaseTx-FD, 100BaseTx-HD, 10BaseT-FD, 10BaseT-HD**
- **`force { mode }`** – forces a specific mode and disables auto-negotiation
- **`power { on | off }`** – enables or disables the Ethernet port
- **`read [ address ]`** – read all or selected MII registers
- **`write { address } { value }`** – writes to an MII register

⚠ *Configuring the Ethernet transceiver may cause loss of the LAN connection, which in turn may make it impossible to manage the port server remotely*

netstat

Shows a list of TCP connections.

ping

Checks the availability of a device with the selected IP address. For example **ping 10.0.0.2** displays the time necessary to send a packet to the 10.0.0.2 station and back, or reports its unavailability:

```
Tahoe> ping 10.0.0.2
PING 10.0.0.2: 64 bytes
64 bytes from 10.0.0.2: seq=0 ttl=64 time=0.623 ms
64 bytes from 10.0.0.2: seq=1 ttl=64 time=0.471 ms
64 bytes from 10.0.0.2: seq=2 ttl=64 time=0.471 ms
--- 10.0.0.2 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
```

```
round-trip min/avg/max = 0.471/0.522/0.623 ms
Tahoe>
```

To stop pinging press Ctrl+C.

prompt

By using the **prompt** command you can change the default `Tahoe>` prompt to any other text that will help you identify the device.

ps

Shows the processes list

quit

This command closes the configuration session and disconnects from the port server.

reboot

Reboots the port server.

All unsaved changes to the configuration will be lost.

route

The **route** command is similar to an analogous Linux command. It is used to configure the IP routing. The **route** alone shows the current routing table. It may be modified using the following options:

route add *<address> <interface>* – adds the route to a specific host directly through the interface (the station with this address has to be in the network directly connected to that interface),

route add *<address>* **gw** *<gateway>* – adds the route to a specific host through a gateway,

route add -net *<address>* **netmask** *<network mask> <interface>* – adds the route to a subnet with given address and network mask directly on the specified interface,

route add -net *<address>* **netmask** *<network mask>* **gw** *<gateway>* – adds the route to a subnet with given address and network mask through the specified gateway,

route add default gw *<address>* – adds the default route through the specified gateway,

route del *<address>* – removes route to the specified IP address,

route del -net *<address>* **netmask** *<network mask>* – removes route to the specified subnet,

route del default – removes the default route.

sifcfg

This command is used to configure serial ports. It can also be used for establishing a connection between the current telnet / ssh / management console session and a given serial port.
The command syntax is the following:

- **sifcfg** - shows a summary of current settings:

```
Tahoe> sifcfg
Port
Number:    Owner:      Description:        State:
-------------------------------------------------------
      1    root        Serial _ Port _ 1    inactive
      2    root        Cisco Catalyst       <-> console
      3    root        Serial _ Port _ 3    inactive
      4    root        Serial _ Port _ 4    inactive
      5    root        FreeBSD _ 1          <-> 6
      6    root        FreeBSD _ 2           <-> 5
       ...
Tahoe>
```

The “Port Number” column shows the number of the port which is visible on the device’s front panel.

The “Owner” column shows who owns a given port. The owner can be chosen from users added by the **user** command. By default all ports are owned by root.

The “Description” column shows the text labels that were given by port users. It should help to find out which devices have been connected to specific ports without manual/visual cable examination.

The “State” column shows how data sent by the connected device are handled.

- the “inactive” state means that nobody is examining the connected device.
- “<-> console” means that the corresponding device is connected with telnet, ssh or the **Tahoe 8316/8332** management console. In that case it sends to and receives data from that console.
- “<-> 6” means that the port visible in the “Port Number” column is internally connected with the port visible in the “State” column.

- **sifcfg** <port number> - shows detailed information about given port settings

```
Tahoe> sifcfg 1
Owner:         root
Description:   Serial _ Port _ 1
State:         inactive
Baud rate:     9600
Data bits:     8
Parity:        none
Stop bits:     1
Flow control:  none
Tahoe>
```

- **sifcfg** <port number> **connect** <port number> - establishes connection between two ports. If the second port number is omitted, then a connection between a given port and the current telnet / ssh / **Tahoe 8316/8332** management console session will be made.

  Console connection can be stopped by “CTRL-A, Q” key combination. Local echo can be toggled by “”Ctrl-A, E” key combination.

  Escape character “CTRL-A” (0x01 ASCII) can be sent to the connected device as a sequence of two escape characters - “CTRL-A, CTRL-A”.

- **sifcfg** <port number> **disconnect** – disconnects a given port.

- **sifcfg** <port number> **baud_rate** <rate> – sets port baud rate. The following values can be used:

400	b/s	50000	b/s
4800	b/s	57600	b/s
9600	b/s	115200	b/s
19200	b/s	200000	b/s
38400	b/s	300000	b/s

Please note that stream concurrent transmission on all ports with 300 kb/s is not supported by the **Tahoe 8316/8332**. Our tests reveal that concurrent transmissions on 32 ports are supported up to 115200 b/s. Nevertheless, external conditions like connection cable quality and length, or electromagnetic fields in the device's environment can decrease this value. The safest way to achieve maximum speeds is to use a software or hardware flow control mechanism.

- **`sifcfg`** <port number> **data_bits** <bits> – sets number of data bits. 5-8 bit words are available.

- **`sifcfg`** <port number> **parity** <value> – sets the parity bit meaning. The following values are possible:

value	**short description**
none	no parity
odd	odd parity
even	even parity
mark	high parity (sticky) - obsolete
space	low parity (sticky) - obsolete

Additional information about parity modes is presented in the Appendix.

- **`sifcfg`** <port number> **stop_bits** <bits> – sets the length of the stop bit. Determines how long the stop bit will be asserted in comparison to a standard data bit period. Three values are possible: 1, 1.5, 2.

- **`sifcfg`** <port number> **flow_control** <control_kind> – sets the type of transmission flow control. The following options are possible:

option	short description
none	no flow control
Xon/Xoff	software flow control
hardware	hardware flow control (RTS/CTS)

- **`sifcfg`** <port number> **description** <label> – labels the port

- **`sifcfg`** <port number> **chown** <user_name> – changes owner of port. The owner must be one of the **Tahoe 8316/8332** users (i.e. someone who has been added to the user list by the **user** command). An unprivileged user may only see and manage ports that he owns. The "root" user can see and manage all available ports.

- **`sifcfg -r`** <port x – port y> <operation> – performs the operations described above on a range of ports, e.g.:

```
Tahoe> sifcfg -r 1-5 baud_rate 9600
Tahoe>
```

This command sets a 9600 kb/s baud rate for ports 1 through 5.

sitest

This command is used for testing serial ports. Two kinds of test are possible:

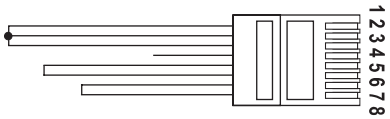
- test of single port:
  sitest <port number>

- test of all ports:
  sitest command with no arguments

The test procedure sets the following parameters for testing ports:

8-bit data, no-parity, 115200 kb/s, hardware flow control, one stop bit.

After performing the test all parameters are restored to the values saved in EEPROM. The test mechanism is simple – it just sends a test message and checks if the port receives the same one. This causes the necessity for a loopback adapter, which transmits the test message back to the device. The following picture shows the wiring of the test adapter:



Signals TXD-RXD, CTS-RTS, DCD-DSR-DTR are shorted together, and GND stays unconnected.

In the case of lack of loopback adapters it is still possible to test output ports. The following syntax is used to perform the internal test:

- test of single port:
  sitest -i <port number>

- test of all ports:
  sitest -i - no more arguments

Internal tests create loopbacks inside UART chips, but output transceivers are not tested in this case.

The following information is presented on a test screen:

```
Test number / failed:    5/5
================================
Ports:   1  2  3  4  5  6  7  8
        ------------------------
Status:  X  O  X  O  O  O  O  O
================================
Ports:   9 10  11 12 13 14 15 16
        ------------------------
Status:  O  O  O  O  O  O  O  O
================================

...

X = test passed
O = test failed
  = dropped packets
Press CTRL-C for exit...
Test report:
Port  1 - received: 6
Port  2 - received: 0
Port  3 - received: 6
Port  4 - received: 0
Port  5 - received: 0
Port  6 - received: 0
Port  7 - received: 0
Port  8 - received: 0
Press any key to continue...
```

The first line shows the number of transmitted test packets and the number of tests where at least one port lost a packet. Port status shows the last test status. 'X' represents a success and 'O' a fail. If a port dropped at least one packet, its status field is highlighted.

The screen can be refreshed by pressing CTRL-L, and the test can be stopped by pressing CTRL-C.

Afterwards, a test report is printed, showing how many test messages have been received by particular ports. If a specific field is not highlighted, then that port received all the test messages that were sent. Highlighting indicates some failures.

snmp

The **snmp** command is used to configure SNMP (Simple Network Management Protocol) support. It has the following syntax:

- **snmp** - shows current settings:

```
Tahoe> snmp
SNMP on
Read community: public
Write community: private
SNMP host1: <any>
SNMP host2: <disabled>
SNMP host3: <disabled>
Tahoe>
```

- **snmp on** - enables SNMP support
- **snmp off** - disables SNMP support
- **snmp rdcomm <community>** - sets the read community – the password used to read the SNMP parameters
- **snmp wrcomm <community>** - sets the write community – the password used to write the SNMP parameters
- **snmp host1 <address>**
- **snmp host2 <address>**
- **snmp host3 <address>** - allows setting of up to 3 addresses, from which SNMP access will be permitted. Entering 0.0.0.0 allows access from any address, while 255.255.255.255 disables an entry (entering 255.255.255.255 in all three positions is equal to disabling the SNMP service)

ssh

The ssh command configures the built-in Secure Shell server. The server can be enabled or disabled by entering, respectively:

ssh on

or

ssh off

The first time the server is enabled the host key must be generated (this may take several minutes). The SSH server port may be changed with

ssh port <port>

The default port is 21.

Access to the server can be limited by entering:

ssh host <IP address>

Then the server is only reachable from the given IP address. To remove the limitation enter 0.0.0.0 as the IP address.

syslog

The port server may send messages about its status and important events to a syslog server. To configure syslog logging the following commands may be used:

- **`syslog on`** - enables logging
- **`syslog off`** - disables logging
- **`syslog host <IP address>`** - sets the IP address to which the messages will be sent

tech

The **tech** command displays a detailed report about the server's internal state. That output may be used by the technical support for debugging purposes.

telnet

The command allows limiting telnet access to the port server. Access may be enabled or disabled by entering:

```
telnet on
```

or

```
telnet off
```

respectively. Moreover, access may be limited to a certain IP address:

```
Tahoe> telnet host <IP address>
```

If the IP address is set as 0.0.0.0, then access is possible from anywhere in the network.

⚠ *If you disable telnet access while connected through a telnet connection, you will lose the possibility to manage the port server remotely, and you won't be able to enable telnet access again without a reboot or local management through the serial console.*

tcpdump

The tcpdump command is used to monitor the network traffic on a specified interface. When no interface is specified eth0 is used by default:

```
Tahoe> tcpdump
05:51:27.453 > ether 00:12:3f:39:c9:dc (56)
       IP 192.168.20.101 -> 192.168.14.67
       ICMP echo request seq 2
05:51:27.541 < ether 00:12:3f:39:c9:dc (62)
       IP 192.168.14.67 -> 192.168.20.101
       ICMP echo reply seq 2
```

To stop monitoring traffic press Ctrl+C.

tftp

The command allows limiting the TFTP access used for the firmware's upgrade. Access may be enabled or disabled by entering:

```
tftp on
```

or

```
tftp off
```

respectively. Moreover, access may be limited to a certain IP address:

```
Tahoe> tftp host <IP address>
```

If the IP address is set as 0.0.0.0, then access is possible from anywhere in the network.

timeout

The command sets the inactivity time (in seconds), after which the telnet connection is closed:

```
Tahoe> timeout <during the session> [<during logging in>]
```

The first parameter is used after logging in, while the second one (optional) is used during the login process. Entering **0** disables the timer.

These settings are also applied to the serial console if its access is password protected (i.e. the **console passwd on** command was used).

Timeout without any arguments displays current settings.

uptime

Shows the time elapsed since server booting, and the current processor temperature.

user

The user command is used to manage users having access to the port server. The server may work in two different modes:

- single user - only the password is necessary to access the server. The user that logs in has full access to the device (default mode)
- multiple users - allows creating many users with different names, passwords and access levels

The **user** command has the following syntax:

- **`user list`** - shows the user list
- **`user add <name>`** - adds a new user
- **`user del <name>`** - removes a user
- **`user passwd <name> <password>`** - changes the user's password
- **`user level <name> <access level>`** - changes the user's access level. The **`<access level>`** argument may be one of:
  - **`admin`** - full access to the device
  - **`read-only`** - permits only reading of the configuration and the statistics

- **user mode { single | multi }** - selects the working mode - to either single or multi-user

ver

Displays current firmware version and compilation date.

vlan

The **vlan** command is used to manage VLAN configuration. The device may work in one of following modes:

- transparent – the VLAN-tagged packets are passed transparently. The device is transparent to the traffic and it's up to user to manage VLANs on external devices (default)
- non-transparent – the device may be set up to analyse the traffic and some packets may be directed to specified interfaces, while others may be filtered. Also VLAN headers may be removed or added while forwarding a packet, thus encapsulating a data stream from a specified interface into a VLAN.

The command has following syntax:

- **vlan show** – shows current settings
- **vlan transparent { on | off }** – enables or disables the transparent mode
- **vlan create** <**vid**> – inserts a new VLAN ID into the list of supported VLANs
- **vlan remove** <**vid**> – removes a VLAN ID from that list
- **vlan** <**vid**> **add** <**interface**> – adds an interface to a VLAN
- **vlan** <**vid**> **del** <**interface**> – removes an interface from a VLAN
- **vlan** <**vid**> **name** <**name**> – sets a VLAN name to ease identification
- **vlan** <**vid**> **{ tag | untag }** <**interface**> – sets an interface as tagged or untagged.

To manage VLAN traffic first you have to follow these steps:

1. Disable transparent mode using **vlan transparent off** command.
2. Add VLANs you want to forward using **vlan create** <**vid**>.

3. Add interfaces to that VLAN using **vlan** <**vid**> **add** <**interface**>.

4. Decide whether interfaces should be tagged or untagged using **vlan** <**vid**> { **tag | untag** } <**interface**> command. A tagged interface means that all traffic belonging to specified VLAN will be transmitted through that interface without modification (with a VLAN header). Such traffic can be further separated using an external VLAN-aware switch.

   In case of an untagged interface the VLAN headers will be stripped from the packets before they are transmitted over that interface. In the opposite direction the VLAN headers will be added to all untagged (i.e. regular) packets received on that interface. This way only regular Ethernet packets would appear on that interface (so you can connect regular Ethernet devices) while the device will see VLAN traffic only. Such VLAN traffic can be sent further to other devices without being mixed with packets coming from other sources.

The non-VLAN traffic is directed to a default VLAN with ID 1. That VLAN is used for internal processing only. All interfaces are added to that VLAN by default and are marked as untagged.

w

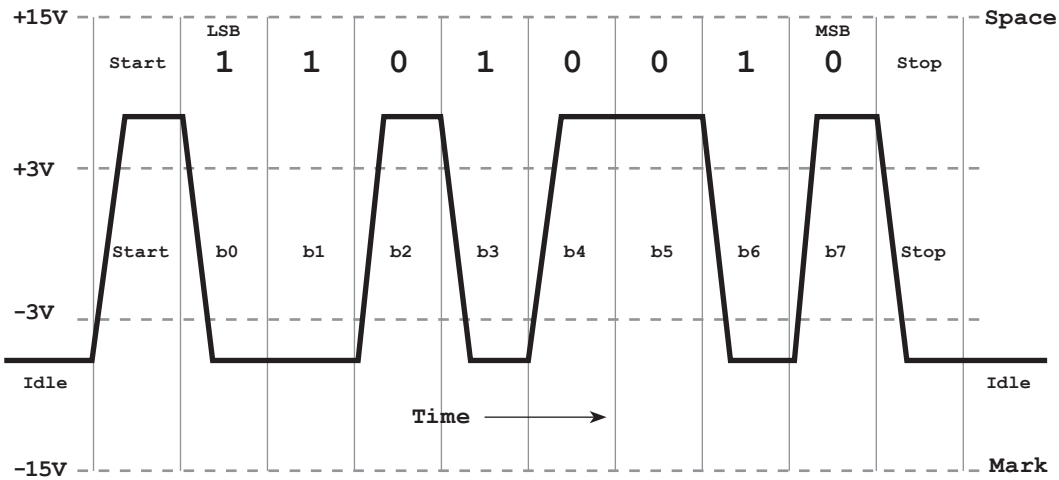
Shows the time elapsed since server booting and the current processor temperature.

write

Saves the current configuration to the EEPROM (non-volatile memory) so the port server keeps it after reboot or power off. The command also displays information about EEPROM usage. If the configuration is too large to be stored, some settings should be deleted, like static ARP entries, DHCP options, etc.

Appendix A, Short description of the RS-232

A typical RS-232 signal trace is presented in the following figure:



RS-232 signal

Mark and Space are terms that correspond to logical 1 and 0, but voltage levels are not intuitive. Here an inverted logic is used and Mark signal (-3V - -15V) corresponds to 1, and Space signal (+3V - +15V) corresponds to 0. Without any transmission the line stays in Mark state. When transmission starts the Space signal is asserted by the time of one bit. This signal is called a Start Bit. Bits that follow it are standard information bits - they carry one word of transmitted information. They are called Data Bits, and their amount can be set by the following command:

sifcfg <port> **data_bits** <value>

The bit that ends transmission of a single word is called the Stop Bit. It's span time can be between 1 and 2 span times of a single Data Bit. This value can be set by:

sifcfg <port> **stop_bits** <value>

A Parity Bit can be placed between Data Bits and a Stop Bit. This provides simple protection against transmission errors. There are several methods to calculate the Parity Bit. The most widely used are Even and Odd parities. Even parity means that the number of '1' between Start and Stop bits should be even. The Odd parity meaning is the opposite. In the above figure even parity would add Parity bit value 0 (because there are 4 ones, which is already an even number), and odd parity would add Parity bit value 1. Parity can be selected by command:

sifcfg <port> **parity** <value>

To avoid a data flood transmission control methods have been introduced. Xon/Xoff and RTS/CTS flow control methods are used most often.

Xon/Xoff is called a software flow control, because it uses special ASCII characters transmitted in RXD/TXD lines to stop transmission when the receiver is overloaded, and start it again when data can be further processed. The Tahoe 8316/8332 uses ASCII character 0x11 as the Xon signal, and 0x13 as the Xoff signal.

The RTS/CTS method uses dedicated lines and thus it is called hardware flow control. The sending device can start transmission to the receiver only if its CTS line is asserted. If receiver is overloaded by incoming data, it de-asserts the RTS line. Since RTS and CTS lines are crossed between sender and receiver, de-assertion of the receiver's RTS line is visible as de-assertion of the sender's CTS line, and it stops the sender.

Flow control can be set by the command:

sifcfg <port> **flow_control** <value>

Appendix B, Technical Specification

processor	Motorola PowerPC, 100MHz
memory	4MB SDRAM
network protocols	IP, TCP, UDP, ICMP, TFTP, SNMP, IEEE 802.1q
serial port throughput	up to 300 kbps for a single serial port
Ethernet interface	10/100Base-T, RJ-45 connector
management serial console	RS-232, DB9/M connector
dimensions	440 mm (width) x 43 mm (height, 1U) x 210 mm (depth)
power supply	100-240V AC, 50/60 Hz, 25W
environmental conditions	storage: temperature -20°C to 65°C, humidity 5 to 95% operation: temperature 0°C to 50°C, humidity 0 to 85%

Appendix C, Safety Information

Read the following safety notices before installing or using the Tahoe port server:

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

Read the installation instructions before you connect the device to its power source.

Do not work on the system or connect or disconnect cables during periods of lightning activity.

Do not connect the low voltage circuits (LAN port) to RS-232 circuits (serial port). Some LAN and RS-232 ports use the same RJ-45 connectors. Use caution when connecting cables.

This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that a fuse no larger than 240 VAC, 16A is used.

Appendix D, Declaration of Conformity

CE

TAHOE
Piotr Kaczmarzyk
ul. Hercena 3/5
50-453 Wroclaw, Poland

We declare that the products Tahoe 8316 and Tahoe 8332 comply with the regulations of the following European Directives:

- 73/23/EEC low voltage safety requirements
- 89/336/EEC EMC requirements
- 99/5/EEC radio & telecommunication terminal equipment requirements

The compliance of the Tahoe 8316 and Tahoe 8332 with the requirements of the above-mentioned directives is ensured by complete application of the following harmonized European Standards:

- EN 60950:2000
- EN 55022:1998
- EN 61000-6-1:2002
- EN 61000-6-3:2002

The products also comply with Directive 2002/95/EC on the restriction of the use of certain hazardous substances in electrical and electronic equipment (the "RoHS Directive") with the exemptions applicable for network infrastructure equipment for switching, signalling, transmission and network management (according to clause 7 of the Annex to the Directive).

Signed: Piotr Kaczmarzyk
Position: Director

Signature: 

Date: 01 August 2009
Place: Wroclaw, Poland

TAHOE®

Hercena 3-5
50453 Wrocław, Poland
phone: +48 71 344 26 37, fax: +48 71 344 26 42
www.tahoe-group.com