TELNET SETUP GUIDE

This manual lists the Telnet commands supported by the Monarch® 9485 printer.

Use this information to configure the print server using Telnet. You must have a basic understanding of Telnet commands. For initial setup, do not use Telnet. Use auto-discover mode. Once you have the IP address, you can use Telnet or a Web browser.

The default port is Port 23.

To access Telnet console mode:

1. Start Telnet.
2. Type **auth admin admin** (on your host) and press **Enter**.
3. Configure your printer as required via Telnet.

Conventions

This manual uses the following conventions:

<ASCII Text> literal ASCII character string without delimiters (no spaces or tabs).

<integer> value represented as a decimal integer or as “asciihex” value in the form 0xhhh…hhh.

<asciihex> one or more pairs of hexadecimal digits with no prefix in the form hhh…hhh.

<portid> an I/O port bit number, from 0 to 7.

<IPadrs> Internet Protocol address string in the format: nnn.nnn.nnn.nnn; for example: 192.0.192.0.

N Numeric digits are indicated by the letter (n). For example,
wl-chan nn
wl-chan 11

Monarch® is a registered trademark of Avery Dennison Corporation.

Settings

1. To view the current wireless settings, type **wl-info** (show network settings) and press **Enter**:

```
Module Firmware Version:    3.23
Radio Firmware Version:     3.1.64.33
Link Status:                Connected
SSID:                       Sewoo_5ghz
MAC Address:                000B2805C877
BSSID:                      E0469A6F44E7
Transmit Rate (Mb/s):       65
Signal Level (dBm):         -63
Noise Level (dBm):          -96
IP Address:                 192.0.192.0
Subnet Mask:                255.0.255.0
Default Gateway:            192.1.192.1
Primary DNS:                210.0.210.0
Secondary DNS:              210.1.210.1
Up Time (Sec):              783
```

2. To change the SSID, type **wl-ssid ssid** and press **Enter**.
3. To set the IP address, type **wl-ip 192.0.192.0** and press **Enter**.
4. To set the subnet mask, type **wl-subnet 255.0.255.0** and press **Enter**.
5. To set the gateway, type **wl-gateway 192.1.192.1** and press **Enter**.
6. Type **commit** and press **Enter** to save the settings.
7. Type **restart** and press **Enter** to restart the unit.

Setting Up the Printer for LPD/LPR

LPD/LPR commands are only available with the new radio in these model printers: M09485NPMNA, M09485NPMEU, M09485NPMAP, M09485NPCNA, M09485NPCEU, and M09485NPCAP.

LPD/LPR Commands

lpd-enable [0(disable)/1(enable)]

Enables or disables the LPD protocol. The default is 1.

lpd-spool-name [ASCII Text string]

Sets the LPD spool name. The default is lp1.

1. Start Telnet. Telnet to the printer.
2. Type **auth admin admin** (on your host) and press **Enter**.
3. Type **lpd-enable 1** and press **Enter**.
4. Type **lpd-spool-name TEST** and press **Enter**.
5. Type **commit** and press **Enter**.
6. Type **restart** and press **Enter**.

General Commands

All CLI commands are terminated with a <CR>.

exit

Exits console mode.

restart

Restarts the radio (reinitializes the radio). Resets all system configuration parameters to defaults unless those parameters were saved using the **commit** command. Wireless connections are also lost (disconnected).

commit

Saves configuration settings.

reset

Sets print server to factory defaults.

save

Saves all user uploaded certificates, private keys, and configuration files to flash.

Use the **save** command after uploading files, or any files uploaded after the last save command, are lost and must be uploaded after the next restart or power cycle.

802.11a/b/g/n Wireless Commands

wl-type [a | p | u | m]

Configures the wireless interface operation type.

a Infrastructure mode. Configures the radio as a client, which talks to an Access Point.

p AdHoc mode. Used for peer-to-peer communications.

u AdHoc mode with unique SSID generated (based on MAC address).

m Access Point. Used to operate as a WiFi cell master. When using AdHoc mode, the static IP addresses are required. If the radio is configured as an Ethernet Bridge, the wireless IP address (**wl-ip**) must match the IP address of the device connected to the Ethernet port.

wl-band-pref [auto | 2.4 | 5]

Configures the preferred radio operation frequency band.

Note: This command is not applicable in Access Point mode. The **wl-chan** sets which **wl-band-pref** is used (2.4 or 5).

In AdHoc mode, the **wl-chan** takes precedence. Adjust the **wl-band-pref** to include the selected channel’s band.

auto Scans both the 2.4 GHz and 5 GHz bands for access points.

2.4 Only scans the 2.4 GHz band.

5 Only scans the 5 GHz band.

wl-rts-threshold

Sets the packet size (in bytes) threshold for the WLAN interface to use the 802.11 RTS/CTS mechanism. The range is 0 - 1500.

wl-rate [0(auto)/1/2/5.5/6/9/11/12/18/24/36/48/54]

Sets the 802.11a/b/g/n wireless speed in megabits per second (Mpbs).

wl-tx-power [5-15]

Reduces the transmit power based on the percentage entered.

wl-ssid [ASCII Text string]

Applies the SSID used for 802.11 association. The SSID can be up to 32 characters. The default is any.

- In Infrastructure mode, the SSID controls which access point the module connects to and affects the module's roaming behavior.
- In AdHoc mode, the SSID defines the network name for the AdHoc devices.
- In Access Point mode, the SSID defines the network name that the Access Point uses. Only devices with the same SSIDs can connect to each other.

any In Infrastructure mode, the module associates with the Access Point that has the best signal quality. This setting is not valid for Access Point mode.

(other) In Infrastructure mode, the module associates with the Access Point matching the SSID that has the best signal quality. In Access Point mode, the Access Point uses this setting to define the network name of the cell.

wl-assoc-retries n

Sets the number of times of retries for an association. The range is 0 – 32. The default is 3.

wl-auth [auto/open/shared]

Configures the authentication type when WEP 64 or 128 is used.

auto authenticates using Open Key algorithm. This is the default.

open authenticates using Open Key algorithm.

shared authenticates using Shared Key algorithm.

wl-wpa-proto [auto | wpa | rsn]

Selects the preferred WPA protocol used for authentication. Selecting a specific protocol (WPA or RSN) increases the roaming speed.

auto Device negotiates the protocol to be used for WPA.

wpa Uses WPA (TKIP) for the protocol.

rsn Uses RSN (WPA2) for the protocol.

wl-chan nn

Sets the 802.11a/b/g/n wireless channel.

wl-security [disable | wep64 |wep228 | wpa-psk | wpa-leap | wpa-leap64 | wpa-leap228| wpa-psk64 | wpa-psk128 | wpa-psk128-tkip |wpa2-psk | wpa2-psk-tkip | tls | ttls | peap | wpa-fast | wpa2-fast | leap-wep]

Selects the Wireless Security Method for authentication and encryption.

disable	Security is disabled. This is the default.
wep64	WEP, 64-bit key length (referred to as 40-bit WEP or WEP-40)
wep228	WEP, 128-bit key length (referred to as 104-bit WEP or WEP-104)
wpa-psk	WPA Pre-Shared Key
wpa-leap	WPA CISCO LEAP
wpa-leap64	Migration mode w/ Cipher suite TKIP+40-bit WEP using EAP (LEAP). Requires LEAP username and password.
wpa-leap228	Migration mode w/ Cipher suite TKIP+128-bit WEP using EAP (LEAP). Requires LEAP username and password.
wpa-psk64	Migration mode w/ Cipher suite TKIP+40-bit WEP using WPA PSK. Requires WPA Passphrase.
wpa-psk128	Migration mode w/ Cipher suite TKIP+128-bit WEP using WPA PSK. Requires WPA Passphrase.
wpa-psk128-tkip	Migration mode w/ Cipher suite TKIP and/or 128-bit WEP using WPA PSK. Requires WPA Passphrase.
wpa2-psk	WPA2 Pre-shared Key, also known as WPA2 Personal. Requires WPA Passphrase.
wpa2-psk-tkip	WPA2 Pre-shared Key with Group Cipher suite TKIP, also known as WPA2 Personal. Requires WPA Passphrase.
tls	WPA/WPA2 with EAP-TLS authentication, also known as WPA-Enterprise (TKIP/AES) and WPA2-Enterprise TLS
ttls	WPA/WPA2 with EAP-TTLS authentication, also known as WPA-Enterprise (TKIP/AES) and WPA2-Enterprise TTLS
peap	WPA/WPA2 with PEAP authentication, also known as WPA-Enterprise (TKIP/AES) and WPA2-Enterprise PEAP v0
wpa-fast	EAP-FAST with Cipher suite TKIP.
wpa2-fast	EAP-FAST with Cipher suite EAS-CCMP.
wep-leap	LEAP with WEP Encryption.

wl-def-key [1/2/3/4]

Sets which WEP key number to use. The default is 1.

wl-key-1, wl-key-2, wl-key-3, wl-key-4 [WEPkey]

Sets the WEP key value. This value must be hexadecimal.

pw-wpa-psk [ASCII Text string]

Configures the Pre-Shared Key used with WPA-PSK security. The input range is 8 to 63 ASCII characters or 64 hex characters. This key must match the key on the Access Point.

eap-anon-ident [text string]

Sets the anonymous identity string for EAP. The maximum length is 64 ASCII characters.

Used as the unencrypted identity with EAP types that support different tunneled identity, e.g., EAP-TTLS. A typical format is shown here: anonident@example.com.

ca-cert-filename [ASCII Text: CA filename.extension]

This command defines the Certificate Authority (CA) filename to be used with the chosen authentication method. The certificate can contain one or more trusted CA certificates. A trusted CA certificate should always be configured when using EAP-TLS, EAP-TTLS or PEAP. The file must be in PEM or DER format for the device server to recognize it as a valid certificate.

client-cert-filename [ASCII Text: filename.extension]

This command defines the Client certificate filename to be used with the chosen authentication method. A client certificate should always be configured when using EAP-TLS. The file must be in PEM or DER format for the device server to recognize it as a valid certificate.

priv-key-filename [ASCII Text: filename.extension]

This command defines the Client Private Key filename to be used with the chosen authentication method. The file must be in PEM or DER format for the device server to recognize it as a valid private key.

Note: When PKCS#12/PFX files are used, the **ca-cert-filename** command should not be used.

priv-key-password [ASCII Text: password]

This command defines the Client Private Key password to be used with the Private Key file identified by the **priv-key-filename** command. The private key is an ASCII text string provided by the generator of the Private Key file.

eap-fast-max-pac-list n

Defines the maximum number of RADIUS servers for which EAP-FAST PAC provisioning is maintained. This is an integer with a range of 1-255 entries. The default is 10.

eap-fast-provisioning [unauthenticated | authenticated | either]

Defines the method by which EAP-FAST credentials (PAC) can be provisioned between the module and a RADIUS server.

unauthenticated The server’s identity is not validated before the credentials are provisioned.

authenticated The server’s identity is validated before the credentials are provisioned. It requires **ca-cert-filename** to be configured and the certificate loaded to the radio. If this is not done, the setting behaves as unauthenticated.

either Instructs the module to use authenticated, if possible; otherwise, use unauthenticated.

eap-ident [text string]

Sets the identity string for EAP which is typically the RADIUS server user login name. The maximum length is 64 ASCII characters.

eap-password [ASCII Text String] or [32hex Digits]

Sets the password string for EAP. The maximum length is 64 ASCII characters. This field can include either the plaintext password (using ASCII or hex string) or a NtPasswordHash (16- byte MD4 hash of password) in hash:<32 hex digits> format.

NtPasswordHash can only be used when the password is for MSCHAPv2 or MSCHAP (EAP-MSCHAPv2, EAP-TTLS/MSCHAPv2, EAP-TTLS/MSCHAP, LEAP). EAP-PSK (128-bit PSK), EAP-PAX (128-bit PSK), and EAP-SAKE (256-bit PSK) is also configured using this field.

For EAP-GPSK, this is a variable length PSK.

eap-phase1 [peaplabel=0 | peaplabel=1| peapver=0 | peapver=1 | peap_outer_success=0 | include_tls_length=1| result_ind=1 | crypto_binding=0 | crypto_binding=1 | crypto_binding=2]

Phase1 (outer authentication, i.e., TLS tunnel) parameters:

peaplable=0 Forces a new label to be used during key derivation when PEAPv1 or newer is used.

Most server PEAPv1 implementations use the value: peaplabel=1 which forces a new label to be used during key derivation when PEAPv1 or newer is being utilized. Some servers may require this setting for use with PEAPv1.

peapver=0 Forces use of PEAPv0.

peapver=1 Forces use of PEAPv1.

peap_outer_success=0 Terminates PEAP authentication on tunneled EAP-Success. This is required with some RADIUS servers that implement draft-josefsson-pppext-eap-tls-eap-05.txt (e.g., Lucent NavisRadius v4.4.0 with PEAP in "IETF Draft 5" mode).

include_tls_length=1 Forces supplicant to include TLS message length field in all TLS messages even if they are not fragmented.

result_ind=1 Enables EAP-SIM and EAP-AKA to use protected result indication.

crypto_binding=0 Do not use Crypto Binding for PEAPv0.

crypto_binding=1 Use Crypto Binding for PEAPv0, if the server supports it. This is the default.

crypto_binding=2 Requires Crypto Binding for PEAPv0.

eap-phase2 [auth=MSCHAPV2 | autheap=MSCHAPV2 | autheap=MD5]

Phase2 (inner authentication used with TLS tunnel) parameters.

auth=MSCHAPV2	Sets the inner encryption to MSCHAPv2. This is required for EAP-PEAPv0 or EAP-PEAPv1.
autheap=MSCHAPV2	Sets the inner encryption to MSCHAPv2. This required for EAP-TTLS/MSCHAPv2.
autheap=MD5	Sets the inner encryption to MD5. This is required for EAP-TTLS/MD5.

user-leap [ASCII Text string]

Configures the WPA-LEAP username. The LEAP username must match the LEAP password assigned to the LEAP user on the LEAP server. The LEAP username is 1 to 32 characters in length and cannot contain spaces.

pw-leap [ASCII Text string]

Configures the WPA-LEAP password. The LEAP password must match the LEAP password assigned to the LEAP user on the LEAP server. The LEAP password is 1 to 32 characters in length and cannot contain spaces.

wl-region [countrycode]

Sets the print server's region of operation using the following table.

County Code	Description	County Code	Description	County Code	Description
AT	Austria	GB	Great Britain	MY	Malaysia
AU	Australia	GR	Greece	NL	Netherlands
BE	Belgium	HK	Hong Kong	NO	Norway
BR	Brazil	HU	Hungary	NZ	New Zealand
CA	Canada	ID	Indonesia	PH	Philippines
CH	Switzerland	IE	Ireland	PL	Poland
CN	China	IL	Israel	PT	Portugal
CY	Cyprus	IN	India	SE	Sweden
CZ	Czech Republic	IS	Iceland	SI	Slovenia
DE	Germany	IT	Italy	SK	Slovak Republic
DK	Denmark	JP	Japan	SG	Singapore
EE	Estonia	KR	Korea	TH	Thailand
ES	Spain	LT	Lithuania	TW	Taiwan
FI	Finland	LU	Luxembourg	US	United States
FR	France	LV	Latvia	ZA	South Africa

stats

Shows the network I/O statistics.

TCP/IP Commands

wl-dhcp [0(disable)/1(enable)]

Sets the method of getting the IP address as [0(static)/1(dhcp)].

wl-ip [IPadrs]

Sets the print server's IP address.

wl-gateway [IPadrs]

Sets the default Router/Gateway address (or access point).

wl-subnet [IPadrs]

Sets the default subnet mask.

wl-tunnel-port [integer]

Sets PORT9100 port.

http-port [disable | enable]

Enables or disables the HTTP protocol.

ping [IPadrs]

Sends IP ping packets to test the host connection.