USER MANUAL

G.703 / Ethernet Routers series

TAHOE 1700

TAHOE

FREEDOM OF COMMUNICATION

TABLE OF CONTENTS

Tahoe® 1700 series (G.703 / Ethernet routers)

User Manual

http://www.tahoe-group.com/

Firmware version 1.2.7

Tahoe® assumes no responsibility for any errors or omissions that may appear in this document. Tahoe® makes no commitment to update the information contained here, and may make changes at any time without notice.

1. Introduction

Tahoe® 1700 series G.703/Ethernet routers are available in four versions:

- **Tahoe® 1701** router contains one unframed G.703 (E1) port and one Ethernet port

- **Tahoe® 1708** router also contains one unframed G.703 port, but instead of a single Ethernet port, a managed 8-port VLAN-enabled switch is built in

- **Tahoe® 1741** router in contrary has a framed G.703 interface and permits transmission over any combination of available timeslots. Single Ethernet port is also available

- **Tahoe® 1748** router is the most expanded model of all four - has a framed G.703 interface and a built-in managed 8-port VLAN-enabled switch

Routers are destined for use with HDLC or synchronous PPP point-to-point connections and Frame Relay networks.

Router software supports IP, ARP, TCP, UDP and ICMP protocols. It is manageable using telnet, SNMP or serial console. Traffic statistics are available through WWW. Router status messages can be sent to a central server using syslog protocol.

One network interface may support more than one IP subnetwork thanks to interface aliases (eth0:0, eth0:1, etc.) and VLAN interfaces (eth0.1, eth0.2, etc.). Router may also work as a bridge - in this mode both interconnected networks create one whole on the hardware level (e.g. computers with Microsoft® Windows™ operating system will see each other in the network neighborhood).

A built-in DHCP/BOOTP server allows assigning of IP addresses, network mask, router addresses and other parameters to the network stations. DHCP/BOOTP Relay Agent listens for DHCP and BOOTP requests and forwards them to a central server.

Routers support Network Address Translation, i.e. make it possible for a whole network to access Internet using only one real IP address. Additional firewall improves the network security by blocking unwanted traffic basing on IP addresses, TCP or UDP ports and protocols appearing in the received packets.

The system firmware is stored in the Flash memory - it is possible to update it using the TFTP protocol. The configuration is stored in the EEPROM memory.

2. Interfaces

2.1. G.703

The G.703 interface is equipped with a 8-pin RJ-45 connector. Although the G.703 standard does not specify the pinout, one used in Tahoe devices is most widely used and a straight patch-cord may be used to connect the router to an external device. Anyway the pinout should be carefully checked before connecting.

Pin	Signal
1	Rx+
2	Rx-
3	-
4	Tx+
5	Tx-
6	-
7	-
8	-

The RX+ pin of the router should be connected to the TX+ pin of the other device, the RX- pin to the TX- pin, TX+ to RX+ and TX- to RX-

2.2. Ethernet

The Ethernet interface is used to connect the router to the Local Area Network. In case of **Tahoe 1701®** and **Tahoe 1741®** routers it is a single RJ-45 connector with four LEDs:

- **LNK** - LAN Link, signals a proper connection to the LAN
- **COL** - Collision, signals an attempt to transmit to the LAN while another device also sends data
- **LRX** - LAN Receive, flashes, when data is received from the LAN
- **LTX** - LAN Transmit, flashes, when data is transmitted to the LAN

A router should be connected to an Ethernet switch or a hub using a straight patch-cord or to a PC, another router or an uplink port in a switch using a crossed-over one. After connecting a LED named "LAN Link" should be lit.

In case of **Tahoe® 1708** and **Tahoe® 1748** routers an 8-port switch is available instead of a single Ethernet interface. Each switch port has three LEDs associated to it:

- **10/100Mbps** - when lit, signals a 100Mbps connection
- **LINK/ACTIVITY** - when lit signals a proper connection to the

other device, flashes while transmitting or receiving data

- **DUPLEX/COLLISION** - when lit signals a full-duplex connection, flashes when a collision occurs in a half-duplex connection

The switch can be managed through a telnet or console connection. It supports VLAN tagging and automatically detects a crossed-over cable (so-called MDIX function).

2.3. Serial console

The RS-232 serial console is used for router 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 (bolded) 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 signaling
2	**RXD**	**data received from the PC**
3	**TXD**	**data sent by the router to the PC**
4	DTR	active, when the PC is switched on
5	**GND**	**signal ground**
6	DSR	active, when the router is switched on
7	RTS	used by the PC to inform that is has data to send
8	CTS	used by the router to permit data transmission
9	RI	ring indicator (signal used in telephone modems)

After connecting the console to the PC and running a terminal software, user has the same access to the router functions, as through a telnet connection (see chapter 3).

3

3. Configuration and management

3.1

3.1. Telnet connection

To connect to the router the network interface in your PC has to be in the same IP subnet as the router. By default the router’s Ethernet interface is set to 10.0.0.1 address and 255.0.0.0 netmask, so the PC may have IP address set to 10.0.0.2 and the same netmask.

If the router was already configured and the routing table is correctly set up, a telnet connection to its IP address is possible from anywhere in the network.

After connecting a password prompt will appear:

```
User Access Verification

Password:
```

The default password is **“Tahoe”** (case sensitive). If the password entered is correct, a command prompt will appear:

```
Tahoe>
```

3.2

3.2. Serial console

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

```
Tahoe>
```

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

3.3. Commands

3.3.1. ?, help

Entering "?" or "help" shows a list of available commands.

3.3.2. arp

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

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

ARP table entries may be deleted using "arp del":

```
Tahoe> arp del 10.0.0.2
```

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

A static ARP entry may be added using "arp add":

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

The dynamic hardware address resolution may be disabled using the "ifconfig" command. If it is disabled, only those stations may connect to the router, whose IP and MAC addresses are entered into the ARP table using the "arp add" command. This way an unauthorized network access may be prohibited.

3.3.3. bridge

The "bridge" command enables or disables the bridge mode, in which two interconnected LANs create one whole in the hardware layer. The stations in both LANs behave like if they were connected to one Ethernet switch, e.g. PCs working under Microsoft® Windows™ operating system will see each other in the network neighborhood. Three settings are available:

- ○ **off** - regular TCP/IP routing
- ○ **on** - bridge enabled, but the router is still available under its IP address and thus may be managed remotely

- **transparent** - completely transparent bridge, inaccessible under its IP address - this mode may be disabled only through the serial console

Entering **"bridge list"** displays a list of MAC addresses with the name of the interface on which certain address was heard.

Note: To make bridging work properly interfaces used in the process have to be indicated. To enable bridging on a certain interface enter "ifconfig <interface name> bridge on".

Note: To enable bridging the Cisco® HDLC link protocol should also be selected using "g703 hdlc" command

3.3.4. con

The „con" command erases whole configuration from the EEPROM. After rebooting the router 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 "write" command.

3.3.5. config

The „config" command displays current configuration. The command output may be entered on another router to make an exact copy of the configuration.

3.3.6. console

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

```
console passwd on
```

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

```
console passwd off
```

3.3.7. dhcp

The "dhcp" command is used to configure DHCP/BOOTP server and relay agent. The server is used to assign IP addresses, network masks, gateway and DNS addresses and other parameters to the network stations. It is easy to reconfigure a network that uses a DHCP server - it is enough to change server settings and every station will automatically retrieve new configuration.

The BOOTP protocol is an earlier and simpler version of DHCP. Its common use is booting of diskless workstations. A workstation uses BOOTP to get its IP address and other network parameters together with TFTP server address, from which the operating system may be downloaded.

The DHCP protocol may deliver more working parameters including domain name, DNS address, print server, syslog server, X-Window fontserver, MTU and TTL settings, and many others.

DHCP/BOOTP Relay Agent transfers DHCP and BOOTP requests and replies between separate networks. The DHCP and BOOTP protocols work only within one physical subnet. The station using such protocols doesn't know its IP address yet, so its packets cannot be routed to other networks. Relay Agent listens for such requests and forwards them to a DHCP server, which may be placed anywhere in the network.

3.3.7.1. Review of the settings

Entering "dhcp" alone displays current server settings. Here is an example:

```
Tahoe> dhcp
DHCP/BOOTP server
default-lease-time 43200
max-lease-time 86400
network "lan" (eth0):
    default-lease-time 43200
    max-lease-time 86400
    domain-name tahoe.pl
    subnet "local": 10.0.0.0/255.255.255.0
        default-lease-time 43200
        max-lease-time 86400
        filename vmlinuz.2.2.19
        next-server 192.168.0.5
    routers 10.0.0.1
        domain-name-servers 192.168.0.4
        domain-name tahoe.pl
        address ranges: 10.0.0.3-10.0.0.15
relay server 192.168.0.5 67
```

3.3.7.2. Basic DHCP server configuration rules

Before starting using DHCP server please read following guidelines:

- the configuration is organized in a hierarchical manner - the most general group of settings is “network” - the physical network connected to the router. Any number of IP “subnets” may exist within a network. Inside an IP subnet an IP address “range” may be selected - these addresses will be dynamically assigned to the network stations. A static connection between an IP address and a hardware address may also be set. Each group (“network”, “subnet”) has its own options. Creating a new group (e.g. a “subnet” within a “network”) causes copying of the options from the parent group (e.g. if the “lan” network has a “domain-name” option, after adding a “local” subnet within “lan” the option will be automatically copied - it may be modified or deleted later)
- on the beginning a “network” for each interface should be created
- in each of the “networks” an IP “subnet” should be created according to IP subnets connected to that interface (router may not have the routing set up to each of them - it’s enough that they are in the same physical network)
- now IP ranges and static IP entries may be added

3.3.7.3. dhcp [on | off | relay]

DHCP/BOOTP server may work in one of three modes:

- **on** - the server in enabled and answers to the requests
- **off -** the server is disabled
- **relay -** the server is disabled, but the relay agent is enabled and listens for the requests to be forwarded to other DHCP server

3.3.7.4. dhcp add

The “dhcp add” commands add a network, subnet, IP range, etc. Following variants are supported:

- **dhcp add network <name>**

Adds a new physical network connected to the router’s interface. There should be the same number of “networks” and interfaces. The “network”-interface connection will be determined later while adding the IP subnets.

```
dhcp add network lan
```

- **dhcp add subnet <name> <network> <address> <netmask>**

Adds a net IP subnet to a given network. For each IP subnet connected to the LAN or WAN interface an DHCP subnet should be added (with the same IP addresses, as configured on each of the interfaces). Moreover additional IP subnets may be added - those which are not set up on any of the interfaces, but do exist in the same physical network or behind a DHCP relay:

```
dhcp add subnet local lan 10.0.0.0 255.0.0.0
```

- **dhcp add host <name> <MAC address> <IP address>**

Adds a static connection between hardware (MAC) and IP addresses. The IP address must belong to one of the configured subnets. Only this IP address will be assigned to the given MAC address:

```
dhcp add host server 00:50:13:2e:15:ca 10.0.0.5
```

- **dhcp add range <start address> <end address>**

Adds an IP address range, from which addresses will be assigned to the network stations. The address range must be contained inside one of the subnets:

```
dhcp add range 10.0.0.5 10.0.0.37
```

- **dhcp add option <option> <value>**

Adds a global DHCP option sent to the requesting station. Available options are:

- **routers** - network gateways (usually the gateways should be separate for each subnet, so they shouldn't be defined globally)
- **domain-name -** domain name
- **domain-name-servers -** DNS addresses
- **filename -** name of the file containing the operating system
- **next-server -** server from which the mentioned above file will be downloaded using TFTP

```
dhcp add option domain-name tahoe-group.com
```

- **dhcp add relay <address> [<port>]**

Adds a DHCP server address to which the DHCP requests are forwarded, when the Relay Agent mode is enabled. The <port> parameter is optional - its default value is 67:

```
dhcp add relay 192.168.0.3
```

3.3.7.5. dhcp del

The command deletes a network, subnet, address range, etc.

- **dhcp del network <name>**
- **dhcp del subnet <name>**
- **dhcp del host <name>**

The commands above delete, respectively, a network, an IP subnet or a host (a static IP-MAC connection) with given name.

- **dhcp del relay <address>**

Deletes a DHCP server address used in the Relay Agent mode.

- **dhcp del range <start address> <end address>**

Deletes an IP address range assigned to the network stations.

- **dhcp del option <name> <value>**

Deletes a global option. Besides the option name, its value should also be given, because some options may have more than one value (e.g. domain name servers, routers, etc.).

3.3.7.6. dhcp rename

The command changes the name of a network, subnet or host:

- **dhcp rename network <old name> <new name>**
- **dhcp rename subnet <old name> <new name>**
- **dhcp rename host <old name> <new name>**

3.3.7.7. dhcp network/subnet/host

The command adds or deletes an option within a specified group - network, subnet or host. It has two forms:

- **dhcp network add <option name> <value>**
- **dhcp network del <option name> <value>**

(instead of „network", a „subnet" or „host" may be given; options are described in 4.3.7.4), e.g. :

```
dhcp network add domain-name tahoe-group.com
```

Options are valid only for a given network, subnet or host. Moreover two other parameters can be set:

- **dhcp network default-lease-time <value>**

Sets the time (in second), for which the IP address is assigned to the station. After that time the station must inform the DHCP server that it still uses that address. Otherwise the address will be considered as unused. This timeout prevents blocking an IP address when a station is switched off without releasing that address.

- **dhcp network max-lease-time <value>**

A station may request other lease time - the negotiated time may not be higher than this setting.

3.3.7.8. dhcp default-lease-time <value>
dhcp max-lease-time <value>

These commands are similar to those described in the previous paragraph, but their meaning is global.

3.3.8. exit, quit

The command closes the configuration session and disconnects from the router.

3.3.9. fr

A group of commands used to configure the Frame Relay protocol parameters. Following options are available:

- **fr { ansi | q933a | cisco } -** selects the LMI signaling: ANSI T1.617 Annex D, ITU Q.933 Annex A or Cisco® LMI

- **fr t391 <value>** - sets the T391 parameter, i.e. the number of failed retries during the communication through the LMI, after which the connection is considered as unusable

- **fr n391 <value>** - sets the N391 parameter, i.e. the time between subsequent LMI retries

- **fr debug { on | off}** - enables and disables sending the Frame Relay debugging information through syslog

3.3.10. g703

This is a group of commands used to configure the G.703 link. Following options are available:

- **g703 { fr | ppp | hdlc | raw }** - selects the protocol used to send data through the WAN port - Frame Relay, synchronous PPP, Cisco® HDLC or raw HDLC. The Cisco® HDLC is recommended if the router has to work in the bridge mode.
- **g703 coding { ami | hdb3 } -** sets the line coding. HDB3 is used by default and AMI is provided for compatibility only.
- **g703 idle <hexadecimal value>** - sets the value sent in unused timeslots
- **g703 { short | long }** - selects the sensivity of the G.703 receiver. In the "short" mode the transceiver's range is 50m and in "long" mode it is 2000m.
- **g703 { on | off }** - switches the G.703 port on and off

The **Tahoe 1741** and **Tahoe 1748** routers have framed G.703 ports, which may be configured using following commands:

- **g703 crc4 { on | off }** - switches the CRC4 transmission and checking on and off
- **g703 slots <comma separated list of timeslots or timeslot ranges>** - selects timeslots used for transmission, for example: "2-6,8,9,15-20"
- **g703 unframed** - selects unframed mode where whole 2048 kbps are used for transmission

Entering "g703" alone displays current settings.

3.3.11. http

The "http" command configures the built-in WWW server. It is used to provide an easy way to read router's statistics. Server can be enabled or disabled by entering, respectively:

http on or **http off**

Moreover the access to the server may be limited by typing:

http host <IP address>

Then the server is only reachable from the given IP address. To remove the limitation a 0.0.0.0 address should be entered.

3.3.12. ifconfig

The command allows configuring the network interfaces. Following interfaces are available:

- ○ **eth0** - Ethernet interface
- ○ **eth0:0, eth0:1,** etc**.** - eth0 interface aliases (one physical interface may support several IP subnets)
- ○ **eth0.1, eth0.2,** etc. - VLAN networks (LAN networks separated from each other, although using the same cabling)
- ○ **eth0.1:0, eth0.1:1**, etc. - VLAN interface aliases
- ○ **fr1, fr2,** etc. - Frame Relay PVCs (the number after "fr" is the DLCI of a given PVC)
- ○ **ppp0** - PPP interface used when the G.703 link works in the PPP mode
- ○ **hdlc0** - HDLC interface used when the G.703 link works in the Cisco® HDLC mode

This command has similar syntax as the Linux "ifconfig":

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

The "ifconfig" alone displays information about the active interfaces. Entering "ifconfig <interface name>" shows information about a certain interface. An information about interface's IP address, number of packets and bytes send and received, number of transmission errors and other important data is displayed..

An IP address may be assigned to an interface, together with subnet mask and broadcast address. A dynamic ARP may also be enabled or disabled.

The "bridge" parameter allows to include or exclude certain protocol from bridging, when the router works in the bridge mode.

3.3.13. ipchains

The command is used to control the firewall and the network address translation (NAT, called also "masquerade" - that is giving a network an access to the Internet using only one real IP address).

- **ipchains add** - adds an entry at the end of the list
- **ipchains insert** - adds an entry at the beginning of the list
- **ipchains del** - removes an entry
- **ipchains list** - displays current settings
- **ipchains flush** - removes all entries from the list

After the "add", "insert" or "del" option following parameters should be given:

- **-s** <source subnet>/<netmask> [port range]

Defines the source addresses which this entry concerns. If this parameter is omitted, then the entry concerns all source addresses.

- **-d** <destination subnet>/<netmask> [port range]

Defines the destination addresses which this entry concerns. If this parameter is omitted, then the entry concerns all destination addresses.

- **-p** <protocol> (optional)

Optionally the application of this rule may be limited to a certain protocol.

- **-y** (optional)

The rule may be applied to the TCP SYN packets only (i.e. the packets that initiate the TCP connection). It allows inhibiting the incoming connections while the returning packets for the outgoing ones will be passed.

- **-m** <IP address>

By default during the masquerade an outgoing interface's IP address is used. The option above allows forcing use of another address.

- **accept / deny / masq** - information, what to do with a packet, that conforms to a given rule (accept / discard / masquerade)

Note: The router always chooses the first matching rule from the list. So if the more general rule comes first, and the more specific is later, then the first one will be applied and the last one - ignored. Thus the specific rule has to be inserted **before** the general one, as in following example:

```
ipchains add -s 215.16.11.0/24 deny
ipchains insert -s 215.16.11.5 accept
```

Commands above inhibit the access for the whole 215.16.11.0/24 subnet **except** the 215.16.11.5 address.

Note: The specific "accept" rule (concerning one IP address) has to be inserted **before** the general one (concerning the whole subnet), either using the "insert" command as in the example above or by adding the specific rule first and then the general one. Otherwise the router will always apply the first rule and will never reach the second one, as the packet coming from 215.16.11.5 fits both of them and if the general one is first, then it will be applied.

More examples:

```
ipchains add d 0.0.0.0/0 80-80 p tcp deny
```

Inhibits access to the port 80 on all external servers.

```
ipchains add s 192.168.0.0/16 masq
```

Enables masquerade for the 192.168.0.0/16 subnet (other addresses are passed unchanged)

3.3.14. lang

Selects the language used to display messages during the telnet or console connection and on the LCD:

- ○ **lang 0 -** Polish
- ○ **lang 1** - English

3.3.15. masq

The "masq" command displays a list of masqueraded connections. The list consists of source and destination addresses, the port assigned by the router, the time remaining to the removal of an entry in case of connection inactivity and the amount of remaining free table entries that may be used for new connections. Both ports and IP addresses are printed as hexadecimal numbers.

3.3.16. mem

"Mem" shows the memory usage statistics. The "free" entry is the most important - it shows how much free memory is left.

3.3.17. netstat

Shows a list of active TCP connections.

3.3.18. ping

Checks the availability of a device with selected IP address. For example:

```
ping 10.0.0.2
```

gives the time necessary to send packet to the 10.0.0.2 station and back or reports its unavailability. Press Ctrl+C to stop the pinging process.

3.3.19. ppp

The "ppp" command sets up the PPP parameters when the G.703 link works in the synchronous PPP mode. Following options are available (the <port> parameter should be set to "ppp0"):

- **ppp <port> defroute on**
- **ppp <port> defroute off** - the command enables and disables, respectively, adding of the default route through the PPP interface after the connection is established
- **ppp <port> mtu <value>** - sets the maximum packet size that the router may send through the PPP interface (the final MTU setting depends also on the MRU setting on the remote router)
- **ppp <port> mru <value>** - sets the maximum packet size that the router will accept to receive
- **ppp <port> ip <local address>[:<remote address>]** - sets the IP addresses used during the PPP connection negotiation
- **ppp <port> up1 <command>**
- **ppp <port> up2 <command>**
- **ppp <port> up3 <command>**
- **ppp <port> up4 <command> -** the "up1" to "up4" options

allow execution of up to four commands after the PPP link is established

- **ppp <port> down1 <command>**
- **ppp <port> down2 <command>**
- **ppp <port> down3 <command>**
- **ppp <port> down4<command>** - the "down1" to "down4" options allow execution of up to four commands after the PPP link is broken down
- **ppp <ppp> user <username> -** sets the username used during the PPP authorization (if required by the remote router)
- **ppp <port> password <password>** - sets the password used during the PPP authorization (if required by the remote router)
- **ppp <port> debug on**
- **ppp <port> debug off**- enables and disables, respectively, the syslog debugging of the PPP link

3.3.20. prompt

The default "Tahoe>" prompt may be changed to help identifying the router. Enter **"prompt <new prompt>"** to change the default.

3.3.21. ps

Show the processes list.

3.3.22. reboot

Reboots the router. All unsaved changes to the configuration will be lost.

3.3.23. route

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

- **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 through a specified interface
- **route add -net <address> netmask <network mask> gw**

<gateway> - adds the route to a subnet with given address and network mask through a specified gateway

- **route add default gw <address>** - adds the default route through a given gateway
- **route del <address>** - removes route to an IP address given
- **route del -net <address> netmask <network mask> -** removes route to a subnet specified
- **route del default -** removes default route

3.3.24. snmp

The "snmp" command is used to configure the SNMP (Simple Network Management Protocol) support. It has 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>
```

- **snmp on -** enables SNMP support
- **snmp off** - disables SNMP support
- **snmp rdcomm <text>** - sets the read community - the password used to read the SNMP parameters
- **snmp wrcomm <text>** - 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 the SNMP access will be permited. 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)

3.3.25. strictarp

The "strictarp" command helps protecting the LAN against the unauthorized access. After enabling the "strictarp" mode (by typing **"strictarp on"**) and entering the static IP-MAC assignments (using "arp add") the router would listen to incoming ARP requests asking for the addresses it has in its static table. If the request comes from another

MAC address than in the router's ARP table, it will send an answer with the correct MAC address.

Such request is sent by the PCs working under the Microsoft® Windows™ operating system during the boot-up. If the ARP reply from the router comes, the PC will show a message that this address is occupied, which will make an illegal use of that IP address impossible. The "strictarp" mode may be disabled using **"strictarp off".**

3.3.26. syslog

The router may send the messages about its status and important events to a syslog server. To configure syslog logging 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

3.3.27. telnet

The command allows limiting the telnet access to the router. The access may be enabled or disabled by entering "**telnet on"** or "**telnet off**", respectively.

Moreover the access may be limited to a certain IP address:

telnet host <IP address>

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

3.3.28. tftp

The command configures the TFTP server used for the firmware upgrade. Three options are possible:

- ○ **tftp on** - enables the TFTP server
- ○ **tftp off** - disables the TFTP server
- ○ **tftp host <IP address>** - if the server is enabled, the access to it may be limited to a certain IP address. If this address is set to 0.0.0.0, then the access isn't limited.

3.3.29. timeout

The command sets the inactivity time (in seconds), after which the telnet connection is closed. It has following syntax:

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

The first parameter is used after the logging in and the second one (optional) during the log-in. Entering “0” disables the timer.

These settings are also applied to the serial console if its access is password protected (using the „console passwd on” command).

3.3.30. uptime, w

Shows the time elapsed since the router booting.

3.3.31. user

The “user” command is used to manage users having access to the router. The router may work in two different modes:

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

The “user” command has following syntax:

- **user list** - shows the user list
- **user add <name> -** adds a new user
- **user del <name> -** removes an user
- **user passwd <name> <password>** - changes the user’s password
- **user level <name> <access level>** - changes the user’s access level. The <access level> parameter 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

3.3.32. ver

Displays current firmware version.

3.3.33. watchdog

The “watchdog” command gives additional control over the router’s unpredicted behavior (i.e. a misconfiguration disabling further communication with the router). The router uses the “ping” command to check the availability of certain IP addresses and reboots, if one of them doesn’t answer.

The command has following syntax:

- **watchdog on** - enables the watchdog
- **watchdog off** - disables the watchdog
- **watchdog <interval> <amount> <wait> <IP address> [<additional IP address>]** - configures the watchdog. After **<interval>** seconds the router sends **<amount>** of pings to the **<IP address>** (and the **<additional IP address>** if set) waiting **<wait>** seconds after each of them. If there is no answer for any of the pings sent to the first address or for any of the pings sent to the second address, then the router is rebooted.

3.3.34. write

Saves the current configuration to the EEPROM and displays an information about the EEPROM usage. If the configuration is to large to be stored some settings should be deleted, like static ARP entries, DHCP options, etc.

4. Technical data

- processor:
  Motorola MC68302

- network protocols:
  IP, TCP, UDP, ICMP, TFTP, SNMP, DHCP, BOOTP, RFC-1490, PPP, Frame Relay, Cisco® HDLC, IEEE 802.1q

- Frame Relay signaling:
  ANSI T1.617 Annex A, ITU Q.933 Annex D, Cisco® LMI

- G.703 interface:

Tahoe® 1701 and Tahoe® 1708:

unframed

coding:	AMI, HDB3
receiver sensitivity:	-12 dB / -43 dB
range:	50m / 2000 m
throughput:	2048 kbps

Tahoe® 1741 and Tahoe® 1748:

framed according to G.704 or unframed

coding:	AMI, HDB3
signaling:	FAS, CCS, CRC4
receiver sensitivity:	-12 dB / -43 dB
range:	50m / 2000 m
throughput:	64 - 2048 kbps

- Ethernet interface:

Tahoe® 1701 and Tahoe® 1741:	10BaseT, RJ45 connector
Tahoe® 1708 and Tahoe® 1748:	10/100BaseT, 8 x RJ45

- serial console:
  RS-232, 9600 bps, 8N1, DB9/M connector

- dimensions:
  229 mm (width) x 57 mm (height) x 152 mm (length)

- power supply:

Tahoe® 1701 and Tahoe® 1741:	7.5V, 400 mA
Tahoe® 1708 and Tahoe® 1748:	7.5V, 1.2A

external power supply included

- environmental conditions:

storage:	temperature	-20°C to 65°C
	humidity	5 to 95%
operation:	temperature	0°C to 40°C
	humidity	0 to 85%

5. Declaration of Conformity

TAHOE
Piotr Kaczmarzyk
ul. Uniwersytecka 1
50-951 Wroclaw, Poland

We declare that the products Tahoe 1701, Tahoe 1708, Tahoe 1741 and Tahoe 1748 routers 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 Tahoe 1701, Tahoe 1708, Tahoe 1741 and Tahoe 1748 routers 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**

Signed: Piotr Kaczmarzyk
Position: Director

Signature: Piotr Kaczmarzyk

Date: 30 Apr 2004
Place: Wroclaw, Poland

Tahoe® assumes no responsibility for any errors or omissions that may appear in this document. Tahoe® makes no commitment to update the information contained here, and may make changes at any time without notice.

TAHOE®
Uniwersytecka 1
50951 Wrocław, Poland
phone +48 50 100 7362
fax +48 71 344 2642
http://www.tahoe-group.com/