Table of Contents

Table of Contents

1. Legal Notices

About this Document

This document provides introductory instructions on how to set up and manage the AXIS 9010 within your networking environment. Should you require more information, please refer to the Axis website at **http://www.axis.com.**

Safety Markings

Please observe all safety markings in this user's guide when using the product.

Caution! - Potential hazard that can damage the product.

Important! - Potential hazard that can seriously impair operation.

Do not proceed beyond any of the above notices until you fully understand the implications.

Maintenance

It is recommended that you use a moist cloth to clean the unit. Do not use petroleum based substances as this may cause damage to the casing.

Trademark Acknowledgements

The *Bluetooth* trademarks are owned by their proprietor and used by Axis Communications AB under license. DOS, Ethernet, Macintosh, Microsoft, OS/2, UNIX and Windows, are registered trademarks of their respective holders.

Copyright Information

Software Disclaimer

Part of the AXIS 9010 is based on a free SNMP package.

Disclaimer of Liability

Every care has been taken in the preparation of this user's guide; if you detect any inaccuracies or omissions,

please inform us by contacting your local Axis office.
Axis Communications AB cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice.
AXIS COMMUNICATIONS AB MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THE MATERIAL CONTAINED WITHIN THIS DOCUMENT, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.
AXIS COMMUNICATIONS AB SHALL NOT BE LIABLE NOR RESPONSIBLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE OR USE OF THIS MATERIAL.

Regulatory Statement

This device must be installed and used in accordance with the user's guide. This device complies with the following radio frequency and safety standards.

USA & Canada - This device complies with part 15 of the Federal Communications Commission (FCC) rules and with RSS-210 of the Industry Canada (IC). Operation is subject to the following conditions:
(1) This device may not cause harmful interference, and
(2) this device must accept any interference received, including interference that may cause undesired operation.

Europe - This device complies with the requirements of the R&TTE Directive 1999/5/EC with the test suites as per standards:
* EN 60950 Safety of Information Technology equipment
* ETS 300 328 Technical requirements for radio equipment
* ETS 300 826 General EMC requirements for radio equipment

CE 0682 !

Limited Hardware Warranty

AXIS 9010

Axis Communications AB warrants the original owner that the product delivered will be free from defects in material and workmanship for 90 days following the date of purchase. This warranty does not cover any damage attributable to erroneous installation of the product.

THIS WARRANTY IS THE SOLE WARRANTY AND IS IN LIEU OF ANY OTHER WARRANTY, WHETHER EXPRESSED, IMPLIED OR STATUTORY, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT, OR ANY WARRANTY ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. NOTWITHSTANDING THE FOREGOING AXIS SHALL HAVE NO LIABILITY FOR ANY INDIRECT OR SPECULATIVE DAMAGES (INCLUDING, WITHOUT LIMITING THE FOREGOING, CONSEQUENTIAL, INCIDENTAL AND SPECIAL DAMAGES) ARISING FROM THE USE OF OR INABILITY TO USE THIS PRODUCT, WHETHER ARISING OUT OF CONTRACT, NEGLIGENCE, TORT, OR UNDER ANY WARRANTY, IRRESPECTIVE OF WHETHER AXIS HAS ADVANCE NOTICE OF THE POSSIBILITY OF ANY SUCH DAMAGES, INCLUDING, BUT NOT LIMITED TO LOSS OF USE, BUSINESS INTERRUPTIONS, AND LOSS OF PROFITS, NOTWITHSTANDING THE FOREGOING, AXIS' TOTAL LIABILITY FOR ALL CLAIMS UNDER THIS AGREEMENT SHALL NOT EXCEED THE PRICE PAID FOR THE PRODUCT. THESE LIMITATIONS ON POTENTIAL LIABILITIES WERE AN ESSENTIAL ELEMENT IN SETTING THE PRODUCT PRICE. AXIS NEITHER ASSUMES NOR AUTHORIZES ANYONE TO ASSUME FOR IT ANY OTHER LIABILITIES.

This warranty does not cover replacement of products damaged by abuse, accident, misuse, neglect, alteration, repair, disaster, improper installation or improper testing.

Support Service

Should you require any technical assistance, please go to the Axis' website, contact your local dealer or use the support addresses at the back of this user's guide. If you are connected to the Internet, you can obtain on-line user's guides, technical support, software updates, application software and general corporate information from Axis' website.

Axis Official Home Page

All applicable software and information are available from the Axis' website at **http://www.axis.com**. This site enables you to access corporate and support information, and learn more about other Axis products.

www.axis.com

AXIS 9010 User's guide
Revision 2.0
Part No: 19966
Dated: February 2003

2. Quick Installation Procedure

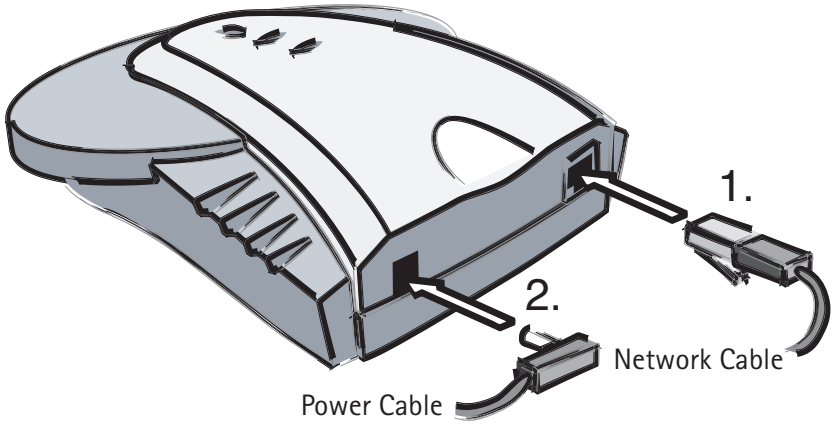
2.1 Installing your AXIS 9010

Follow the instructions below to quickly install the AXIS 9010 on an Ethernet network, which must be a TCP/IP-based system.

The AXIS 9010 supports DHCP server management and client IP address management. By default, the IP address of the AXIS 9010, as well as the IP addresses for the *Bluetooth* clients, are set automatically. No configuration is therefore necessary and you can follow the instructions below.

If you do **not** have a DHCP server, IP address for the AXIS 9010 must be assigned manually. Please go through the instructions 1-2 below and then refer to the installation instructions in section *5. AXIS 9010 IP Setting*, on page 15.

1. Connect your AXIS 9010 - first to the network with an Ethernet cable and then to the mains supply with the power supply (AXIS type PS-B):



2. Check the following after about 30 seconds:
   - The Power indicator displays a steady green light.
   - The Network indicator displays a steady or a flashing orange or green light.

Your AXIS 9010 is now ready for use.

2.2 Using your AXIS 9010

Make sure that the *Bluetooth* client, such as a laptop or a PDA, operates with *Bluetooth* wireless technology and supports the LAN access profile or the PAN profile.

1. Start the *Bluetooth* application in your client.
2. Start an inquiry and scan for *Bluetooth* devices.
3. Choose your AXIS 9010 from the list of alternatives and set up a *Bluetooth* radio link.
4. By default, the *Bluetooth* Passkey is set to a default value for your AXIS 9010. This means that if a login window appears in your client before you have established a *Bluetooth* radio link, the default PIN code which is printed on the product label on the underside of your unit, should be entered in the *Bluetooth* Passkey entry field.

2.3 Accessing AXIS 9010 Web Interface

To access the internal Web interface, you enter the IP address of your AXIS 9010 in the location field of your Web browser. By default, the *Bluetooth* Device Name of the AXIS 9010 is: “AXIS 9010 (<IP address>)”. This makes it easy to find the IP address of the AXIS 9010. The AXIS 9010 user ID is *root* and the default password is *pass*.

3. Preface

Thank you for purchasing the AXIS 9010 which uses *Bluetooth* wireless technology in order to connect to traditional networks.

3.1 About Axis Communications

Axis develops solutions for user-friendly and secure communication over wired and wireless networks. The company is a worldwide market leader in network connectivity, with products for the office, facility and industrial environments. Axis was founded in 1984 and is listed on Stockholmsborsen (XSSE:AXIS). With more than 300 employees, and offices in 14 countries, Axis operates globally in cooperation with distributors and OEM partners in 70 countries. Approximately 95 percent of production is exported out of Sweden. Information about Axis can be found at http://www.axis.com/.

3.2 About this User's guide

This user's guide provides introductory information as well as detailed instructions on how to set up and manage the AXIS 9010 in wireless network environments. It is intended for everyone involved in installing and managing the AXIS 9010.

To fully benefit from the user's guide, you should be familiar with basic networking principles.

This user's guide is applicable for the AXIS 9010 with software version release 2.0.

4. Product Overview

4.1 Package Contents

Verify that the AXIS 9010 package is complete by using the checklist below.

Please contact your dealer if anything should be missing or damaged. All packing materials are recyclable.

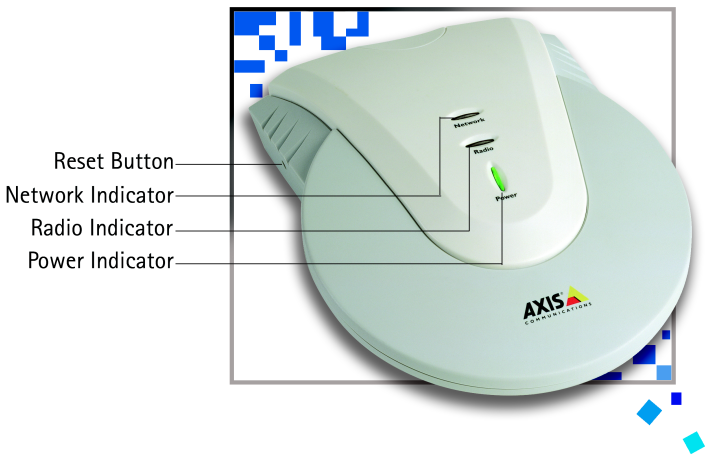
Hardware	Quantity	Model Variants	Part Numbers
AXIS 9010	1	9010 E3	0128-001-04
The AXIS 9010 User's Guide	1	rev. 2.0	19966
Power Supply (AXIS PS-B)	1	Australia	13269
		Europe	13267
		Japan	13936
		UK	13268
		USA	13270
Mounting Bracket	1	9010 E1	17662
Screws	2	ST4.2x25 RXS-Z FZB	17645

Note:

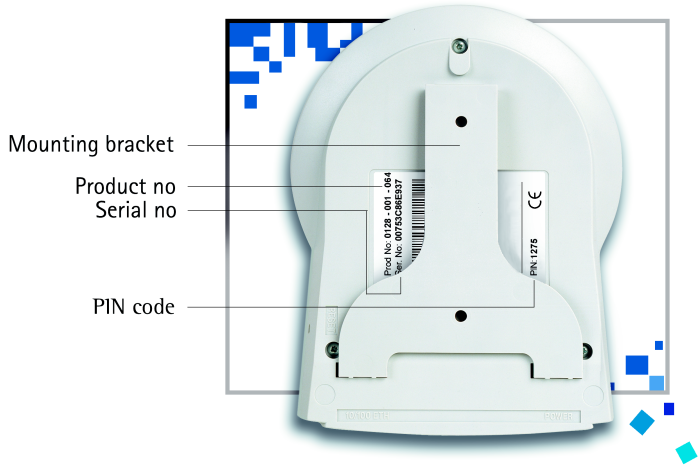
If you need to mount your AXIS 9010 on a wall or ceiling, the AXIS 9010 comes with a mounting bracket.

4.2 Physical Description

Front Panel



Underside



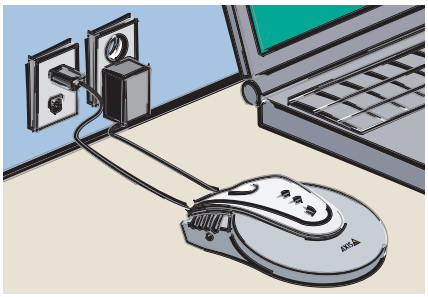
Rear Panel

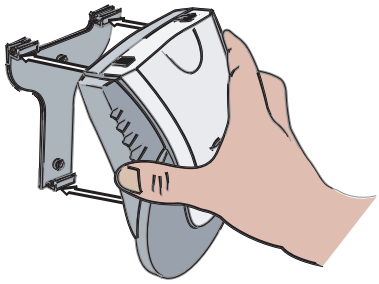
4.3 Indicators

Indicator	Color/Behavior	Explanation
Power	Green	OK
	Not lit	No power/Error
Network	Green	OK – 100 Mbps network connected
	Green flashing	Activity on 100 Mbps network
	Orange	OK – 10 Mbps network connected
	Orange flashing	Activity on 10 Mbps network
	Red	No physical connection to the network
Radio	Green	*Bluetooth* Radio link connected
	Green flashing	Activity on a *Bluetooth* Radio link
	Not lit	No *Bluetooth* Radio link connected
	Red (during upstart)	Settings are being restored/upgraded
	Red flashing	Error/Flash upgrading defective
	Orange flashing	*Bluetooth* module firmware upgrading

4.4 Placing the AXIS 9010

The AXIS 9010 can be placed horizontally on a flat surface, e.g. on your office desk, or with the mounting bracket on a wall or a ceiling. Place the AXIS 9010 close to power outlet and network connection.

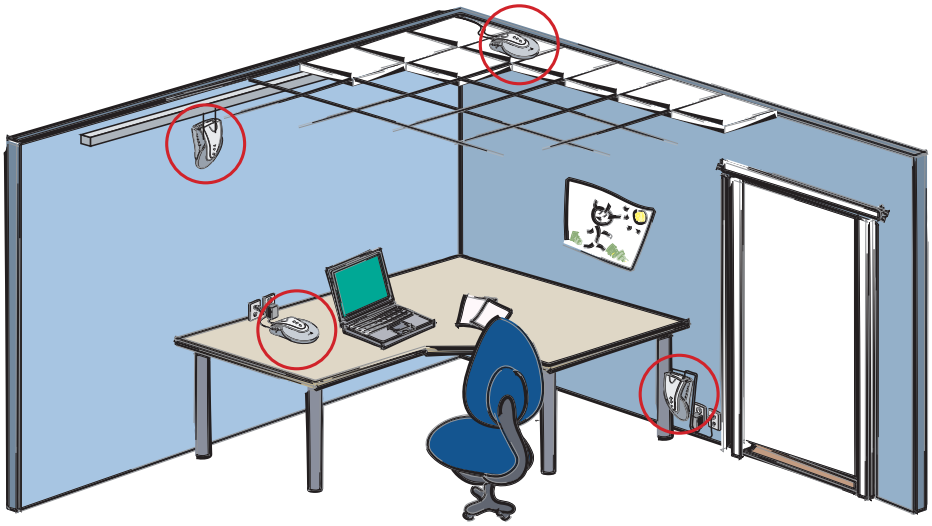




When placing the AXIS 9010, consider that it uses radio waves for transmission. Because the surrounding environment affects the range of the *Bluetooth* radio signal, try to avoid placing the AXIS 9010 where the radio signal can be shadowed by nearby obstacles.

The *Bluetooth* radio signal and its transmission quality can also be interfered with by other devices, such as microwave ovens, that use the same or adjacent frequencies. Do not place the AXIS 9010 close to any such devices.

To mount the AXIS 9010 on a wall, screw the mounting bracket into a wall using the two screws, and carefully attach the AXIS 9010 to the mounting bracket.

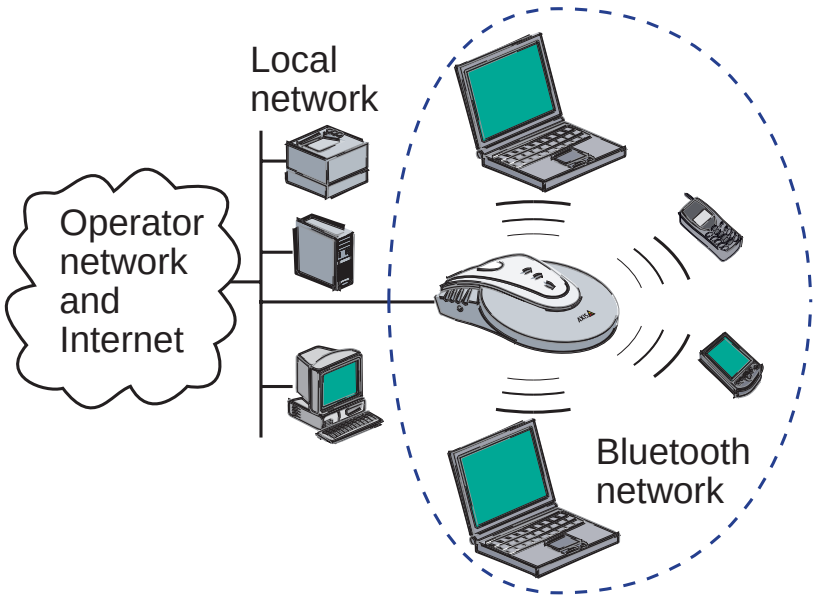


4.5 *Bluetooth* Wireless Technology

A revolution taking shape today is fundamentally changing the way people work, communicate and access information. The Internet is going wireless with an emerging world of new devices that bring mobile freedom to everyone.

Bluetooth wireless technology allows users to make effortless, wireless and instant connections between various communication devices, such as notebook computers and PDAs. Data can be sent at a speed of up to 723 kbps and for as many as seven simultaneous data users. The sophisticated mode of transmission adopted in the *Bluetooth* specification ensures protection from interference and security of data.

The *Bluetooth* radio operates in an unlicensed frequency band ensuring communication compatibility worldwide. This makes it easier for anyone to set up a local network and provide tailored wireless services based on *Bluetooth* wireless technology.



4.6 AXIS 9010

The AXIS 9010 provides the ”missing link” between devices powered by *Bluetooth* wireless technology and the Internet. Wireless devices within range have a simple, high-speed way to access network resources. The AXIS 9010 also provides a firm, flexible foundation for access control, security and other management and administration functions. Furthermore, the AXIS 9010, like other newly developed Axis products, has been designed around Axis' Linux-based ThinServer technology. It utilizes the latest version of the highly recognized ETRAX ”system on a chip” technology developed by Axis and runs an embedded Linux operating system and built-in Web-server.

The *Bluetooth* protocol stack developed by Axis, the OpenBT, is available for download at http://developer.axis.com/.

The AXIS 9010 includes a Linux operating system, which is freely distributed under the GNU General Public License as published by the Free Software Foundation. This software provides a stable and reliable platform.

5. AXIS 9010 IP Setting

When connecting to the network, your AXIS 9010 needs an IP address in order to be identified in the network. For the AXIS 9010, you can either set the IP address automatically or manually.

5.1 AXIS 9010 Automatic IP Setting

If you have access to a DHCP server, you can choose to let it assign an IP address to your AXIS 9010. All parameters needed for connection between the network, the AXIS 9010 and the *Bluetooth* clients are preset. Assignment through masquerading is the default setting.

Please follow the instructions in section *2. Quick Installation Procedure*, on page 6.

If you use DHCP to automatically assign a dynamic IP address to your AXIS 9010, the IP address is not known. You can locate the IP address by making an inquiry from a *Bluetooth* client to find the AXIS 9010, which will be shown in a list of devices. By default the *Bluetooth* Device Name of the AXIS 9010 is: AXIS 9010 (<IP address>). If the above method is not possible, check the IP address in the DHCP server or contact your network administrator.

5.2 AXIS 9010 Manual IP Setting

If you do not have access to a DHCP server, you must set the IP address for your AXIS 9010 manually. Start by installing the AXIS 9010 according to the instructions steps 1-2 in section *2.1 Installing your AXIS 9010*, on page 6.

To assign the IP address manually, map the AXIS 9010 physical address (also called MAC address) to the IP address. The physical address of your AXIS 9010 is the same number as the serial number. The serial number is located on the label placed on the underside of the unit.

You can easily assign a unique IP address to your AXIS 9010 from a computer on your network with the ARP command. The ARP commands will show and change the address conversion table for IP addresses and the physical addresses.

Important!

Do NOT use the IP addresses used in the following examples when installing your AXIS 9010. Always consult your network administrator before assigning an IP address to your AXIS 9010.

Follow the instructions below to set the IP address manually with ARP:

1. Note the serial number found on the underside label of the AXIS 9010. You need to know this to assign the IP address.
2. Acquire an unused IP address (external or internal) for your AXIS 9010 from your network administrator or Internet Service Provider (ISP).
3. Use a Windows- or a UNIX-based computer on your network to assign the new IP address to your AXIS 9010. You must set the IP address for the AXIS 9010 from a workstation within the same subnet.
4. If the AXIS 9010 is already connected to the network, restart it by removing and replacing the power cable. If you do not set the new IP address within 2 minutes you have to reset the AXIS 9010 again.
5. Map the physical address (equivalent to the serial number) of your AXIS 9010 to the IP address using the ARP command.
   Then ping your IP address by sending a packet with 408 bytes of data to the specified address and wait for a reply.

Windows 98/ME & NT/2000/XP:

Start a command prompt window and type these commands:

Syntax:

```
arp -s <IP address> <Serial number>
ping -t -l 408 <IP address>
```

Example:

```
arp -s   192.168.0.91 00-40-8C-18-10-D0
ping -t -l 408 192.168.0.91
```

The following message will be displayed in the command prompt window.

```
C:\WINDOWS>arp -s 192.168.0.91 00-40-8C-18-10-D2
C:\WINDOWS>ping -t -l 408 192.168.0.91

Pinging 192.168.0.91 with 408 bytes of data

Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.0.91: bytes=408 time=3ms TTL=64
Reply from 192.168.0.91: bytes=408 time=2ms TTL=64
Reply from 192.168.0.91: bytes=408 time=2ms TTL=64
```

Important!

In order for the pinging procedure to work correctly, the length must be 408.

UNIX:

Type these commands at your command line:

Syntax:

```
arp -s <IP address> <Serial number>
ping -s 408 <IP address>
```

Example:

```
arp -s   192.168.0.91 00:40:8C:18:10:D0
ping -s 408 192.168.0.91
```

The following text will be displayed in the command window:

```
>arp -s 192.168.0.91 00:40:8C:18:10:D0
>ping -s 408 192.168.0.91
PING 192.168.0.91 (192.168.0.91): 408 data bytes
416 bytes from 192.168.0.91: icmp_seq=12 ttl=64 time=1.7 ms
416 bytes from 192.168.0.91: icmp_seq=13 ttl=64 time=1.3 ms
416 bytes from 192.168.0.91: icmp_seq=14 ttl=64 time=1.3 ms
416 bytes from 192.168.0.91: icmp_seq=15 ttl=64 time=1.2 ms
416 bytes from 192.168.0.91: icmp_seq=16 ttl=64 time=1.3 ms
416 bytes from 192.168.0.91: icmp_seq=17 ttl=64 time=1.2 ms
416 bytes from 192.168.0.91: icmp_seq=18 ttl=64 time=1.2 ms
416 bytes from 192.168.0.91: icmp_seq=19 ttl=64 time=1.2 ms
```

6. Stop pinging the AXIS 9010 by pressing "Ctrl-C".

The IP setting is complete.

If your network has sub-networks or if you want to access the Internet, the subnet mask and gateway to your AXIS 9010 must also be defined. Please consult your network administrator or your ISP. You can set these parameters in the AXIS 9010 Web interface. Please refer to section *11. AXIS 9010 Web Interface*, on page 29.

6. *Bluetooth* Client IP Setting

When connecting to the AXIS 9010, your *Bluetooth* client (e.g. laptop) needs an IP address in order to be identified on the network.

Depending on the client, two network profiles are possible: the Local Area Network (LAN) access profile or the Personal Area Network (PAN) profile.

6.1 PAN Profile

The PAN profile defines a means of enabling *Bluetooth* devices to participate in a personal area network. The AXIS 9010 can be used as a network access point and acts as a bridge between a *Bluetooth* network and Ethernet. The AXIS 9010 will provide network services for each of the connected *Bluetooth* devices.

- Bridging

An AXIS 9010 which supports Network access point services can provide some of the features of an Ethernet bridge. The AXIS 9010 will forward Ethernet packets between each of the connected *Bluetooth* devices. The AXIS 9010 with the PAN profile has an additional connection to stationary network in which the Ethernet packets are exchanged via bridging.

Note

If a DHCP server is available on the network, the client should be configured to use DHCP.

If no DHCP server is available, the client could be configured to use manually assigned IP addresses.

- IP Masquerading

For the PAN profile the AXIS 9010 will assign IP addresses for the *Bluetooth* clients through IP Masquerading, within a Private network. If the PAN profile is used, the client should use DHCP for IP setting.

Note

If masquerading is disabled, all network traffic from the client is bridged and the client will not be assigned an IP address from the AXIS 9010.

6.2 LAN Access Profile

For the LAN access profile, there are three different ways for the AXIS 9010 to assign IP addresses for your *Bluetooth* clients:

- Automatic
- IP Masquerading
- Manual

6.3 IP setting methods

Important!

Set the dial-up application in your client to - server assigned IP address - in order to let the AXIS 9010 assign IP addresses to the *Bluetooth* clients.

Bluetooth Client IP Setting within a Private Network (IP Masquerading)

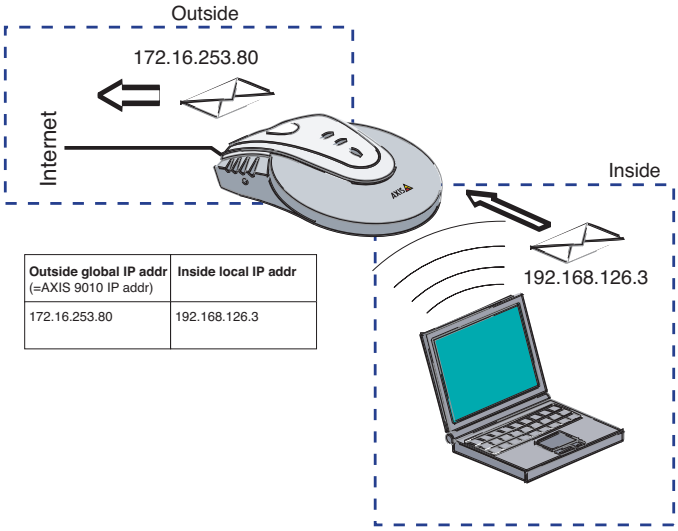
You can choose to assign the IP addresses for your *Bluetooth* clients within a range reserved for Private networks, using IP Masquerading. IP address assignment through masquerading is the default setting.

Important!

You must set the IP address to your AXIS 9010 before you can set the IP addresses to your clients. Please refer to section *5. AXIS 9010 IP Setting*, on page 15 for more information.

If you use IP Masquerading, the IP addresses for your *Bluetooth* clients will only apply between the *Bluetooth* clients and your AXIS 9010. They will be hidden to any network on the other side of the AXIS 9010.

The packets transmitted from the *Bluetooth* clients will appear as if they were originated directly from the AXIS 9010. IP Masquerading enables you to use several clients with unique internal identities through only one "official" IP address.



IP Masquerading uses almost the same method for IP translation as NAT (Network Address Translation), except that masquerading also uses the port number in the translation.

The default IP range for masquerading is 172.16.0.1-172.16.255.254. In addition the following IP ranges may be used: 192.168.126.1 - 192.168.126.254 and 10.0.0.1 - 10.255.255.254.

You assign the IP addresses for the *Bluetooth* clients in the AXIS 9010 Web interface. For more information please refer to section *11. AXIS 9010 Web Interface*, on page 29.

Note:

If you do not have access to more than one IP address on your network, you should select IP Masquerading for your clients.

Bluetooth Client Automatic IP Setting (LAN Access Profile)

If you have access to a DHCP server, you can choose to let it assign IP addresses to your clients via the AXIS 9010. All parameters needed for connection between the network, the AXIS 9010 and the *Bluetooth* clients are preset.

If you use Automatic IP setting and you activate the authentication function (RADIUS), the IP addresses for the *Bluetooth* clients will primarily be assigned by the RADIUS server and secondly by the DCHP server. For more information about RADIUS refer to section *8. Authentication for the LAN Access Profile*, on page 23.

Bluetooth Client Manual IP Setting (LAN Access Profile)

If you choose to assign the IP addresses for the *Bluetooth* clients manually, you need to specify the range of your IP addresses. Assign a unique and unused address range in order to prevent conflicts with other network devices.

To obtain the range of your IP addresses, consult your network administrator.

Important!

You must set the IP address to your AXIS 9010 before you can set the IP addresses to your clients. Please refer to section *5. AXIS 9010 IP Setting*, on page 15 for more information.

You assign the IP addresses for the *Bluetooth* clients in the AXIS 9010 Web interface. For more information please refer to *11. AXIS 9010 Web Interface*, on page 29.

7. Security

The AXIS 9010 has built-in functionality providing security for both management and access control.

7.1 Web Interface and FTP Security

In order to protect the settings from being changed by an unauthorized user, a security login process is initiated before you can access the Web interface or an FTP session. The user ID is *root* and the default password is *pass* in your AXIS 9010.

It is strongly recommended that you set a new password instead of the default password, *pass*. This password will apply for all users of the Web interface.

You can change the password in the AXIS 9010 Web interface.

7.2 *Bluetooth* Radio Link Security

To prevent unauthorized use of your AXIS 9010 a security login process is initiated before you can set up a *Bluetooth* radio link. By default, the *Bluetooth* Passkey is set to a default PIN code for each AXIS 9010. You will find the default PIN code on the underside of your AXIS 9010. This means that if a login window appears in your client before you have established a *Bluetooth* radio link, the PIN code should be entered in the entry field. It is strongly recommended that you set a specific passkey for your AXIS 9010.

When two *Bluetooth* devices connect to each other, a link key is created. By default the storing of link keys is active. If you deactivate the storing of link keys, the login window will appear in your client when connecting to your AXIS 9010. The number of link keys that can be stored is limited to 8 clients.

You can change the *Bluetooth* Passkey and deactivate the storing of link keys in the AXIS 9010 Web interface.

8. Authentication for the LAN Access Profile

The AXIS 9010 has support for RADIUS (Remote Authentication Dial-In User Service). RADIUS enables you to consolidate the management of all your remote users and enhance the security of your network. RADIUS is an encrypted protocol that provides authentication, authorization and accounting of user access in a network. It supports encrypted exchange of credentials between the remote end-user and the authentication server.

User credentials are forwarded to a RADIUS server, which in turn manages a credentials database. The login parameters in the *Bluetooth* client, user ID and password are the input to the RADIUS server. The server checks the user ID and password, then replies with the access privileges for the user.

Authentication checks user credentials to verify the user's identity. Authorization controls user privileges and access restrictions. Accounting keeps track of the amount of bytes and time for each connected session.

The RADIUS server can also handle the IP address assignment to the *Bluetooth* clients. If you use Automatic IP setting for the client and you activate RADIUS, the IP addresses for the *Bluetooth* clients will primarily be assigned by the RADIUS server and secondly by the DCHP server.

You activate the RADIUS function in the AXIS 9010 Web interface.

9. Monitoring

The AXIS 9010 has support for SNMP (Simple Network Management Protocol). SNMP is a protocol that enables remote management and monitoring of network entities. Functions like activity tracking, performance adjustment, error detection, resource monitoring, status control, initialization and security management are available through this protocol.

The AXIS 9010 has support for both SNMP version 1 (SNMPv1) and version 3 (SNMPv3). SNMPv1 transmits everything unencrypted and for access control it relies on community names, which are often known secrets. SNMPv3 uses encryption and can therefore provide a more secure configuration and monitoring link.

You activate the SNMP function in the AXIS 9010 Web interface.

9.1 AXIS MIB

The actual management is handled by a Network Management System (NMS) software running on a host on your network. To enable the NMS to read events from AXIS 9010 you need to add the AXIS MIB to your NMS software.

The AXIS MIB is available at www.axis.com. Download the MIB to your NMS.

10. Default Settings

The AXIS 9010 comes with a number of default settings. All of these settings are changeable.

Setting	Default Setting
Host name	axisxxxxxx
Bluetooth Device Name	AXIS 9010 (<IP address>)
Access Point name	AXIS 9010
User ID	root
Password	pass
Bluetooth Passkey	default value (PIN code)
Store *Bluetooth* Link keys	active
Date and time	not active
Time zone	GMT
AXIS 9010 IP address assignment	automatic (DHCP)
Bluetooth clients IP address assignment: - IP address assignment for PAN profile - IP address assignment for LAN profile	 masquerading masquerading
Enable DHCP on the masquerading net (PAN profile)	active
Masquerading range (when masquerading is chosen)	172.16.0.1-172.16.255.254
AXIS 9010 accessibility - Access area - Maximum number of *Bluetooth* clients	 largest possible 7
RADIUS	not active
RADIUS Authentication Port (when RADIUS is activated)	1812
RADIUS Accounting Port (when RADIUS is activated)	1813
SNMP	not active
Read community (when SNMPv1 is activated)	public
Trap port number (when SNMP is activated)	162
Trap on Authentication failure (when SNMP is activated)	not active
PPPoE	not active

Host Name

Your AXIS 9010 has a specific unit name, a Host name. This name is used in welcome and error responses from the FTP or Web server used by your AXIS 9010. By default, the Host name for your AXIS 9010 is *axisxxxxxx,* where *xxxxxx* is the last 6 characters of the serial number found on the underside label of your AXIS 9010.

If your network is using a DNS server, use the assigned name for your AXIS 9010 in that DNS server as the Host name. If your network does not have a DNS server, you can use the default name or enter a name of your own.

Bluetooth Device Name

The *Bluetooth* Device Name is the name that a *Bluetooth* device presents itself with. By default, the *Bluetooth* Device Name for your AXIS 9010 is "AXIS 9010 (<IP address>)".

Access Point Name

When connecting to your AXIS 9010 from a *Bluetooth* client you can perform an inquiry to scan for and discover other connectable *Bluetooth* devices, such as your AXIS 9010. In most cases, these devices are displayed in a list with the *Bluetooth* Device Address and/or the *Bluetooth* Device Name. To more easily find your AXIS 9010 in these lists the first part of the *Bluetooth* Device Name, the Access Point name, is by default set to "AXIS 9010".

User ID and Password

To access the AXIS 9010 Web interface or an FTP session a security login process is initiated. The user ID is *root* and the default password is *pass* in your AXIS 9010.

Bluetooth Passkey

To prevent unauthorized use of your AXIS 9010 you have a *Bluetooth* Passkey that restricts access to the *Bluetooth* radio link. The *Bluetooth* Passkey is set to a default PIN code for each AXIS 9010. You will find the default PIN on the underside of your AXIS 9010. If a login window appears in your client before you have established a *Bluetooth* radio link, the default PIN for the *Bluetooth* Passkey should be entered in the entry field.

Bluetooth Link key

When two *Bluetooth* devices connect to each other, a link key is created. By default the storing of link keys is active. If you deactivate the storing of link keys, the login window will appear in your client when connecting to your AXIS 9010.

Date and Time

The AXIS 9010 supports the Network Time Protocol. NTP is used to synchronize the date and time of a client to the AXIS 9010 or other reference time source. This can be used for e.g. invoicing purposes.

Time Zone

You can choose any of the 24 time zones of the globe (loosely divided by longitude) throughout which the same standard time is used. The default time zone is set to GMT.

AXIS 9010 IP Settings

By default, the IP address for your AXIS 9010 is set to be assigned automatically (DHCP).

Bluetooth Client IP Settings

The IP addresses for your *Bluetooth* clients are set to be assigned automatically by default, both the LAN access profile and for the PAN profile.

If you use Automatic IP setting for the LAN access profile, and you activate the authentication function (RADIUS), the IP addresses for the *Bluetooth* clients will primarily be assigned by the RADIUS server and secondly by the DCHP server. If you do not activate RADIUS, the DHCP server will handle the IP address assignment for the *Bluetooth* clients.

For the PAN profile, DHCP is enabled on the masquerading net by default.

Masquerading Range

If you choose to assign the IP addresses for your *Bluetooth* clients within a Private network (IP Masquerading), the range 172.16.0.1-172.16.255.254 is preset as the default range.

AXIS 9010 Accessibility

The maximum number of connected *Bluetooth* clients is 7, and the size of the access area can be set by radio buttons in seven steps. The default is set to largest possible access area.

Authentication (RADIUS) for the LAN access profile

RADIUS is a protocol used by remote access servers to provide authentication, authorization and accounting of user access in a network, and for automatic IP setting. If you choose to activate the authentication function, specify your RADIUS server and the transmission parameters in the AXIS 9010 Web interface. By default, RADIUS is set to “not active”. When activated, the default Authentication port number is 1812, and the default Accounting port number is 1813. RADIUS is only used for the LAN access profile.

SNMP

SNMP is a protocol that enables remote management and monitoring of network entities. If you choose to activate the SNMP, you need to specify the SNMP parameters in the AXIS 9010 Web interface. By default, SNMP is set to “not active”. When SNMPv1 is activated, the default Read community name is *public*. By default, the Trap port number is set to 162, and the Trap on Authentication failure is set to “not active”.

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a protocol used by many ADSL Internet Service Providers to allow authentication and maintain the familiar “dial-up experience” when connecting to the Internet. PPPoE specifies how a host personal computer (PC) interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) to achieve access a highspeed data network.

You activate the PPPoE function in the AXIS 90101 Web Interface

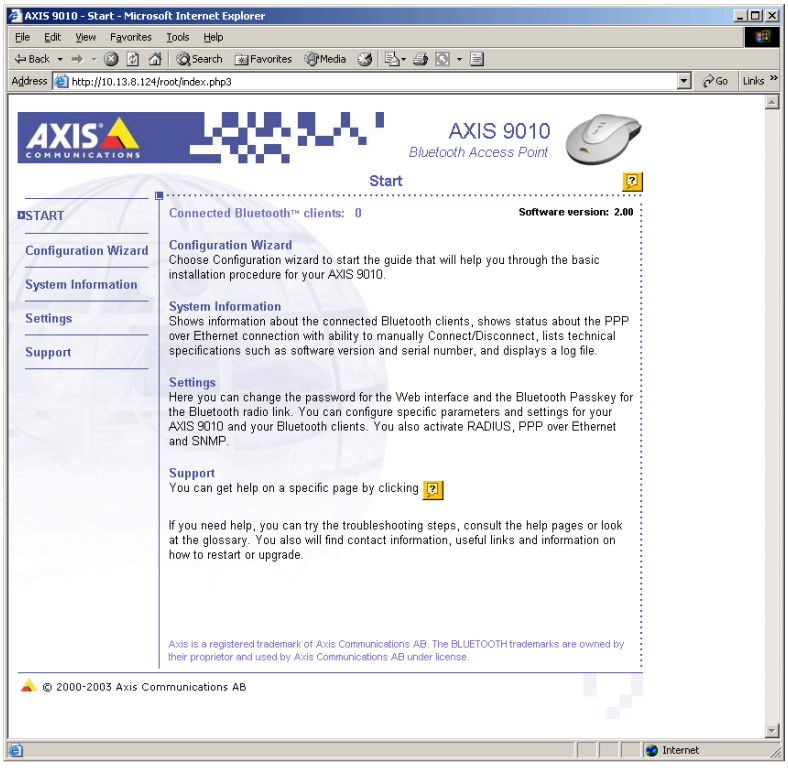
11. AXIS 9010 Web Interface

The AXIS 9010 has a built-in Web server with a Web interface for configuration, remote management and support information. In the Web interface you can check the settings and configure parameters.

11.1 Accessing the AXIS 9010 Web Interface

To access the Web interface, enter the IP address of the AXIS 9010 in the location field of a Web browser.

A login process is initiated before you can access the Web interface. The AXIS 9010 user ID is *root* and the default password is *pass*.



The left part of the window consists of a menu with links from which you can reach all the pages in the Web interface.

Note:

Online help  is available on every page within the AXIS 9010 Web interface. This is of particular relevance when configuring the unit. Use online help as a first point of reference for all administration queries.

11.2 Start Page

On the **Start page** of the AXIS 9010 Web interface, you will find general information about the contents of the Web interface and the number of connected *Bluetooth* clients.

11.3 Configuration Wizard

You can easily configure your AXIS 9010 by using the **Configuration Wizard**.

You can view the previous page by clicking Back and exit the Configuration wizard at any time by clicking **Close** or **Cancel**. The new configuration settings will not be saved to the AXIS 9010 until you click the **Finish** button on the last page of the wizard. The progress bar in the lower left corner of the Configuration wizard displays how far it is to the last wizard page.

11.4 System Information

System Information displays information about the connected *Bluetooth* clients, status for PPPoE, technical specifications and a log file. The log file lists events like restarting information and error messages for your AXIS 9010.

11.5 Settings

You can configure the parameters directly from the **Settings** link in the Web interface, and set an identity for your AXIS 9010.

Security Web & FTP

In order to protect the settings from being changed by an unauthorized user, a security login process is initiated before you can access the Web interface or an FTP session. The user ID is *root* and the default password is *pass* in your AXIS 9010. It is strongly recommended that you set a new password. This one password will apply for all users of the Web interface.

Security *Bluetooth*

To prevent unauthorized use of your AXIS 9010 a security login process is initiated before you can set up a *Bluetooth* radio link. The *Bluetooth* Passkey is set to a default PIN code for each AXIS 9010. You will find the default PIN on the underside of your AXIS 9010. It is strongly recommended that you set a specific passkey for your AXIS 9010. You can also deactivate the storing of link keys.

Date & Time

On the **Date & Time** page you can synchronize the computer clock times with a NTP Server using the Network Time Protocol. You choose time zone for the network, and you may also automatically adjust for daylight saving time changes.

Network

Under **Network** you can decide which method to use for AXIS 9010 IP setting - Automatic or Manual. You will also find the Host name and current IP address for your AXIS 9010 as well as other network specific parameters like Subnet mask, Default gateway, Domain name, DNS servers and WINS servers. These parameters set a network identity for your AXIS 9010.

Bluetooth

Here you can set a *Bluetooth* Device Name for your AXIS 9010. You can also choose which method to use to set the IP addresses for the *Bluetooth* client.

For the LAN access profile the following methods are available: Automatic, IP Masquerading and Manual. For the PAN profile IP Masquerading is used.

RADIUS

This page enables you to activate RADIUS and set specific parameters for it. RADIUS is a protocol that enables remote authentication, authorization and accounting of user access in a network, plus automatic IP setting.

SNMP

This page enables you to activate SNMPv1 and SNMPv3. You can also set the specific trap parameters.

PPPoE

To manually connect with PPP over Ethernet you must first check the Enable PPP over Ethernet checkbox. Then a Login User name must be set. You may also check the Dial On Demand checkbox.

Saved Settings

A complete list of all saved settings for an overview of the AXIS 9010 is displayed in this page.

11.6 Support

Troubleshooting

If you have problems, please try the troubleshooting steps first. Troubleshooting provides useful information to help you resolve any difficulty with your AXIS 9010. You can also find troubleshooting tips in this user's guide. Please refer to *Appendix B - Troubleshooting*, on page 42.

Help Contents

Help pages are sorted both by topic and alphabetical order. You can get specific, context-sensitive help on any page by clicking the **Help** icon  .

Glossary

The glossary contains explanations of different words and abbreviations that will appear in the Web interface or in the AXIS 9010 User's guide.

Contact and Links

Here you can find support information and useful links which will take you to the **AXIS 9010 Support page** and the **AXIS 9010 Product page**. They offer technical support, the latest news and problem forms for e-mail to Axis.

Status Report

The **Status Report** shows system information and the status of your AXIS 9010. When contacting Axis support, please copy the information in the Status Report and attach it to your message. This will help the support personnel to diagnose your problem.

Restart Options

Here you find information on how to restart, restore or reset your AXIS 9010.

Upgrade

When you click on the **Upgrade** link, your current software version is shown. You will also find a link to the download page on the Axis website, where software updates are offered.

12. Installing New Software

12.1 Obtaining New Software

The latest version of the AXIS 9010 software is available at www.axis.com.

12.2 Installing Updated Software

Download the updated software file and install it by doing the following:

1. Start a DOS window or a UNIX shell and find the catalogue where you have downloaded the new software.

Important!

Do NOT use the IP addresses used in the following examples when installing new software in your AXIS 9010.

2. Start an FTP session and write the following command:

   Syntax:

   ```
   ftp <IP address>
   ```

   Example:

   ```
   ftp 192.168.0.91
   ```

3. Log In to the AXIS 9010 using the correct user ID and password. By default, these are set to *root* and *pass* respectively. (The same login parameters as to the Web interface.)

   Syntax:

   ```
   user id: <user ID>
   password: <password>
   ```

   Example:

   ```
   user id: root
   password: pass
   ```

4. Set the session to binary transfer mode.

Syntax:

```
bin
```

Example:

```
bin
```

5. Upload the new software to your AXIS 9010.

   Syntax:

   ```
   put <file name> flash
   ```

   Example:

   ```
   put 9010_200.bin flash
   ```

Important!

Be careful not to interrupt the file transfer. If the transfer is interrupted, the AXIS 9010 may have to be re-programmed. More information is available in section *12.4 RFL*, on page 34.

6. The FTP prompt is returned once the programming is complete. The AXIS 9010 will restart automatically.
7. Exit the ftp session by typing “bye” or “quit“.

12.3 Software installation failure

If something is wrong with the software file (the file is corrupt or intended for another product), an error message will be communicated via the FTP prompt before the programming of the AXIS 9010 is initiated. Verify that the upgrade software corresponds with your AXIS 9010 version. The correct version of the AXIS 9010 software is available at www.axis.com.

If the software installation is interrupted while the AXIS 9010 is being programmed, the Radio indicator will blink red when the unit is restarted. Please refer to section *12.4 RFL* below.

12.4 RFL

The AXIS 9010 is equipped with a Resident Flash Loader (RFL), which allows you to program the unit when a previous software installation has been interrupted.

The RFL can detect an interrupted software installation, and will make the Radio indicator blink red when the unit is restarted. A simple web server has now been started with the same IP address that the unit had when the FTP upgrade was initiated. Opening a browser and entering the unit's IP address in the location field will bring up a simple form, containing two buttons. Use the Browse button to locate and select the correct software file, and then press Load. If the software file is correct the programming of the unit will start, and the Radio indicator will start blinking green. The unit will restart automatically when the programming is finished. More information about the RFL is available at www.axis.com.

13. Restart Options

In certain circumstances, it may be necessary to restart, restore or reset your AXIS 9010.

If you choose to restart your AXIS 9010, all your current connections with your *Bluetooth* clients will be lost. However, all the settings in your AXIS 9010 will remain as before. This is performed by clicking the **Restart** button in the AXIS 9010 Web interface.

If you choose to restore your settings, all settings in your AXIS 9010 - except the IP address, Subnet mask, Default gateway, password and the IP address assignment method for your AXIS 9010 (DHCP or manual) - will be returned to their original default values. This is performed by clicking the **Restore** button in the AXIS 9010 Web interface.

When you reset your AXIS 9010, all settings are set to factory defaults. Use the Reset button on your AXIS 9010.

13.1 Restart

1. In the AXIS 9010 Web interface, click on the **Support** link and choose the **Restart Options** link.
2. Click on the **Restart** button.
3. All connections to the clients will be lost, while all settings in the AXIS 9010 remain intact.

13.2 Restore Settings

1. In the AXIS 9010 Web interface, click on the **Support** link and choose the **Restart Options** link.
2. Click on the **Restore** button.
3. Your AXIS 9010 is now restored to its original factory default settings except for the IP address, Subnet mask, Default gateway, password and the IP address assignment method for your AXIS 9010 (DHCP or manual).

13.3 Reset to Factory Default Settings

1. Switch off the AXIS 9010 by disconnecting the power cable.
2. Press and hold the Reset button with a small tool, such as a pen or a paper clip, and reconnect the power supply cable.
3. Continue to press the Reset button until the Network indicator displays red (this may take up to 30 seconds), then release the Reset button.
4. Your AXIS 9010 is now reset and all settings are returned to factory default.

14. *Bluetooth* Client Installation

The client you want to connect to the AXIS 9010 must operate with *Bluetooth* wireless technology and support the LAN Access Profile or the PAN profile.

Set the dial-up application in your client to - server assigned IP address - to let the AXIS 9010 assign IP addresses to the *Bluetooth* clients.

Please refer to the specific *Bluetooth* client manual for information.

Appendix A - Technical specification

Supported System

Protocols:

- TCP/IP
- HTTP
- FTP
- ARP
- DHCP
- PPP
- PAP
- RADIUS
- SNMP
- NTP
- PPPoE
- *Bluetooth* (L2CAP/BNEP/SDP/RFCOMM)

Network

- 10baseT Ethernet or 100baseTX Fast Ethernet, auto-sensing.

Operating System

- Embedded Linux

Hardware

- ETRAX 100LX (100 MHz, 32-bit RISC processor)
- 4 MB FLASH PROM
- 16 MB DRAM
- One RJ-45 connector (twisted pair)

Bluetooth Specification

- *Bluetooth* LAN Access Profile, *Bluetooth* PAN Profile, *Bluetooth* Generic Access Profile and *Bluetooth* Serial Port Profile supported
- Point to multipoint operation, connecting up to 7 simultaneous clients.

- Internal antenna for optimal size and performance.
- Supports data rate up to: 723 kbps

RF Specification

- RF output power *Bluetooth* class 1
- Frequency range 2.402 to 2.480 GHz
- Double sided IF bandwidth 1 MHz

Receiver Performance

- Sensitivity (Pin=-70dBm) max 0.1% BER
- Max input level (Pin=-20dBm) max 0.1% BER
- C/I 1MHz (C=-60dBm) min 0dB

Transmitter Performance

- Output power max 20 dBm
- Frequency deviation 140 to 175kHz
- Carrier drift (1 slot, 366us) max +/-25kHz
- Carrier drift (3 slots, 1598us) max +/-40kHz
- Carrier drift (5 slots, 2862us) max+/-40kHz

Built-in Web Server

Configuration

- Access point IP address assignment: Automatically (DHCP) or proprietary arp-ping method
- Client IP address assignment from the AXIS 9010: Automatically, via masquerading or manually
- RADIUS control settings
- SNMP control settings

Management

- *Bluetooth* monitor, connected clients
- System log file

Support Information

- Troubleshooting, glossary, contacts, FAQ

Security

- Web interface – password
- AXIS 9010 *Bluetooth* radio link – *Bluetooth* Passkey
- Support for RADIUS

Monitoring

- Support for SNMP

Software Upgrades

- Free updated software is available at Axis Communications' website: http://www.axis.com
- Internal flash memory allows simple, central and remote software upgrades over the network using FTP.

Operating Conditions

- Indoor use only
- Temperature +5°C to +40°C (+40°F to +105°F)
- Humidity 20 – 80% RHG, non condensing humidity

Metrics

- Height 50 mm (1.97 inches)
- Width 143 mm (5.63 inches)
- Length 178 mm (7.01 inches)
- Weight 280 g (0.62 lbs.)

Power Consumption

- Maximum 2.5 W. Power provided by external supply (Type PS-B, 12 V, 500 mA)

Appendix B - Troubleshooting

This section provides useful information to help you resolve any difficulty you might have with your AXIS 9010. Fault symptoms, possible causes and remedial actions are provided within a quick reference table.

Please visit www.axis.com for latest troubleshooting tips, more support and additional help through the FAQ database or to fill in and mail a problem form.

Troubleshooting is also available in the AXIS 9010 Web interface.

Hardware

Symptoms	Possible causes	Remedial actions
The Power indicator is not constantly lit.	Faulty power supply.	Check your power supply and replace if needed.
The Network indicator is red.	No network access.	1. Verify that your network is accessible through your network socket. 2. Verify that your network cable is functional.

Bluetooth Radio Link

Symptoms	Possible causes	Remedial actions
Your *Bluetooth* client cannot find the AXIS 9010 after an inquiry has been made.	Insufficient *Bluetooth* radio signal. You are not within the radio range of the AXIS 9010 or too many obstacles between the AXIS 9010 and your *Bluetooth* client obstruct the *Bluetooth* radio signal.	Move to another position or move closer to the AXIS 9010 and try again.
	The AXIS 9010 is already serving a maximum number of *Bluetooth* clients.	Wait and try to connect again later.

Connecting

Symptoms	Possible causes	Remedial actions
Your *Bluetooth* client can find the AXIS 9010 after an inquiry has been made, but you cannot connect to the AXIS 9010.	The AXIS 9010 is already serving a maximum number of *Bluetooth* clients.	Wait and try to connect again later.
	The AXIS 9010 is not connected properly.	1. Check Power and Network indicator. 2. Check that assignment of IP addresses for the AXIS 9010 and for *Bluetooth* clients is correct. 3. To further check the IP addresses, run the Ping command from another computer as described in "IP address check" at the end of this chapter. Follow the appropriate recommendations.
	Your *Bluetooth* client lacks the correct *Bluetooth* Profile - the LAN Access Profile or the PAN Profile.	Contact the supplier of your *Bluetooth* client and check if an upgrade with the correct profile is possible. Otherwise, obtain a *Bluetooth* client with the correct profile.
	The settings of your *Bluetooth* client are not correct.	Check instructions for your *Bluetooth* client.
	Your *Bluetooth* client does not support master/slave configuration.	Instructions for disconnecting the master/slave function can be found at www.axis.com
	Your *Bluetooth* client does not support passkey configuration.	Instructions for disconnecting the authentication function can be found at www.axis.com

You are connected to the AXIS 9010 but when you try to dial up and access applications, the connection fails (only applicable if Radius is enabled and the LAN access profile is used)	The RADIUS parameter settings are incorrect.	1. Check the RADIUS parameter settings in both the RADIUS server and in AXIS 9010 Web interface.
		2. If you do not find any incorrect parameter settings, switch off the RADIUS function and try again to dial up your application. If you still cannot connect check the other troubleshooting steps for more help.
When you try to dial up and access other applications you get authentication failure (only applicable if Radius is enabled and the LAN access profile is used)	Your UserID and/or password are incorrect.	1. Make sure that you enter the correct UserID and password.
		2. Check that your UserID is registered in the RADIUS server.
		3. Check the RADIUS parameter settings in both the RADIUS server and in AXIS 9010 Web interface.

PPP over Ethernet

Symptoms	Possible causes	Remedial actions
You cannot connect to the Internet using PPPoE.	The Login User name and/or Login Password is wrong.	Check the Login Surname and Login Password.

Session

Symptoms	Possible causes	Remedial actions
The data rate of the transmission is very low.	Insufficient *Bluetooth* radio signal. You are not within the radio range of the AXIS 9010 or too many obstacles between the AXIS 9010 and your *Bluetooth* client obstruct the *Bluetooth* radio signal.	Move to another position or move closer to the AXIS 9010.
	The settings of your *Bluetooth* client are not correct.	Check instructions for your *Bluetooth* client.
	The *Bluetooth* radio signal is interfered.	Check that other devices using the same or adjacent frequencies are not placed close to the AXIS 9010 or the *Bluetooth* client.
Some of your applications will not run.	The IP address of your *Bluetooth* client is set through IP Masquerading. Applications outside your network that try to connect to a *Bluetooth* client served by your AXIS 9010 do not know the correct IP address since it is masqueraded.	If possible, choose another IP setting than IP Masquerading for your *Bluetooth* client.

The *Bluetooth* Client is not accessible from outside the network.	The AXIS 9010 is not connected properly.	1. Check Power and Network indicator. 2. Check that assignment of IP addresses for the AXIS 9010 and for *Bluetooth* clients is correct. 3. To further check the IP addresses, run the Ping command from another computer as described in "IP address check" at the end of this chapter. Follow the appropriate recommendations.
	The *Bluetooth* client is not connected to the AXIS 9010.	Wait and try to connect again later.
	The IP address of the *Bluetooth* client is set through IP Masquerading. Clients trying to connect to a *Bluetooth* client served by your AXIS 9010 do not know the correct IP address since it is masqueraded.	If possible, choose another IP setting than IP Masquerading for your *Bluetooth* client.
You lose the connection.	Insufficient *Bluetooth* radio signal. You are not within the radio range of the AXIS 9010 or too many obstacles between the AXIS 9010 and your *Bluetooth* client obstruct the *Bluetooth* radio signal.	Move to another position or move closer to the AXIS 9010 and try to reconnect.
	The settings of your *Bluetooth* client are not correct.	Check installation instructions and the manual for your *Bluetooth* client.
	The *Bluetooth* radio signal is interfered.	Check that other devices using the same or adjacent frequencies are not placed close to the AXIS 9010 or the *Bluetooth* client.

Software

Symptoms	Possible causes	Remedial actions
The AXIS 9010 Radio LED is blinking red.	Software upgrading failure	See *Installing Updated Software*, on page 33 and also the axis web site, www.axis.com
	It is not possible to upgrade or downgrade the software version	Install the original software version which corresponds with your AXIS 9010.

Web Interface

Symptoms	Possible causes	Remedial actions
The AXIS 9010 Web interface cannot be accessed from a Web browser.	The AXIS 9010 is not connected properly.	1. Check Power and Network indicator. 2. Check that assignment of IP addresses for the AXIS 9010 and for *Bluetooth* clients is correct. 3. To further check the IP addresses, run the Ping command from another computer as described in "IP address check" at the end of this chapter. Follow the appropriate recommendations.
	Problem with your proxy server.	Verify the proxy server setting in your Web browser.
	Other networking problems.	1. Verify that your network is accessible through your network socket. 2. Verify that your network cable is functional.

IP Address Check

By sending a data packet to a specific IP address and waiting for a reply, Ping can determine whether that IP address is accessible. Ping can also help you determine IP address conflicts with your AXIS 9010 and troubleshoot TCP/IP problems on the network. Follow the instructions below in association with Symptoms/Possible causes/Remedial actions when diagnosing your problem.

Ping Command:

1. Start a command prompt window or a UNIX shell.
2. Type ”ping x.x.x.x”, where x.x.x.x is the IP address you want to check - for example the IP address of your AXIS 9010.

3. Subsequent replies will provide an explanation of the cause of the problem. Replies from the command prompt can be interpreted as defined in the table below:

Ping Reply	Interpretation and recommendation	
	AXIS 9010 connected	AXIS 9010 disconnected
bytes = 32 time = 2 ms..... - or something similar	The AXIS 9010 is responding correctly. There are probably no conflicts with the IP address - disconnect the AXIS 9010 and ping again to verify.	The IP address is already used and cannot be used again. You must obtain a new IP address for your AXIS 9010.
destination host unreachable	The AXIS 9010 is not accessible. Check your network settings.	_____
request timed out	The IP address is not in use. You are either pinging the wrong IP address or your AXIS 9010 does not have the correct IP address.	This IP address is not used by anyone and is available for use for your AXIS 9010. Set the IP address again, power on the AXIS 9010 and then try accessing the unit.
no response from ping command	The AXIS 9010 is not accessible. Check your network settings.	_____

Note:

Please visit www.axis.com for more support and additional help through the FAQ database or to fill in and mail a problem form.

Appendix C - Definition of Terms and Abbreviations

The most needed phrases are described in brief here. For a full glossary please refer to the Web interface.

ARP

ARP (Address Resolution Protocol) is an Internet protocol that allows a host to find the physical address of a node on the same network when only the logical IP address of the node is known. An ARP request is broadcasted onto the network, and the node with that IP address sends back its hardware address.

Access Point Name

To more easily find your AXIS 9010 in scanning lists the first part of the *Bluetooth* Device Name, the Access Point name, is by default set to "AXIS 9010".

Bluetooth Device Address

An address set at the factory and a specific identity for the device (not to be confused with the IP address). In most cases, you can find the *Bluetooth* Device Address somewhere on your *Bluetooth* device.

Bluetooth Device Name

The *Bluetooth* Device Name is the name that a *Bluetooth* device presents itself with. By default, the *Bluetooth* Device Name for your AXIS 9010 is "AXIS 9010 (<IP address>)".

Bluetooth Passkey

The *Bluetooth* Passkey is a security login parameter you enter before you can set up a *Bluetooth* radio link.

Bluetooth Wireless Technology

Bluetooth wireless technology makes it possible to connect any compatible portable and stationary communication device without any cable. The technology is based on a radio link that offers transmissions of both voice and data. *Bluetooth* wireless technology operates on local mobile systems and local networks using radio transmissions.

DHCP

DHCP (Dynamic Host Configuration Protocol) is a protocol that lets network administrators centrally manage and automate the assignment of Internet Protocol addresses in a network. Using the Internet's set of protocol (TCP/IP), each machine that can connect to the Internet needs a unique IP address. When users want to access the Internet, an IP address must be assigned to each unit.

DNS Server

DNS (Domain Name Service) servers translate Internet domain names and Host names to IP addresses on your network. If you choose to set the AXIS 9010's IP address manually, you can specify the address to the Primary and Secondary DNS server.

Domain Name
A Domain is a set of computers on a network that have been assigned a group name. If you have chosen to set the IP address for the AXIS 9010 manually, you can specify the Domain Name to which the AXIS 9010 belongs.

Gateway
A gateway is a network point that acts as an entrance to another network. If you choose to set the IP address for the AXIS 9010 manually and wish to access the Internet, you must specify the Default gateway.

IP Address
In the most widely installed level of the Internet Protocol (IP) today, an IP address is a 32-bit binary digit number that identifies each sender or receiver of information that is sent in a packet across the Internet.

IP Masquerading
A firewall or router performs IP Masquerading if it changes the source IP address and port number on every packet that originates from one side of the client before forwarding that packet to the other side. Returned packets are similarly translated, so that they return to the internal machine which initiated a connection. IP Masquerading is a popular method for hiding a protected IP address space from the Internet. Internal users access services on the Internet as usual, but Internet services only see connections that originate on the firewall or the router. IP Masquerading uses almost the same method for IP translation as NAT, except that masquerading also uses the port number in the translation.

ISP
An ISP (Internet Service Provider) is a company that provides access to the Internet and other related services.

Link key
A link key is partly based on the Bluetooth Passkey and is created and exchanged as authentication when establishing connection between *Bluetooth* devices.

MAC Address
On a local area network or other networks, the MAC (Media Access Control) address is your computer's unique hardware number, the physical address.

NTP
NTP (Network Time Protocol) is used to synchronize computer clock times in a network of computers.

PAN Profile
A PAN (Personal Area Network) is a network of Bluetooth devices that share the same master unit and frequency-hopping sequence. A PAN starts with two Bluetooth connected devices and may grow up to seven connected devices. When establishing a PAN, the AXIS 9010 will act as a master and the devices as slaves. To insure security, authorization is needed when joining the PAN.

Ping
Ping is a basic Internet program that lets you verify that a particular IP address exists and can accept requests. Ping can also be used with an operating host to see how long it takes to get a response. Ping sends a packet to a designated address and waits for a response. The computer acronym was contrived to match the submariners term for the sound of a returned sonar pulse.

PPPoE
PPPoE (Point-to-Point Protocol over Ethernet) is a protocol used by many ADSL Internet Service Providers to allow authentication and maintain the familiar "dial-up experience" when connecting to the Internet. PPPoE specifies how a host personal computer (PC) interacts with a broadband modem (i.e. xDSL, cable, wireless, etc.) to achieve access to a highspeed data network.

RADIUS
RADIUS (Remote Authentication Dial-In User Service) is a protocol used by remote access servers for user authentication. User credentials are forwarded to a RADIUS server, which manages a credentials database. The RADIUS server carries out authentication. This delegation of the authentication process allows users to have a single set of credentials across all remote access servers. RADIUS is an encrypted protocol, and supports the encrypted exchange of credentials between the remote end-user and the authentication server.

RFL
RFL (Resident Flash Loader) allows you to program the AXIS 9010 when a previous software installation has been interrupted. The RFL can detect an interrupted software installation and re-install the software.

Serial Number
The serial number is located on the underside label of the AXIS 9010. Please note that the serial number of your AXIS 9010 is identical to the unit's physical address (MAC address).

SNMP
SNMP (Simple Network Management Protocol) is a protocol that governs network management and the monitoring of network devices and their functions. SNMP refers to a set of standards for network management, including a protocol, a database structure specification and a set of data objects.

Subnet Mask
A network can be divided into one or more physical networks to form sub-networks. A subnet mask indicates which portion of the IP address that represents the sub-network and the host address (the main network) respectively. If you choose to manually assign the IP address for your AXIS 9010, you can specify the subnet mask. To access the Internet, you must specify the Subnet mask. 255.255.255.0 is an example of a subnet mask. Consult your network administrator or your ISP to obtain the Subnet mask.

Web Interface
The AXIS 9010 includes a Web server and an internal Web interface. This means that you can browse to your AXIS 9010 Web interface using the IP address in the location field of your browser.

WINS Server

WINS (Windows Internet Naming Service) manages the association of workstation names and locations with the IP addresses. Its function resembles the DNS server.

Appendix D - Software Disclaimer

OpenSSL

OpenSSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

dhcpd

The Internet Software Consortium

Net-SNMP

Carnegie Mellon University

The Regents of the University of California

EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

PHP

The PHP Development Team

Copyright (c) 2000 The PHP Development Team. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software written by the PHP Development Team"
4. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission from the PHP Development Team. This does not apply to add-on libraries or tools that work in conjunction with PHP. In such a case the PHP name may be used to indicate that the product supports PHP.
5. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software written by the PHP Development

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

PPPD/RADIUS Client

Carnegie Mellon University

Copyright (c) 1984-2000 Carnegie Mellon University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any legal details, please contact Office of Technology Transfer Carnegie Mellon University 5000 Forbes Avenue Pittsburgh, PA 15213-3890 (412) 268-4387, fax: (412) 268-7395 tech-transfer@andrew.cmu.edu
4. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/)."

CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Paul Mackerras

Copyright (c) 1993-2002 Paul Mackerras. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name(s) of the authors of this software must not be used to endorse or promote products derived from this software without prior written permission.
4. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Paul Mackerras <paulus@samba.org>".

THE AUTHORS OF THIS SOFTWARE DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Pedro Roque Marques

Copyright (c) 1995 Pedro Roque Marques. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name(s) of the authors of this software must not be used to endorse or promote products derived from this software without prior written permission.
4. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by Pedro Roque Marques <pedro_m@yahoo.com>"

THE AUTHORS OF THIS SOFTWARE DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Tommi Komulainen

Eric Rosenquist

Google, Inc.

WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Gregory M. Christy

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by Gregory M. Christy. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

RSA Data Security, Inc.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message- Digest Algorithm" in all material mentioning or referencing this software or this function. License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work. RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind. These notices must be retained in any copies of any part of this documentation and/or software.

Roaring Penguin Software Inc.

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Roaring Penguin Software Inc. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Roaring Penguin Software Inc. Roaring Penguin Software Inc. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Lars Fenneberg

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Lars Fenneberg not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Lars Fenneberg.

Lars Fenneberg makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Livingston Enterprises, Inc.

Livingston Enterprises, Inc. 6920 Koll Center Parkway Pleasanton, CA 94566 Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Livingston Enterprises, Inc. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission,

and notice be given in supporting documentation that copying and distribution is by permission of Livingston Enterprises, Inc. Livingston Enterprises, Inc. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

The Regents of the University of Michigan and Merit Network, Inc.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies of the software and derivative works or modified versions thereof, and that both the copyright notice and this permission and disclaimer notice appear in supporting documentation.

THIS SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE REGENTS OF THE UNIVERSITY OF MICHIGAN AND MERIT NETWORK, INC. DO NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET LICENSEE'S REQUIREMENTS OR THAT OPERATION WILL BE UNINTERRUPTED OR ERROR FREE. The Regents of the

University of Michigan and Merit Network, Inc. shall not be liable for any special, indirect, incidental or consequential damages with respect to any claim by Licensee or any third party arising from use of the software.

Index