

Issued: July 5, 2004



Network Security White Paper

ver.B.1.0

Concerned Products:

Model J-P3

Model PL-P1

Notice :

THIS DOCUMENT MAY NOT BE REPRODUCED OR DISTRIBUTED IN WHOLE OR IN PART, FOR ANY PURPOSE OR IN ANY FASHION WITHOUT THE PRIOR WRITTEN CONSENT OF RICOH COMPANY LIMITED. RICOH COMPANY LIMITED RETAINS THE SOLE DISCRETION TO GRANT OR DENY CONSENT TO ANY PERSON OR PARTY.

Copyright © 2004 by Ricoh Company Ltd.

All product names, domain names or product illustrations, including desktop images, used in this document are trademarks, registered trademarks or the property of their respective companies. They are used throughout this book in an informational or editorial fashion only. Ricoh Company, Ltd. does not grant or intend to grant hereby any right to such trademarks or property to any third parties. The use of any trade name or web site is not intended to convey endorsement or any other affiliation with Ricoh products.

Although best efforts were made to prepare this document, Ricoh Company Limited makes no representation or warranties of any kind with regards to the completeness or accuracy of the contents and accepts no liability of any kind including but not limited to performance, merchantability, fitness for any particular purpose, or any losses or damages of any kind caused or alleged to be caused directly or indirectly from this document.

T

Version history :

Version	Issue Date	Revised item
B.1.0	Jul. 5, 2004	1 st release

The following terms are used in this document. Please familiarize yourself with them.

Terms:

the products: This refers to the digital multifunction and printing devices covered by this document, as noted in the Model Cross Reference table. “the products” refers to all of these machines collectively.

Host Interface: The physical interface of the Ethernet board on the products.

Model Cross Reference:

Model Name	Product Code	Brand					
		Ricoh	Savin	Gestetner	Lanier	NRG	infotec
Model J-P3	G106	Aficio CL7100	Savin CLP35	Gestetner C7435n	Lanier LP235c	NRG C7435n	IPC 3535
Model PL-P1	G108	Aficio CL1000N	Savin CLP831	Gestetner P7431cn	Lanier LP031c	NRG P7431cn	-

Table of contents

- 1 Introduction
- 2 Embedded services and potential security issues
 - 2.1 telnet
 - 2.2 ftp
 - 2.3 http
 - 2.4 snmp
 - 2.5 shell (rsh/rcp)
 - 2.6 lpd
 - 2.7 ipp
 - 2.8 diprint (RAW print)
 - 2.9 nbt
 - 2.10 mdns
 - 2.11 https
 - 2.12 Others
- 3 Appendix
 - A) The list of services provided with open TCP/UDP ports
 - B) Related Protocols
 - C) The purpose of Access Control
 - C)-1. Web Image Monitor
 - C)-2. mshell
 - D) How to disable services
 - D)-1. Web Image Monitor
 - D)-2. mshell
- 4 Reference List

1 Introduction

This document describes potential network threats and recommended precautions for them. The products have built-in network services for providing a variety of features for network clients, such as network scanning, printing or faxing, and also client services for accessing network servers running outside the products, such as an LDAP server, NetWare server, or Mail server.

This document focuses on how-to protect against potential threats from external attacks.

As the products are designed for use inside an Intranet where network clients and servers are protected by firewalls, the products rely on the Intranet's security policy, like the security provided by other network servers and clients. However, some customers require more strict security levels for network devices, because potential threats from inside the firewalls are increasing, and some configurations even use a secure connection to the Internet as a part of the Intranet.

To satisfy these demands, the products are all evaluated by security scanning applications during development, and also are checked for known vulnerability issues reported by Internet security organizations, such as CERT Coordination Center (CERT/CC : <http://www.cert.org/>). Whenever we find security vulnerabilities in the products, we provide appropriate countermeasures.

2 Embedded Services and Potential Security Issues

Some server services allow write access from network clients. Because of this, some customers may feel that the products are insecure against viruses, worms, or intruder accesses. The products are secure against such attacks and provide security measures against potential threats to specific services, but some of these measures can make the services unavailable. For example, disabling the LPD port will make the products unavailable for LPR clients.

To avoid such inconvenience, specifying an Access Control list of “safe” client host addresses is strongly recommended. Once you set up Access Control for specific IP addresses, the products will receive print or scan requests from the specified hosts only. This Access Control is applied for lpd printing, rcp/rsh access, http/https access, ftp printing, TCP raw printing (diprint), ipp printing, and scanning from DeskTopBinder. For information on how to set up access control, refer section 3.C) of the Appendix.

In the following sections, the potential threats and recommended precautions are given for each service. The recommended precautions should be accompanied by a firewall and restricted by Access Control.

2.1. telnet

2.1.1. Function Overview

The telnet service provides a virtual terminal service in order to use the maintenance shell (mshell). It is compliant with RFC 854. The mshell uses tcp port 23 and provides a dedicated command interface for the following functions.

- Configuring network settings of the products from remote terminals
- Monitoring device status and settings from remote terminals
- Getting system logs from remote terminals

Unlike shell services for UNIX/Linux, the mshell provides a command interface for configuration purposes only. Access to the file system or kernel, or modifying system files inside the products is not possible.

When logging into the mshell, the user must enter a correct password (The default password is "password" but this is changeable.).

2.1.2 Potential threats and recommended precautions

1) Destruction, corruption and modification of the file system and kernel.

There is no possibility of destruction, corruption or modification of the file system.

The mshell permits write-access to network parameters only and no one can access the file system or kernel.

2) Possibility of acting as a server for relaying viruses.

There is no possibility that the products will be used by viruses as an open relay server, because unrecognized data is disregarded. Also, neither the local file system nor remote host can be accessed via the mshell.

3) Theft of password

When accessing the mshell, the password is sent in clear text. Because the telnet protocol itself does not support encryption. So if the password is intercepted by a packet sniffer, the possibility of unauthorized access and changes being made does exist.

4) Recommended precautions

The following are suggested precautions against threats to the embedded telnet service.

The levels described below indicate the level of security (Level 1 is lowest). Please take the appropriate action for your security policy.

Level 1: Change the password from the default value to something difficult to guess and change it regularly.

- The password is the same as the one for logging into Web Image Monitor in Administrator mode. So, changing the password for the mshell means changing it for Web Image Monitor's Administrator mode.

Level 2: Close the telnet port.

- The telnet port can be completely closed using the mshell. When telnet is disabled, the services provided by the mshell will no longer be available. A Memory clear by a customer engineer is required in order to start the telnet service again.

2.2. ftp

2.2.1. Function Overview

The ftp (File Transfer Protocol) service provides the function of receiving data with reliability and efficiency. This service is compliant with RFC 959. tcp port 20 is used for ftp-data service and tcp port 21 is used for ftp-control service. The ftp client must be compliant with RFC 959.

The following functions are provided by the ftp service.

- Receiving print jobs from ftp clients
- Providing the following files to ftp clients

File name	Description	Attribute
Syslog	System log information	Read-only
Install	Install Shell script	Read-only
Stat	Printer Status	Read-only
Prnlog	Print log information	Read-only
Info	Printer Information	Read-only
Help	Help	Read-only
<i>Fax application files (hidden)</i>	Fax job log information Fax counter Fax address book	SmartDeviceMonitor for Admin/Client is required to read/ manage these files.

- Receiving firmware files from remote clients.

Note: Only Service Technicians can add firmware to the ftp server. In addition, some of the products do not have this function.

2.2.2 Potential threats and recommended precautions

1) Destruction, corruption and modification of the file system.

There is no possibility of destruction, corruption or modification of the file system.

Although the ftp service permits write-access, any files that are received by the printer are considered to be a print job or firmware data. When the embedded ftp server receives an executable file, the product prints a binary representation (garbage characters) of the data contained in the executable. As for firmware, a dedicated account and password that are disclosed only to Service Technicians is required to input firmware to the printer using the ftp service. In addition, data is verified by checking the header, IDs and the file format before being used. It is impossible to make a pseudo firmware file to destroy the file system.

2) Possibility of acting as a server for relaying viruses.

There is a possibility of accessing other hosts through the products by using the PORT command. This is known as "FTP bounce attack" (see:

<http://cgi.nessus.org/plugins/dump.php3?id=10081> for more information). To prevent this type of attack, please close the ftp port.

3) Possibility of successful DoS (Denial of Service) attack

There is a possibility of coming under hostile DoS attack when using the PASV command (see: <http://cgi.nessus.org/plugins/dump.php3?id=10085> for more information). If the FTP server continues to receive the PASV command, other FTP connection requests will be refused. In order to recover the status of the products, rebooting is required. To prevent this vulnerability, please close the ftp port.

4) Theft of password

When accessing the FTP service, the user name and the password are sent in clear text because the ftp protocol itself does not support encryption. However, this does not present a major security risk because no changes can be made to the system via ftp. In fact a password is not even necessary to input when logging onto an ftp session except for updating the firmware. When putting firmware data onto an ftp server, a dedicated account and password are required and they are disclosed to only Service Technicians. There is no possibility of destruction of the file system from someone using a sniffed account and password because it is impossible to make a pseudo firmware file to destroy the file system.

5) Recommended precaution

As stated earlier, the suggested precaution against the threats to the embedded ftp service is closing the ftp port if you maintain a strict security policy. The port for this service can be completely closed using Web Image Monitor or the mshell.

2.3. http

2.3.1. Function Overview

The http (Hypertext Transfer Protocol) service provides web services. This service is compliant with RFC 1945. tcp port 80 is used for the http service.

The following functions are provided by the http server service.

- Configuring machine settings via Web Image Monitor in Administrator mode
- Viewing machine settings and status via Web Image Monitor
- Managing files saved in the Document Server of the products via DeskTopBinder.
- Managing user information and retrieving counter information when using User Management Tool in SmartDeviceMonitor for Admin/Client
- Managing the Product's address book when using Address Management Tool in SmartDeviceMonitor for Admin.
- Printing a job from an ipp client.
- Providing job status to an ipp client.

Note: When logging into Web Image Monitor in Administrator mode, the user must enter the password. It is the same as the password used for the mshell.

2.3.2 Potential threats and recommended precautions

1) Destruction, corruption and modification of the file system

There is no possibility of destruction, corruption or modification of the file system. Because no one can access the file system and executable files cannot be processed on the products web server.

2) Possibility of acting as a server for relaying viruses

There is no possibility that the products will be used by a virus as an open relay server. The web server was developed by Ricoh and does not allow any malicious and executable files to be processed.

3) Theft of password

When accessing Web Image Monitor, the password is sent with BASE64 encode. In this case, the password is not sent in clear text, but it is not particularly difficult to decode. Therefore, if the password is intercepted using a packet sniffed and then decrypted, the possibility of unauthorized access and changing of network settings does exist.

4) Recommended precautions

The following are suggested precautions against threats to http service. The levels described below indicate the level of security (Level 1 is lowest). Please take the appropriate

action for your security policy.

Level 1: Change the password from the default value to something difficult to guess and change it regularly.

- The password is the same as the one for logging in to the mshell. So, changing the password for Web Image Monitor's Administrator mode means changing it for the mshell as well.

Level 2: Disable web function.

- If it is not needed, Web Image Monitor can be disabled using the mshell. When web is set to 'Down', Web Image Monitor does not activate and the error "503 Service Unavailable" is displayed. Even when not in use, tcp port 80 stays open and is therefore http is available for ipp printing.

Level 3: Close the http port.

- The HTTP port can be completely closed with mshell. In this case, both Web Image Monitor and ipp (Internet Print Protocol) are unavailable via http. ipp printing provides printer access via http (`http://<printer host name or ip address>/... (an ipp function)`). If the HTTP port is closed, Web Image Monitor and ipp printing are still available via https.

Note: We recommend using https instead of http for Web Image Monitor and ipp printing.

2.4. snmp

2.4.1. Function Overview

SNMP (Simple Network Management Protocol) is used to communicate management information between the network management stations (SNMP manager), such as a PC running a management application, and the agents in the network (SNMP agent), such as printers, scanners, workstations or servers, routers and hubs. The SNMP service is embedded in the products, to provide a method of managing them on the network. This service is compliant with RFC 1157 for SNMP v1 and RFC 1902 for SNMP v2. udp port 161 is used for SNMP service and udp port 162 is used for SNMP-trap.

The following functions are available.

- Configuring the settings of the products.
- Monitoring the status of the products.
- Detecting errors affecting the products.
- Communicating with the client PC for Scanning using the TWAIN driver.

Although the SNMP service is not protected by a password, it is protected using unique community names and assigned access rights (read-only, read-write and trap) within those communities. You can only communicate with or configure an agent if it is a member of the same community and if the access rights allow you to get or modify data in the MIBs (Management Information Base) embedded in the products.

Default settings of SNMP community names are follows;

- Read-only : public
- Read-Write : admin

2.4.2. Potential threats and recommended precautions

Management hosts and agents belong to an SNMP community. An SNMP community is a collection of hosts grouped together for administrative purposes. Defining communities provides security by allowing only management systems and agents within the same community to communicate with each other. However community names are sent in clear text because of the specification of the protocol.

The suggested precautions against this threat are as follows. The levels described below indicate the level of security (Level 1 is lowest). Please take the appropriate action for your security policy.

Level 1: Change the community names from the default value to something difficult to guess and change it regularly.

- When the community name settings are changed in the agents, the community name settings in the management utilities must also be changed.

Level 2: Close the SNMP port

- If it is not absolutely necessary, the SNMP port should be closed via Web Image Monitor or the mshell.

2.5. shell (rsh/rcp)

2.5.1. Function Overview

Remote shell (rsh/rcp) services provide the following functions via tcp port 514.

- Printing jobs from rsh/rcp clients.
- Monitoring machine status and settings from rsh/rcp clients.
- Providing the print logs and the system logs to rsh/rcp clients.
- Transferring scan data to the Twain driver.

2.5.2. Potential threats and recommended precautions

1) Destruction, corruption and modification of the file system

There is no possibility of destruction, corruption or modification of the file system. Because no one can access the file system or kernel and executable files cannot be processed via the remote shell service

2) Possibility of acting as a server for relaying viruses

There is no possibility that the products will be used by a virus as an open relay server.

Although the remote shell service permits write-access, all written data are treated as print jobs. Even if someone sent an executable file via the embedded remote shell service, the products prints the file as garbage data.

3) Theft of user name

The user name is sent in clear text when using the remote shell service. If the user is concerned about this, the port for remote shell service can be completely closed via Web Image Monitor and mshell.

4) Recommended precaution

As stated above, there are not many threats that apply to the products. However, if you want to maintain a strict security policy, the rch/rcp service can be disabled and the port for this service can be completely closed using Web Image Monitor or the mshell.

2.6. lpd

2.6.1. Function Overview

The lpd service is one of the TCP/IP Printing Services known as LPD or LPR. This service is compliant with RFC 1179 and uses tcp port 515 for connection with a RFC 1179 compliant client. The following functions are provided by this service.

- Printing a job from lpr clients
- Monitoring the status of the printer and print queues from lpr clients.
- Deleting print jobs from the print queue by lpr clients.

2.6.2. Potential threat and recommended precaution

1) Destruction, corruption and modification of the file system

There is no possibility of destruction, corruption or modification of the file system or kernel because no one can access it via the lpd service.

2) Possibility of successful DoS (Denial of Service) attacks.

There is no possibility of successful DoS attacks.

When the products receive the data that does not meet the protocol specification, the products will stop the lpd service, and the executed application (if any), at regular steps.

3) Recommended precautions

As stated above, there are not many threats that apply to the products. However, if a strict security policy is to be maintained, the lpd service can be disabled and the port for this service can be completely closed using Web Image Monitor or the mshell.

2.7. ipp

2.7.1. Function Overview

The ipp (Internet Printing Protocol) service is used for Internet printing from ipp clients. This service is compliant with RFC 2565 and it uses tcp port 631.

The following functions are provided by the ipp service.

- Printing a job from an ipp client.
- Providing job status to an ipp client.

The ipp service has a user authentication function. 10 accounts are available for ipp service and the password can be set for each account. Both “BASIC” and “DIGEST” authentication are supported. “BASIC” authentication is common, but the user name and password are sent in clear text. “DIGEST” authentication is more secure with the user name and password irreversibly encrypted and the popularity of “DIGEST” authentication had been increasing at the time of this writing.

Both authentication methods are selectable in Web Image Monitor and mshell.

ipp authentication can also be disabled. In this case, usernames and passwords are not authenticated (The default setting is “disabled”).

2.7.2. Potential threat and recommended precaution

1) Destruction, corruption and modification of the file system

There is no possibility of destruction, corruption or modification of the file system because it can't be accessed via the ipp service in the products.

2) Possibility of successful DoS (Denial of Service) attacks

There is no possibility of successful DoS attacks.

When the products receive data that can carry out a DoS attack, a waiting period is implemented in the reply process of the products. This reduces the system load and stops the service and application at regular steps if data that falls outside of the specification of the protocol is present in the system.

3) Recommended precautions

As stated above, there are not many threats that apply to the products. However, if you want to maintain a strict security policy, we recommend the following precautions. The levels described below indicate the level of security (Level 1 is lowest). Please take the appropriate action for your security policy.

Level 1: Set ipp Authentication to either “BASIC” or “DIGEST” from “Disabled” in Web Image Monitor, the mshell or the operation panel.

- “DIGEST” authentication is more secure than “BASIC” because the username

and the password are not sent in clear text.

Level 2: Close the ipp (631/tcp) port.

- If it is not absolutely necessary, the ipp port should be closed via Web Image Monitor or the mshell.

Note: This only closes the ipp port. The ipp service is still available using http or https.

2.8. diprint (RAW print)

2.8.1. Function Overview

The diprint (Direct Print or RAW Print) service is Ricoh Company Ltd's name for port 9100 communication. This service provides direct printing from remote terminals using tcp port 9100.

2.8.2. Potential threat and recommended precaution

There are not many threats in this service because all written data is treated as a print job. Even if someone sent an executable file via the embedded remote shell service, the products prints the file as garbage data.

1) Recommended precautions

As stated above, there are not many threats that apply to the products. However, if you want to maintain a strict security policy, the diprint port can be changed and the port for this service can be completely closed using Web Image Monitor or the mshell.

2.9. nbt

2.9.1. Function Overview

The NBT (NetBIOS over TCP/IP) service provides the NetBIOS service over TCP/IP instead of NetBEUI. Using this service, a remote host can access network services of the products by the NetBIOS name (Computer Name) instead of IP address. This service uses 3 ports, udp port 137 for netbios-ns (NetBIOS Name Service), udp port 138 for netbios-dgm (NetBIOS Datagram Service) and tcp port 139 for netbios-ssn (NetBIOS Session Service). SMB (Server Message Block) over TCP/IP is provided by this service as follows.

- Browsing the print servers from SMB clients
- Printing a job from SMB clients
- Sending job queue information to SMB clients
- Sending notifications of a job completion to SMB clients

2.9.2. Potential threat and recommended precaution

1) Possibility of browsing the network by unauthorized parties

If you would not like the products to be browsed by unauthorized parties, the SMB service should be disabled using Web Image Monitor or the mshell.

2) Possibility of successful DoS (Denial of Service) attacks

There is no possibility of successful DoS (Denial of Service) attacks. Repeated access and disconnection to tcp port 139 is a well known DoS (Denial of Service) attack. The products are protected against this by accepting the connections sequentially. And also when the products receive data that can carry out a Dos attack, the connection with the sender will be disconnected.

3) Recommended precautions

As stated above, if you want to maintain a strict security policy and it is not absolutely necessary, the NetBIOS Session Service (139/tcp) can be disabled using Web Image Monitor (set SMB to disable) or the mshell (set SMB to 'Down'). When SMB is disabled, SMB over NetBEUI is also disabled. There is no method to disable only NetBIOS Session Service (139/tcp) without disabling SMB over NetBEUI. udp port 137 and 138 cannot be closed even if SMB is disabled.

2.10. mdns

2.10.1. Function Overview

mdns (Multicast DNS) is a way of using familiar DNS programming interfaces, packet formats and operating semantics, in a small network where no conventional DNS server has been installed.

the products only use mdns for rendezvous. If rendezvous is not being used, this port can be closed.

2.10.2. Potential threat and recommended precaution

Threats to this service are unlikely. mdns is only used for advertising services. No settings or commands can be sent using mdns.

1) Recommended precautions

As stated above, there are not many threats that apply to the mdns. However, if you want to maintain a strict security policy, the mdns port (5353/udp) can be completely closed using Web Image Monitor or the mshell. (If rendezvous is turned off, the mdns port is closed automatically.)

2.11. https

2.11.1. Function Overview

https is http over SSL (Secure Socket Layer). https provides the same functions as http.

https maintains higher security than http because SSL provides the following features:

- Server authentication/certification. (Protects against server spoofing.)
- Data Encryption. (Protects against wiretap/falsification.)

*About SSL

SSL is a communication technology used for secure connections between 2 hosts. The primary goal of the SSL Protocol is to provide privacy and reliability between two communicating applications. SSL is layered on top of some reliable transport protocol (e.g., TCP). SSL allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data.

2.11.2. Potential threat and recommended precaution

1) Destruction, corruption or modification of the file system

There is no possibility of destruction, corruption or modification of the file system. Because no one can access the file system and executable files cannot be processed on the products web server.

2) Possibility of acting as a server for relaying viruses

There is no possibility that the products will be used by a virus as an open relay server. The web server was developed by Ricoh and does not allow any malicious and executable files to be processed.

3) Possibility of attacker taking advantage of a heap corruption error in OpenSSL.

There is a possibility of causing a crash on the products by taking advantage of a heap corruption bug in the version of the OpenSSL used by the products. This heap corruption will result in a crash causing a DoS (Denial of Service) or will disable secure communications (HTTPS).

(see: <http://cgi.nessus.org/plugins/dump.php3?id=11875> for more information). To prevent this vulnerability, please close the https port.

4) Theft of password

When using https, all data including the password is encrypted using SSL. This is safer than sending passwords encoded in Base 64 (using the http).

5) Recommended precautions

The following are suggested precautions against threats to the https service. The levels

described below indicate the level of security (Level 1 is lowest). Please take the appropriate action for your security policy.

Level 1: Change the password from the default value to something difficult to guess and change it regularly.

- The password is the same as the one for logging in to the mshell. So, changing the password for Web Image Monitor's Administrator mode means changing it for the mshell as well.

Level 2: Disable web function.

- If it is not needed, Web Image Monitor can be disabled using the mshell. When web is set to 'Down', Web Image Monitor does not activate and the error "503 Service Unavailable" is displayed. Even when not in use, tcp port 443 stays open and is therefore https is available for ipp printing.

Level 3: Close the https port.

- The https port can be completely closed with mshell. In this case, both Web Image Monitor and ipp (Internet Print Protocol) are unavailable via https. If the https port is closed, Web Image Monitor and ipp printing are still available via http.

2.12. Others

Tcp port 7443 and 7444 are reserved for a remote service that we will launch in the future. This service accepts only a Ricoh-confidential protocol and it is impossible to emulate it without knowledge of the protocol specification. In addition, we will not disclose the protocol specification to anyone outside of Ricoh Company, Ltd.. As just described, there are no threats that apply to the products. However if a strict security policy is to be maintained, those ports can be closed in SP mode. SP mode for this service is mentioned in the service manual for each product.

https is used for this service as an underlying layer. Please refer to “2.11 https” section for the potential threats and recommended precautions for https.

3. Appendix

A) The list of services provided with open TCP/UDP ports

Protocol	Port Num.	Login	Default Username	Username Changeable	Password	Default Password	Password Changeable	Note
telnet	23/tcp	N/A	N/A	N/A	Y	password	Y	This is the same password as is used for Web Image Monitor.
ftp-control	21/tcp	Y	ANONYMOUS	N/A	N/A	N/A	N/A	
http	80/tcp	N/A	N/A	N/A	Y	password	Y	This is the same password as is used for telnet. If no password is input, then only read access is available.
netbios-ns	137/udp	N/A	N/A	N/A	N/A	N/A	N/A	
netbios-dgm	138/udp							
netbios-ssn	139/tcp							
snmp	161/udp	Y	RO: public RW: admin	Y	N/A	N/A	N/A	Although there is no concept of user accounts, it can perform access restrictions using the Community Name. Up to 10 Communities can be registered.
https	443/tcp	N/A	N/A	N/A	Y	password	Y	This is the same password as is used for telnet and http. If no password is input, then only read access is available.
rsh/rcp (shell)	514/tcp	N/A	N/A	N/A	N/A	N/A	N/A	
lpd	515/tcp	N/A	N/A	N/A	N/A	N/A	N/A	
ipp	631/tcp	Y	ANONYMOUS	Y	Y	N/A	Y	Authentication by account/password is not performed by default. In this case all users are ANONYMOUS. When ipp authentication is enabled, a username and password will be required.
mdns	5353/udp	N/A	N/A	N/A	N/A	N/A	N/A	

Protocol	Port Num.	Login	Default Username	Username Changeable	Password	Default Password	Password Changeable	Note
future remote service	7443/tcp 7444/tcp	-	-	-	-	-	-	
diprint	9100/tcp	N/A	N/A	N/A	N/A	N/A	N/A	

B) Related Protocols

Protocol	Protocol Suite	Commonly Used Port Num.	Description of the protocol's function in the Products.
ip	TCP/IP	-	
icmp	TCP/IP	Protocol Num. 1	
udp	TCP/IP	Protocol Num. 17	
tcp	TCP/IP	Protocol Num. 6	
ftp-data	TCP/IP	20/tcp, udp	1) Sending scan data to the FTP server. (Scan to FTP)
ftp-control	TCP/IP	21/tcp, udp	2) Sending scan data to ScanRouter
smtp	TCP/IP, IPX/SPX	25/tcp, udp	1) Sending scan data to the SMTP server. (Scan to E-mail)
domain (dns)	TCP/IP	53/tcp, udp	1) Resolving IP addresses from the server name.
bootp	TCP/IP	67/tcp, udp 68/tcp, udp	1) Getting IP addresses and other network parameters from the DHCP server.
pop	TCP/IP	110/tcp, udp	1) Using POP before SMTP authentication for 'Scan to E-mail'. 2) Receiving internet-fax data.
sntp	TCP/IP	123/tcp, udp	1) Getting GMT from the NTP server.
netbios-ns	TCP/IP, IPX/SPX, NetBEUI	137/tcp, udp	1) Sending scan data to SMB clients. (Scan to SMB)
netbios-dgm		138/tcp, udp	
netbios-ssn		139/tcp, udp	
imap	TCP/IP	143/tcp, udp	1) Getting internet-fax data
snmp-trap	TCP/IP, IPX/SPX	162/tcp, udp	1) Sending status information to Network Management Server.
ldap	TCP/IP	389/udp, tcp	1) Searching e-mail addresses from the LDAP server's address book.
syslog	TCP/IP	514/udp	1) Sending system logs to a syslog server.
ncp	TCP/IP, IPX/SPX	524/tcp, udp	1) Logging in to a Netware server.

Protocol	Protocol Suite	Commonly Used Port Num.	Description of the protocol's function in the Products.
			2) Printing from the Netware environment.
slp	TCP/IP	427/tcp, udp	1) Searching for a Netware Server.
ipx	IPX/SPX	-	1) Providing ipx connections
spx	IPX/SPX	-	1) Providing spx connections
sap	IPX/SPX	-	1) Broadcasts to availability of print services.
rip	IPX/SPX	-	1) Broadcasts route information.
appletalk	APPLETALK	-	1) Providing appletalk connections.
pap	APPLETALK	-	1) Providing appletalk printing services
netbeui	NETBEUI	-	1) Providing netbeui connections.

Commonly User Port Number: This is meant to be general information. This column contains well known port numbers commonly used in industry. This is not necessarily the port used by the products.

C) The Purpose of Access Control

The printer will accept communication only from a set range of IP addresses. This can be applied to connections from lpr, rcp/rsh, http, https, ftp, diprint, smb, ipp, and DeskTopBinder.

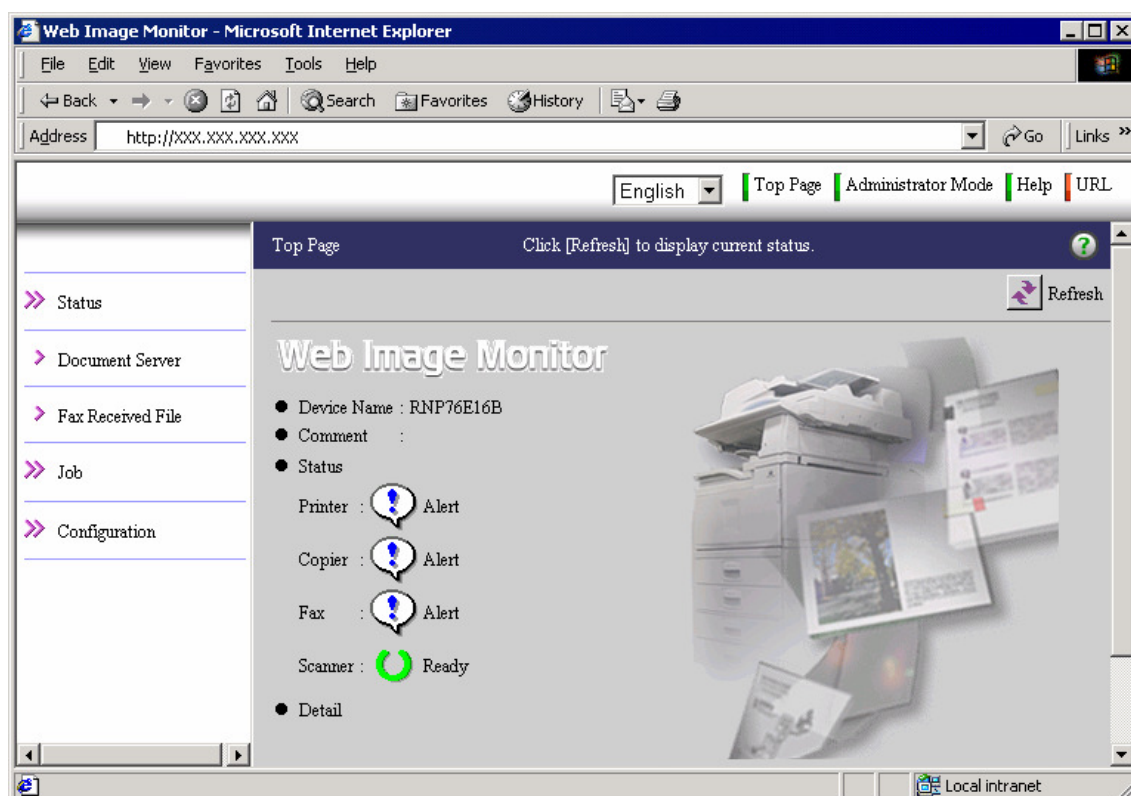
The cannot be applied to telnet and SmartDeviceMonitor.

C)-1 Web Image Monitor

(1) Web Image Monitor can be used for accessing the products. A supported Browser such as Microsoft Internet Explorer and the product's IP address is required. Enter the IP address as shown below.

http://<<printer host name or ip address>>

And then click "Administrator Mode"



(2) In order to access Administrator mode, a password is required. (The default password is 'password')



Enter Network Password

Please type your user name and password.

Site: XXX.XXX.XXX.XXX

Realm: Configuration

User Name:

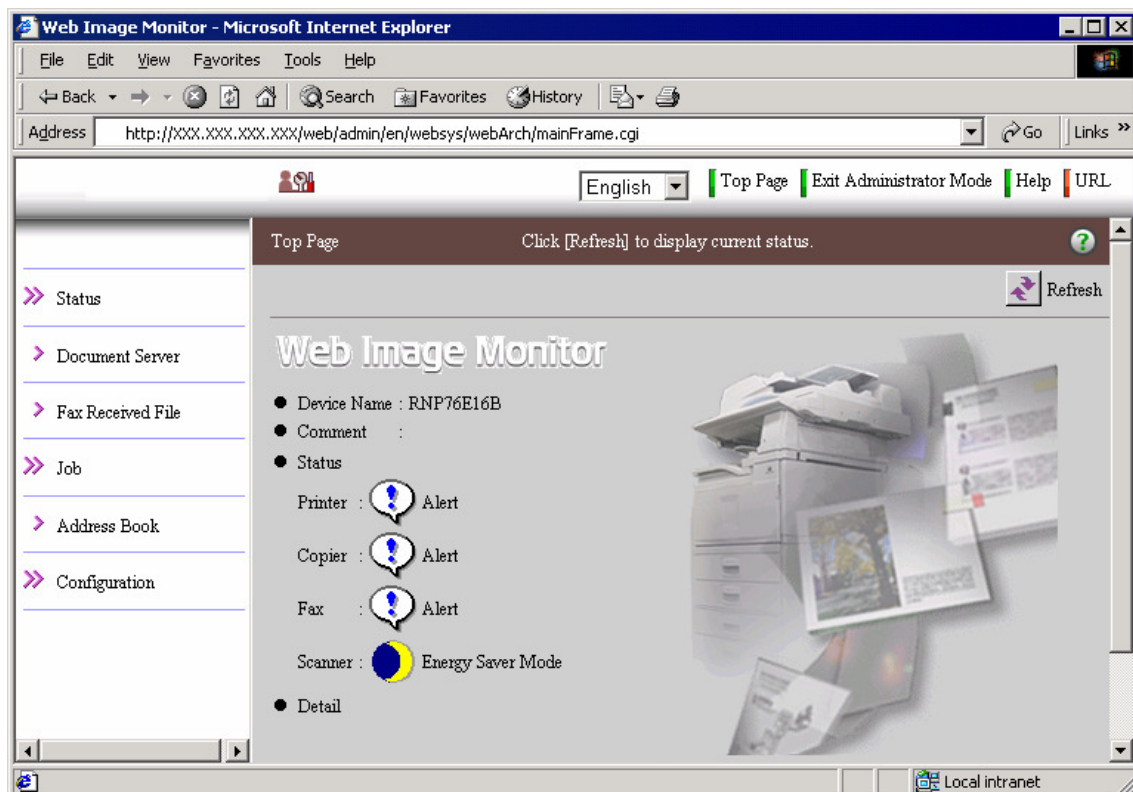
Password:

☐ Save this password in your password list

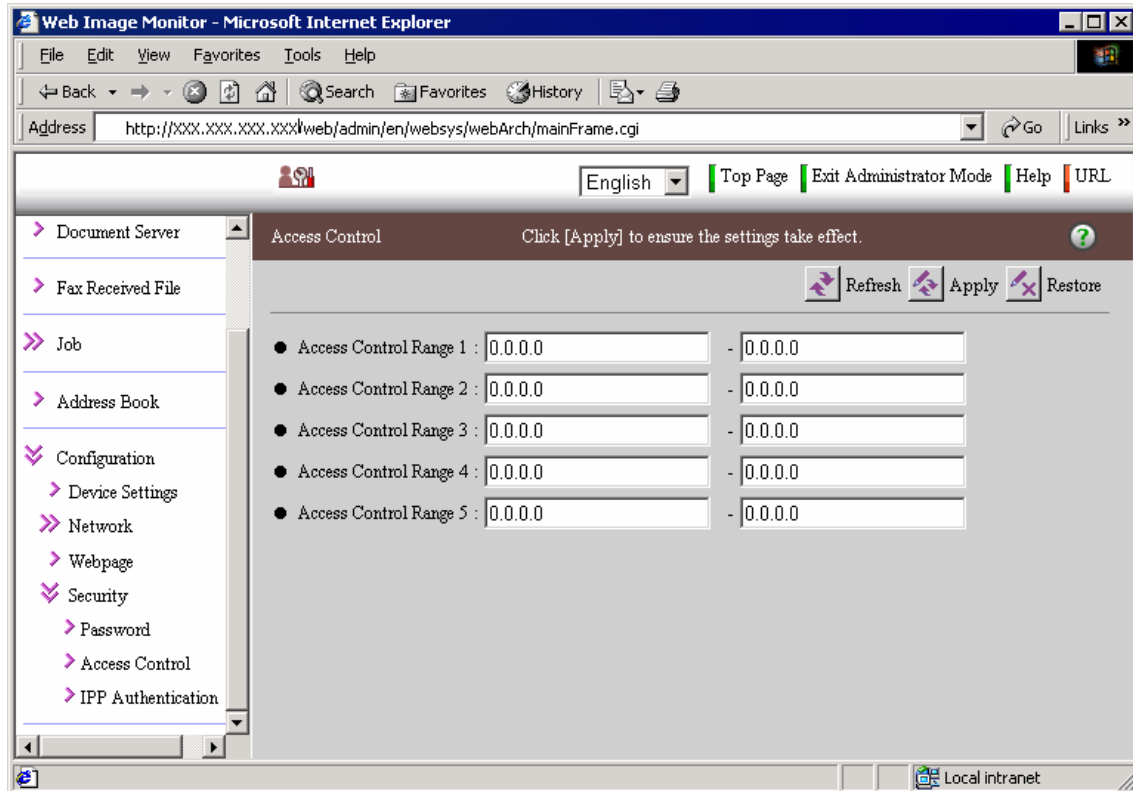
OK Cancel

(3) Login to enter Administrator mode.

You will know that you are in administrator mode if the bar at the top of the main frame is brown instead of blue as shown below.

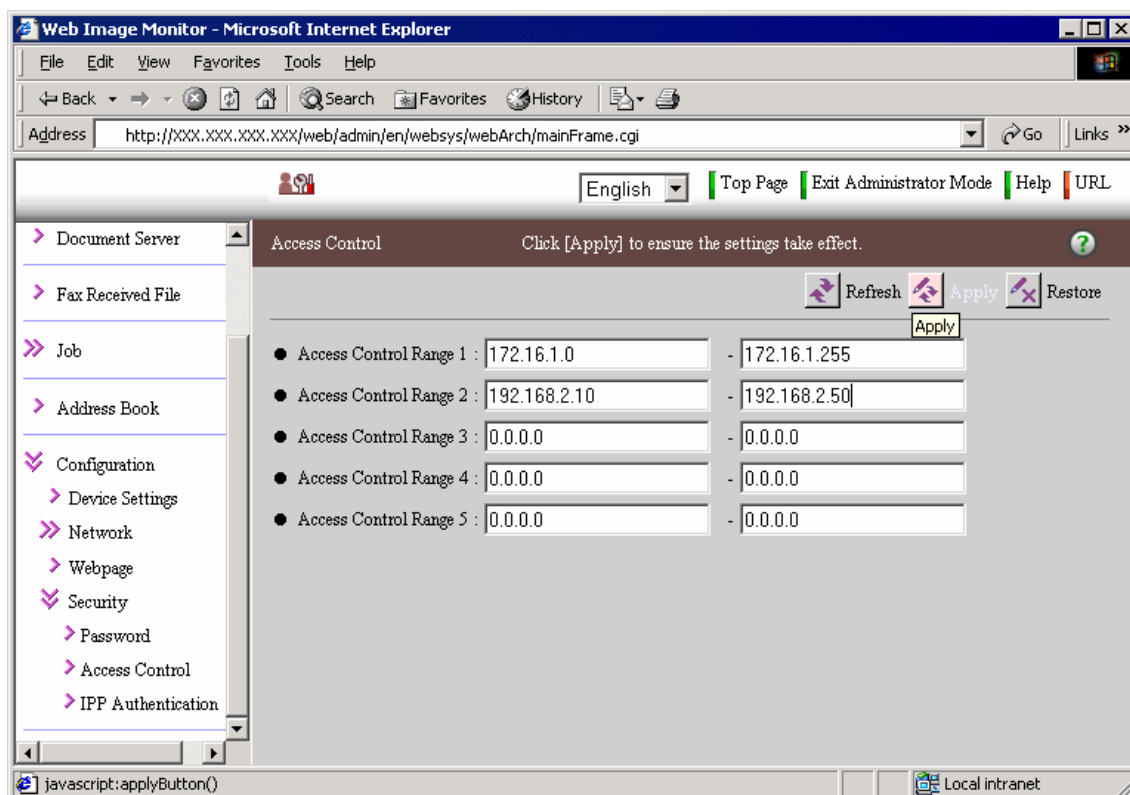


(4) To open the access control settings, click 'Configuration' -> 'Security' -> 'Access Control'.



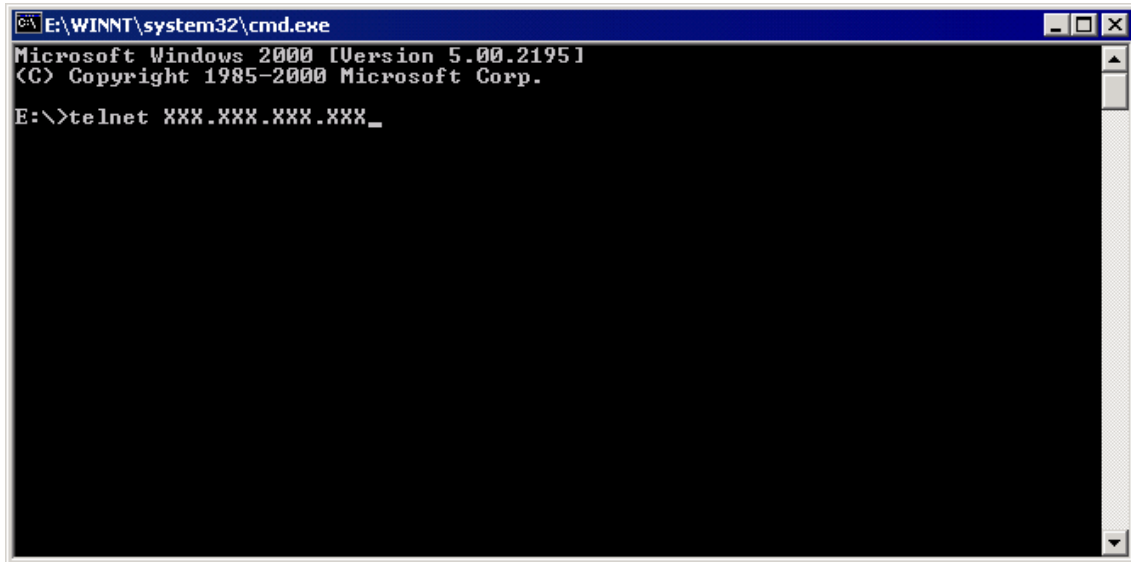
(5) Input the range of IP addresses that you wish to permit communication with.

Click the 'Apply' button to commit the changes.



C)-2 mshell

(1) Access the products, using a telnet client. In this case the Windows 2000 standard telnet client is shown.

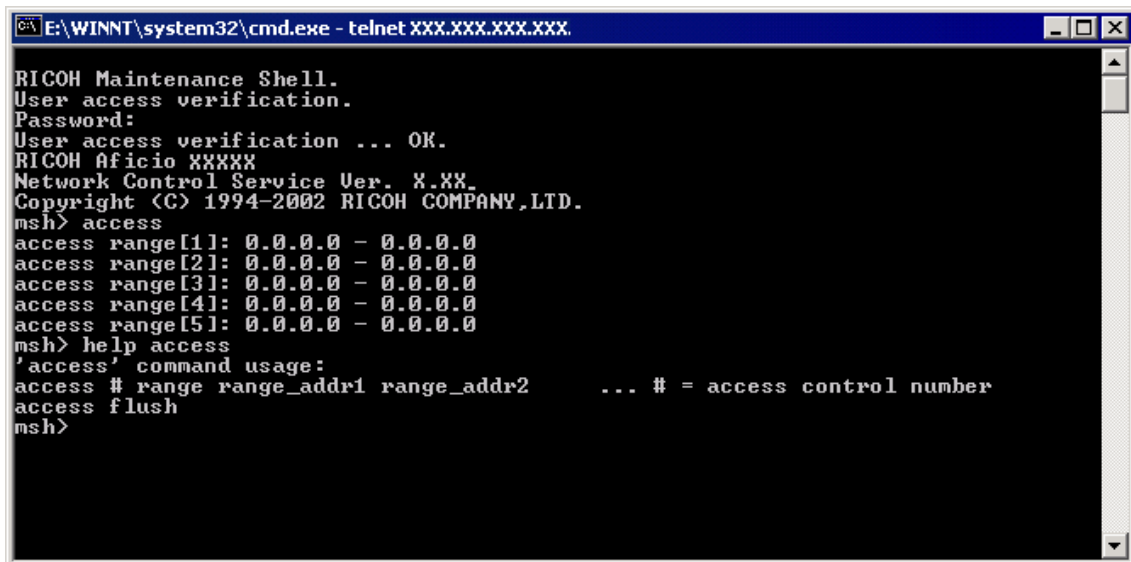


```

E:\WINNT\system32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

E:\>telnet XXX.XXX.XXX.XXX_
  
```

(2) Open the Maintenance Shell (mshell). A password will be required for this. (The default password is 'password'). Using the access command input the access control range.



```

E:\WINNT\system32\cmd.exe - telnet XXX.XXX.XXX.XXX
RICOH Maintenance Shell.
User access verification.
Password:
User access verification ... OK.
RICOH Aficio XXXXX
Network Control Service Ver. X.XX
Copyright (C) 1994-2002 RICOH COMPANY,LTD.
msh> access
access range[1]: 0.0.0.0 - 0.0.0.0
access range[2]: 0.0.0.0 - 0.0.0.0
access range[3]: 0.0.0.0 - 0.0.0.0
access range[4]: 0.0.0.0 - 0.0.0.0
access range[5]: 0.0.0.0 - 0.0.0.0
msh> help access
'access' command usage:
access # range range_addr1 range_addr2    ... # = access control number
access flush
msh>
  
```

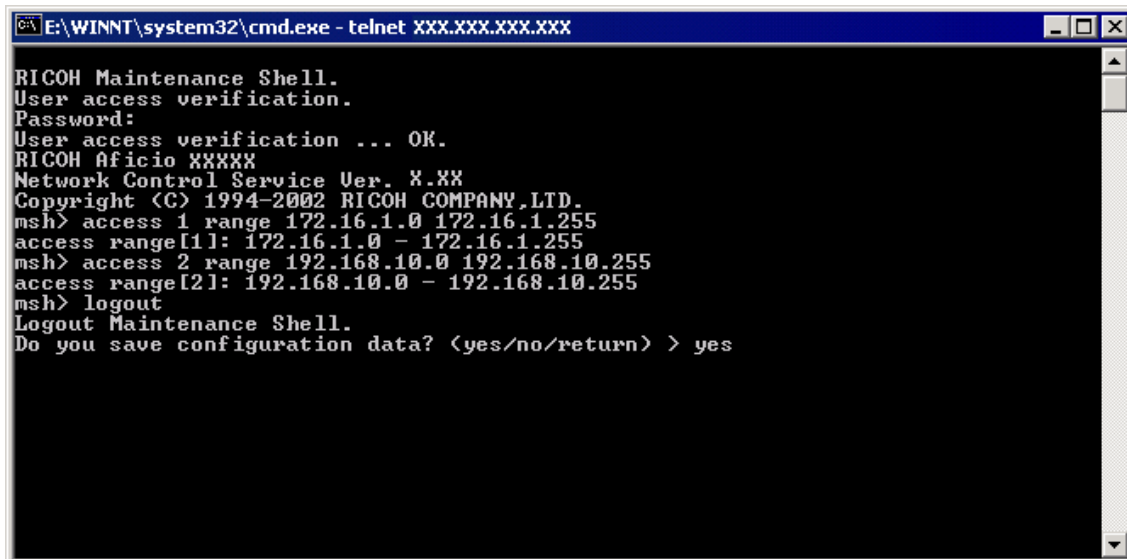
E.g.1 Input the following command to permit only access from 172.16.1.0 to 172.16.2.0

msh> access 1 range 172.16.1.0 172.16.2.0

E.g.2 Input the following command to clear all access ranges.

msh> access flush

(3) If changes have been made, the following question will appear before the user logs out.
'Do you save configuration data?' Input 'yes' to commit the changes. Input 'no' to discard them.



```
E:\WINNT\system32\cmd.exe - telnet XXX.XXX.XXX.XXX

RICOH Maintenance Shell.
User access verification.
Password:
User access verification ... OK.
RICOH Aficio XXXXXX
Network Control Service Ver. X.XX
Copyright (C) 1994-2002 RICOH COMPANY,LTD.
msh> access 1 range 172.16.1.0 172.16.1.255
access range[1]: 172.16.1.0 - 172.16.1.255
msh> access 2 range 192.168.10.0 192.168.10.255
access range[2]: 192.168.10.0 - 192.168.10.255
msh> logout
Logout Maintenance Shell.
Do you save configuration data? (yes/no/return) > yes
```

D) How to disable services

The following services can be enabled or disabled by selecting up or down.

tcpip, netware(*1), smb(*2), appletalk, lpr, ftp(*3), rsh, diprint, web(Only mshell) (*4), snmp(*5), ipp(*6), http(Only mshell) (*7), ip1394, scsiprint, telnet (Only mshell), rendezvous(*8), ssl(*9)

*1; netware; Setting netware to down, disables the IPX/SPX protocol and NCP/IP. Therefore if netware is down, printing in the IPX/SPX environment and in the pure IP environment is unavailable. LPR in NDPS and iPrint (ipp Printing) are unaffected.

*2; smb; Setting smb to down, closes NetBIOS Session Service (139/tcp) The NetBIOS Session Service (139/tcp) and netbeui service will be down. However affects only the server service. The client service is not affected. Therefore, if smb is down, Scan to SMB can still be used.

*3; ftp; Setting ftp to down, closes ftp port (21/tcp). The FTP server service will be down but the FTP client function is still available. Therefore if this function is down, Scan to FTP is still available.

*4; web; Setting web to down, disables the Web Image Monitor. However even if this function is disabled, HTTP Port (80/tcp) will still be open. Therefore if this function is disabled, ipp printing using HTTP Port (80/tcp) is still available.

*5; snmp; Setting snmp to down, closes snmp port (161/udp). In addition when snmp is down, the snmp trap function and snmp function over IPX/SPX are not available.

*6; ipp; Setting ipp to down, disables the ipp printing function but doesn't close ipp Port (631/tcp). Therefore if ipp is down, ipp printing using HTTP (80/tcp) is still available.

*7; http; Setting http to down, closes HTTP Port (80/tcp). Therefore, not only Web Image Monitor but also ipp printing using HTTP port (80/tcp) is disabled.

*8; rendezvous; Setting rendezvous to down makes rendezvous is unavailable and closes the mdns port (5353/udp).

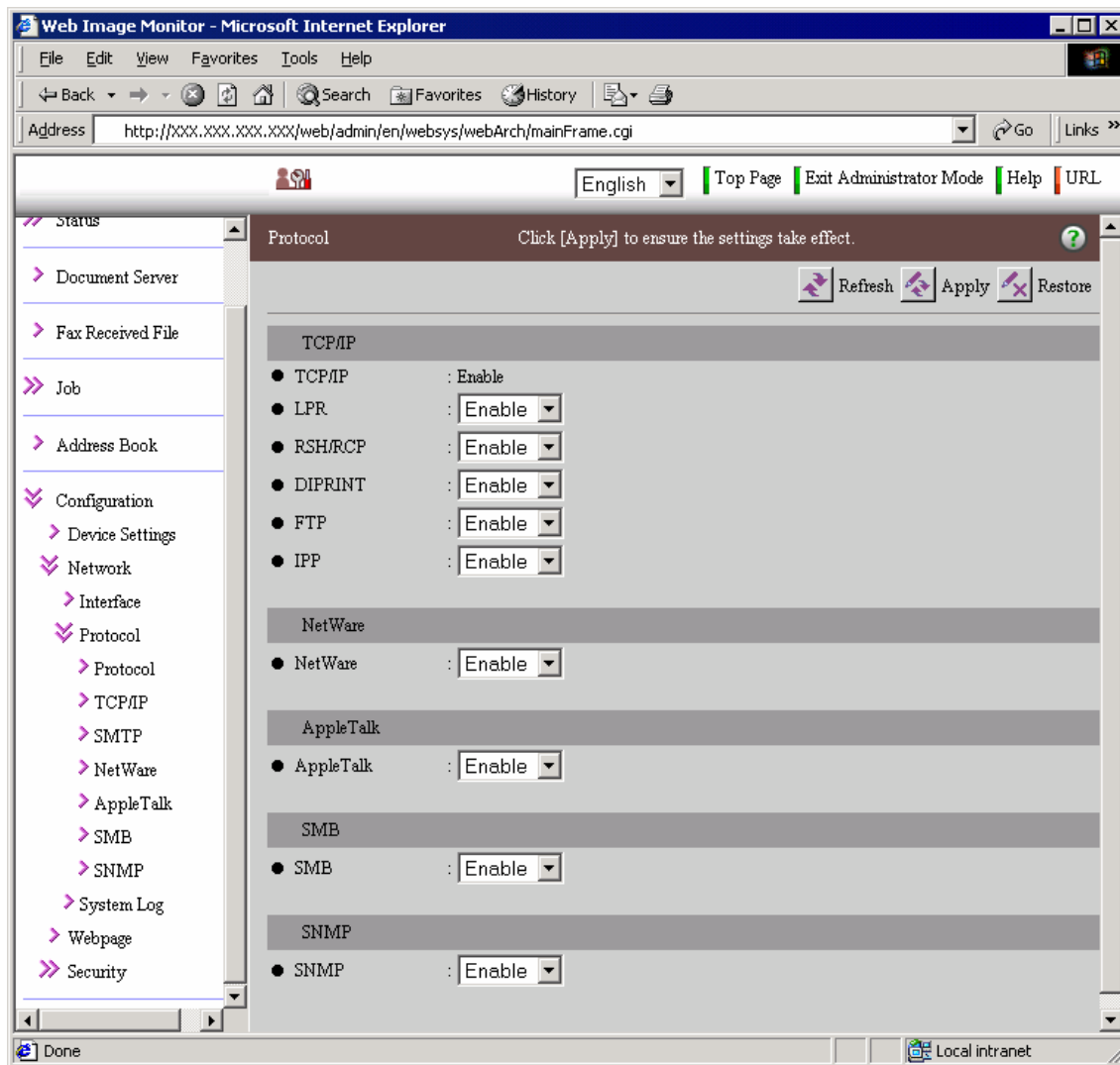
*9; ssl; Setting ssl to down, closes the https port. Therefore, Web Image Monitor and ipp printing using https port (443/tcp) are disabled.

D)-1 Web Image Monitor

Steps (1) to (3) are the same as C)-1 (previous section)

(4) Click 'Configuration' -> 'Network' -> 'Protocol' -> 'Protocol' to access the protocol settings.

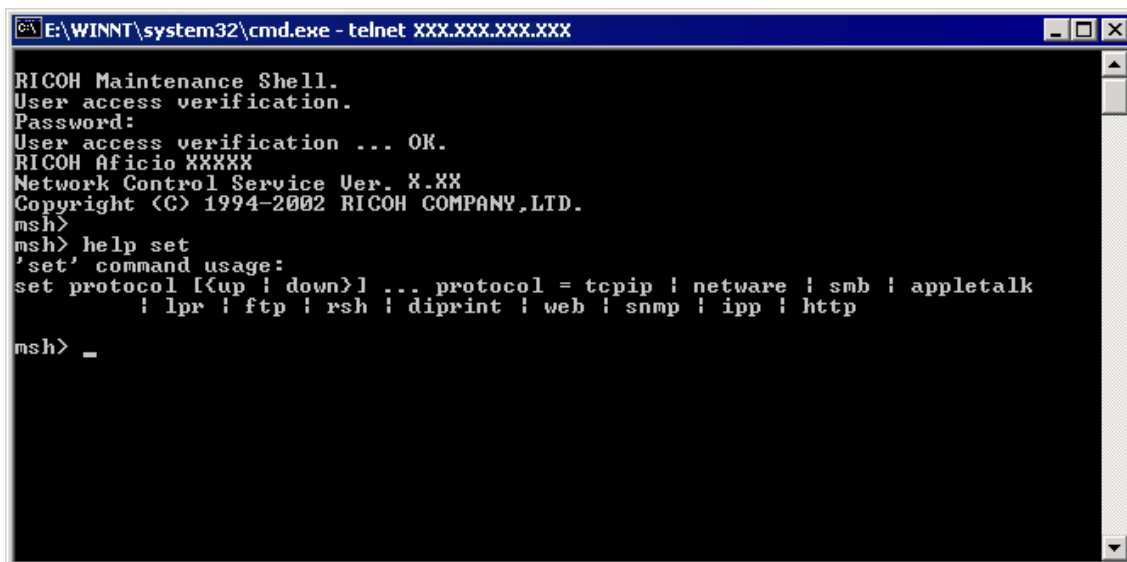
By default all protocols are enabled.



(*) The SSL settings can be accessed via 'Configuration' -> 'Security' -> 'SSL/TLS'

D)-2 mshell

- (1) The procedure for this is the same as is shown in section C)-2
- (2) Using the 'set' command, input the access control range.



```

E:\WINNT\system32\cmd.exe - telnet XXX.XXX.XXX.XXX

RICOH Maintenance Shell.
User access verification.
Password:
User access verification ... OK.
RICOH Aficio XXXXX
Network Control Service Ver. X.XX
Copyright (C) 1994-2002 RICOH COMPANY,LTD.
msh>
msh> help set
'set' command usage:
set protocol [{up | down}] ... protocol = tcpip | netware | smb | appletalk
        | lpr | ftp | rsh | diprint | web | snmp | ipp | http
msh> _

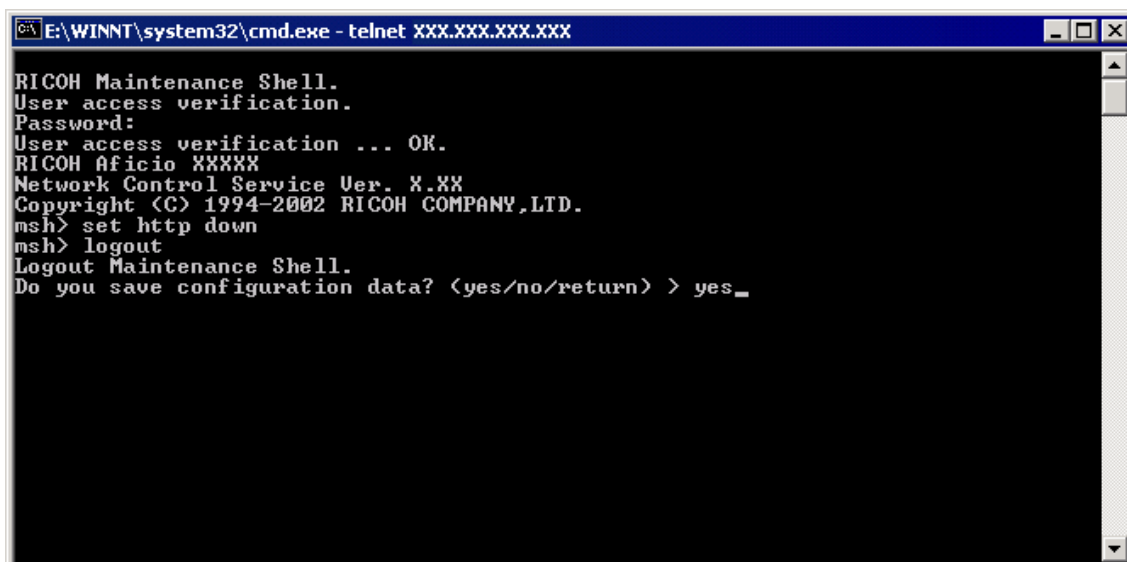
```

E.g.1 Input the following command to disable the http protocol.

msh> set http down

Note: telnet does not appear in the help menu.

- (3) The procedure for this is the same as is shown in section C)-2



```

E:\WINNT\system32\cmd.exe - telnet XXX.XXX.XXX.XXX

RICOH Maintenance Shell.
User access verification.
Password:
User access verification ... OK.
RICOH Aficio XXXXX
Network Control Service Ver. X.XX
Copyright (C) 1994-2002 RICOH COMPANY,LTD.
msh> set http down
msh> logout
Logout Maintenance Shell.
Do you save configuration data? (yes/no/return) > yes_

```

4. Reference list

RFC: <http://www.fags.org/rfcs/>

CVE: <http://cve.mitre.org/>

CERT: <http://www.cert.org/>

CIAC: <http://www.ciac.org/ciac/>

SecurityFocus: <http://www.securityfocus.com/>

NESSUS: <http://www.nessus.org/index2.html>