Setting Up Dial-In Service

TABLE OF CONTENTS

Copyright © Nokia Mobile Phones 2001. All rights reserved.

1. Introduction

The Nokia 9210 Communicator is a versatile communications product, offering full-fledged TCP/IP connectivity for mobile applications.

This document describes how to set up servers to provide dial-up connections for Internet/intranet connectivity.

2. Nokia 9210 Communicator Internet Features

2.1 Basic Features

- Normal single-slot GSM data calls using either 9600 bps or 14400 bps
- High Speed Circuit Switched Data (HSCSD) multi-slot GSM data calls of maximum uplink/downlink speeds of 43200 bps/14400 bps or 28800 bps/28800 bps[1]
- Support for analog modem connections and ISDN V.110 and ISDN V.120 rate adaption protocols
- Point-to-Point Protocol as the data link level protocol, RFC 1661
- PPP link level authentication using the Password Authentication Protocol (PAP) or Challenge Authentication Protocol (CHAP), RFC 1334
- PPP link level compression using Stac LZS (modes 4 and 3), MPPC and Predictor compression methods, RFC 1974
- PPP callback using the Microsoft callback protocol (client supplied number, server supplied number), and PPP callback type 0 as specified in RFC 1570
- Internet Protocol Control Protocol (IPCP) extensions for Domain Name Service (DNS)
- Scripting language for automating login procedures, compatible with previous EPOC devices (such as Psion's Series 5 PDAs)
- Van Jacobson TCP/IP header compression, RFC 1144
- Secure Sockets Layer (SSL) version 3 and Transport Layer Security (TLS) version1 protocols

2.2 Nokia 9210 Communicator Internet Applications

The Nokia 9210 Communicator has several Internet applications. It has a Web browser, a WAP browser, and a mail client that can use the IMAP4 and POP3 remote mailbox protocols and SMTP for sending mail. For details on how to configure your servers to work with the Nokia 9210 Communicator, please see the corresponding Quick Guide.

In addition, the Nokia 9210 Communicator has a full-featured TCP/IP stack programming interface, so you can create your own Internet applications. See the Nokia 9210 Communicator Software Development Kit for details.

2.3 Setting Up Internet Connections

The Nokia 9210 Communicator uses an Internet access point (IAP) to connect to the Internet. The Internet access point contains all the information required to connect to a service provider. Please refer to the Nokia 9210

[1] The support for all data call features depends on the GSM network and the user's subscription to network services. The indicated speeds are theoretical maximum speeds. Please contact your network operator for details on how to activate the required GSM data services.

Communicator User guide for instructions on how to create new Internet access points. The following sections describe the technical details of the different settings.

WAP connections require extra information in addition to Internet access points, such as the WAP gateway address. This information is called the WAP access point.

2.3.1 Internet Connections

Preferred connection lists the IAP which is used by default in the Web browser.

If idle, stay online determines the time the data call is open if no other data traffic occurs than PPP/LCP EchoReqeust/EchoReply frames. Available selections are 2, 5, 10, and 60 minutes.

Show connection dialog is for the users who want to select the IAP to be used when calling out. If this field is set to "Yes", the connection dialog will be displayed every time a data call is opened and the application does not explicitly request a certain IAP. When the connection dialog is displayed, some other IAP can be selected instead of the default (preferred) IAP. If the connection dialog is disabled, all data calls are established using the preferred IAP unless the application explicitly selects the IAP to be used.

2.3.2 Enter Your Account and Connection Details

Connection name can be any string of characters like "Corporate Dial-in #1". The purpose of this field is to name the connection with user-readable names.

Phone number field is for the remote access server phone number. The number can be entered in the international form with the plus mark "+" preceding all numbers and the country code, or just in national form. Most access servers use the same phone number for analog and ISDN calls, but the connection method must be defined by the user when creating a new IAP (See Advanced settings/Data call).

Prompt password contains two options "Yes" and "No". If "Yes" is selected, the access server password is prompted when PPP authentication occurs. This feature is useful when using one-time-password systems, or as an added security measure (the password will not be stored in the device). If this option is set to "Yes" and login scripts are used, the password is prompted and placed in the login_pass$ variable before executing the script. If the option is set to "No", the password to be used will be taken from the password field.

Password and *Confirm password* fields are for storing the static access server password. The password must be entered in both fields to prevent typing mistakes.

2.3.3 Advanced Settings for IAP: Proxies

Use proxy server defines if a proxy is to be used for HTTP when using this IAP.

Port number is the port number of the proxy server. Proxy servers tend to run on ports 80, 8000, or 8080, but it depends on the configuration and can be any TCP port.

Proxy server contains the proxy server name or IP address.

No proxy for contains the domain names for which the proxy will not be used. Domain names are separated by semicolons. As an example, ".fi;.nokia.com" specifies that this proxy will not be used for the top-level domain .fi (Finland) or any of the hosts in the domain nokia.com.

2.3.4 Advanced Settings for IAP: Data Call (and High-Speed data options)

Connection type gives two alternatives for the connection type. The default for every IAP is “Normal”, which stands for a normal single time slot GSM data call. The connection speed can be either 9600 or 14400 bps, and in addition for analog calls autobauding is the third speed option. “High speed” selects the High Speed Circuit Switched Data (HSCSD) data calls. Higher transfer speeds are achieved by reserving multiple GSM time slots for a single user.

> **Note:** The 14400 bps speed for normal GSM data call and HSCSD services are not basic GSM data services. These services may not be available in all networks in all areas, and they may require a separate subscription. If the network does not support the call type, or it has not been enabled in the user's subscription, the data call may fail. Even the basic data call services may need to be subscribed to separately.

Remote modem type defines the connection method to be used. There are three alternatives available: Analog (for normal modems), ISDN v.110, and ISDN v.120. The GSM network and the remote access server or dial-in modem pool must support the selected connection method, otherwise the connection attempt will fail.

> **Note:** Analog (normal modem) connections are usually supported in all networks. The connection time (before the data call is established) is about 40 seconds for analog connections and 15 seconds for ISDN connections[2]. Maximum data speeds are 28800 bps for analog, 38400 bps downstream for V.110, and 43400 bps downstream with V.120. In addition, the data flow may be smoother when using ISDN connections. These restrictions are caused by the GSM network, and are not inherent to the Nokia 9210 Communicator.

Max. connection speed is for determining the maximum connection speed. The GSM network may change the current connection speed at its discretion, for example when the network becomes congested.

> **Note**: All HSCSD connections are always made with a 14400 bps per time slot. This speed is almost always available in the areas where network coverage is good and the network supports HSCSD. If the network signal quality gets weaker, the speed is automatically downgraded to 9600 bps per time slot by the GSM network. The network can also decrease the number of time slots allocated for a user if network congestion occurs. These actions may cause fluctuations in the data rate, and may cause the total data rate to be lower than the requested data rate.

[2] These times are rough estimates, and depend on the network coverage, on the Internet service provider, and on other variables.

Available connection speeds are:

Connection type	Remote modem type	1 time slot	2 time slots	3 time slots
Normal data call	Analog	Autobauding, 9600, 14400	Not available	Not available
	ISDN V.110	9600 or 14400	Not available	Not available
	ISDN V.120	9600 or 14400	Not available	Not available
High-speed data call	Analog	9600-14400	19200-28800	Not available
	ISDN V.110	9600-14400	19200-28800	28800-38400
	ISDN V.120	9600-14400	19200-28800	28800-43200

When HSCSD connections are used, the user may control how many time slots are used for the connection. Some GSM operators may charge on a slot amount usage basis, while other GSM operators may implement a fixed charging model for HSCSD calls. Please contact your network operator for HSCSD coverage and charging details.

Modem init string is empty by default, but any valid GSM AT command can be typed here (start the string with "at"). AT strings are used to configure the internal modem of the Nokia 9210 Communicator. If you experience problems when creating data calls, please contact your GSM network operator or Internet service provider, who may provide a suitable configuration string for this setting.

2.3.5 Call Back

Today it is very important to have the best available security in Internet connections. One feature to increase security in the Nokia 9210 Communicator is support for call back on a PPP link. The other advantage of the call back is to control phone costs of mobile terminals.

When using call back in the Nokia 9210 Communicator, call back is requested during PPP negotiation. After negotiating call back, the remote server should close the connection and call back within one minute (60 seconds) using the same connection rate which was used to connected to the call back server.

There are three call back modes available:

- IETF PPP callback with a server-specified number (type 0)
- Microsoft Callback with a server-specified number
- Microsoft Callback with a client-supplied number

Use call back is used to set call back feature on or off. If this is set to "Yes", the callback will be negotiated during the PPP link configuration phase.

Call back type contains three alternatives. The first two options (MS call back and IETF call back) will use server number call back, meaning that the call back number is stored in a database on the remote server. The remote server finds the correct call back number after the client has authenticated itself to the server.

If the *call back type* is “Use number below”, the user must define the number where server will call back. It is suggested that the server checks the authentication credentials before calling the number, in order to avoid misuse.

Call back number is the number to which callback is requested when “Use number below” is selected as the *call back type*.

Note that the incoming callback data call (from the dial-up server to the Communicator) is expected to use the same data call parameters (normal or high speed call, analog or ISDN call) as the outgoing callback-requesting call (from the Communicator to the dial-up server). The GSM network and the dial-up systems must support this call type in both directions.

2.3.6 Other settings

The *Other* settings pages contains miscellaneous settings which may have to be defined to make successful Internet connections.

Allow plain text login determines the PPP authentication method. If it is set to “Yes”, the Password Authentication Protocol (PAP) is enabled. When PAP is used, the authentication password is passed to the remote server in cleartext. Setting this to “No” will activate Challenge Authentication Protocol (CHAP), which will use a challenge-response authentication protocol and the password itself will not be transferred over the PPP connection. It is advisable to configure the server to accept CHAP for increased security. Note that if CHAP is not supported on the server and the client is set to use it, the login will fail and the data call will be dropped as the communicator will not try to fall back to PAP for security reasons. On the other hand, if PAP was enabled, the server may opt to use CHAP instead.

Use PPP compression switch is used to control the PPP level data compression. In most cases compression will be used, but if the connection is unreliable or it fails, this is recommended to be switched off. Compression will usually speed up the data transfer. For some forms of data which cannot be compressed (pictures, previously compressed files or encrypted data), compression may not have the desired effect.

The supported compression methods are Stac LZS, Microsoft Point-to-Point Compression, and Predictor, and they are negotiated in this order. If the communicator and the remote access server do not agree on the compression method, no compression is used.

2.3.6.1 Script Options (in Other Settings)

Script options is used for selecting and editing the login script to be used.

If *Use login script* is set to “Yes”, a specified script is run after the data call has been established and before the PPP negotiation. Scripts can be used to authenticate the user on systems which do not support PPP authentication, and to start PPP on terminal servers which do not start it by default. Documentation for scripting syntax will be made available through Forum Nokia (http://www.forum.nokia.com/).

If *Display terminal window* is set to “Yes”, a terminal window is opened after the data call establishment which allows the user to see the script execution. If there is a “READ” command in the script, the user can type information in the window that will be sent to the remote host. The scripting and terminal window always use 8 data bits, none parity, one stop bit.

2.3.6.2 Address Options (in Other Settings)

Get IP address automatically enables dynamic IP addresses. The remote PPP server will provide the IP address for the communicator during PPP link negotiation. If this option is turned off, the IP address of the communicator must be defined manually before the connection. Most dial-up servers make use of dynamic IP addresses, as this gives a better utilisation of the restricted IP address space and contributes to better security.

IP address field contains a fixed IP address for the communicator and it stays the same for every connection using this IAP. This field can not be edited if automatic IP address configuration is used.

Get DNS address automatically enables automatic Domain Name Server IP address configuration from the access server. If this is switched off, DNS addresses must be defined manually. Not configuring the DNS IP addresses will cause the communicator to be unable to connect to servers by using their domain names.

Primary DNS address and *Secondary DNS address* fields are for manually defined Domain Name Server IP addresses.

2.4 Remote Configuration of Internet Settings

The most important Internet access settings can be configured by sending a short message (SMS) to the device. This enables the Internet access provider to configure the customer's communicator without manually entering all settings.

The messages are compatible with those of the Nokia 9110 Communicator, with some exceptions. For a description of remote configuration messages, please see the Nokia 9210 Communicator *Remote Configuration Guide*.

2.5 Secure Internet Connections

2.5.1 Secure Sockets Layer and Transport Layer Security

The Nokia 9210 Communicator supports the Secure Sockets Layer (SSL) version 3 and Transport Layer Security (TLS) version 1 protocols. These protocols can be used to secure the connections to remote mailboxes, connections to mail server while sending mail, and when connecting to Web servers. Software developers can use the SSL/TLS capabilities through the EPOC socket interface for their own purposes. Note that TLS is not available in the Web browser due to bugs in certain Web server implementations. The Web browser only uses SSLv3. There are no security implications.

When using SSL or TLS to secure mailbox access or mail sending, the mail server must support TLS negotiation during the IMAP or SMTP connection (the STARTTLS directive). Please refer to the *Setting Up E-Mail Service* document for details on how to use this feature.

Connections always default to TLSv1, and if the server does not support TLSv1, the connection is downgraded to SSLv3. In some rare cases, the SSL server will fail during SSL handshake when TLS is negotiated. This is the problem with some SSL servers. If this is the case, please contact your SSL server vendor for a fix.

2.5.1.1 Supported Algorithms

The selection of algorithms depends on the used protocol. It is advisable to avoid the use of "export-grade" algorithms (RC4 with 40 secret bits and DES) for security reasons. The Nokia 9210 Communicator supports the following cryptographic algorithms in SSL/TLS:

For server authentication and/or key exchange: RSA, DSA, and Diffie-Hellman. For data encryption: RC4™ (plus the "export" version with 40 secret bits), DES, and Triple-DES. (For WTLS in the WAP browser, RSA and RC5™ are supported.)

2.5.2 Certificate Management

SSL, TLS and software installation use certificates to authenticate remote peers. The Nokia 9210 Communicator supports X.509 certificates, both RSA and DSA keys. The user can specify whether the certificate is trusted and for what purposes the certificate is trusted. Certificates can be imported to the device by downloading them from the Web, in mail attachments, etc. New 3rd party applications can register themselves for the certificate management and can use the services provided by the certificate management, such as certificate chain validation and storage.

The Nokia 9210 Communicator contains some factory-installed root certificates of popular certification authorities and Nokia itself. You may wish to get your server certificate from one of these certification authorities, or you can install a new root certificate to the communicators. Users can freely delete certificates from the device. The certificate store is contained in ROM and removing the certificate database will revert to factory configuration.

Installation of new certificates is done using a DER encoded (binary) X.509 certificates (PEM or base64 encoding is not accepted). The user can view the details of a new or already installed certificate, such as the issuer name, subject name, validity period, serial number, and the fingerprint. The fingerprint can be used to verify the certificate's authenticity by out-of-band means.

To find out more about certificates and how they are used in secure communications, please refer to any good textbook on the subject, for example *Applied cryptography: Protocols, algorithms, and source code in C, 2nd edition* by Bruce Schneier.

2.6 Tested Nokia 9210 compatible PPP access servers

This section contains a list of commonly used PPP dial-in access servers which have been compatibility tested with the Nokia 9210 Communicator. Another type of PPP server may also work, assuming the server has been configured with generally used PPP settings such as:

- The PPP server is capable of establishing data calls using the PSTN/ISDN V.110/ISDN V.120 method
- The server is able to handle a maximum transfer unit (MTU) of at least 1500 octets
- Login script authentication with terminal server or PAP/CHAP authentication with PPP server
- Van Jacobson TCP/IP header compression on/off
- Dynamically/manually set IP and DNS addresses
- PPP compression provided by Compression Control Protocol on/off
- IP packet routing gateway information is set by the PPP server

The configuration options listed above may differ for your local Internet access point. Please contact your local ISP or corporate information management to get more information about used parameters for your Internet access point.

Compatibility tested PPP servers:

Cisco AS5300

Cisco AS5200

Shiva Access Switch

Shiva LanRover E+

Microsoft NT RAS 4.0

Ericsson Tigris AXC 623

Ascend Max 4004

Lucent PortMaster 3

Nortel/Bay Networks Versalar 8000

Morning Star PPPD

Various Linux/Unix based PPP daemons conforming RFC 1661.

3. Appendix A: Default Parameters and Settings

Async Control Character Map (ACCM) 0x00000000

Dynamic protocol timeout for LCP, IPCP, CCP, PAP, and CHAP 3 seconds

Maximum Receive Unit (MRU) 1500

Magic number negotiation is on

Address and Control field Compression is on

Maximum configure request restart 10

Maximum configure Naks before failure 5

Link quality report interval 10 seconds

Compression method negotiation order (PPP compression on by default):

- Stac LZS mode 3
- Stac LZS mode 4
- Microsoft PPC
- Predictor 1

PPP callback is off

TCP/IP-header Van Jacobson compression on

TCP maximum segment size (MSS) 536 bytes

Maximum time-to-live (TTL) 64

Default PPP idle timeout is 2 minutes

Show connection dialog is off

Proxy servers are off by default

Default data call parameters are normal analog data calls, autobauding and no AT commands

Plain text login is allowed by default

Login scripts are not used by default

IP addresses and DNS addresses are requested dynamically from server by default

For SSL and TLS, a collection of well-known certification authorities' root certificates has been installed and marked as trusted