



Xerox Phaser 3610/WorkCentre 3615 Information Assurance Disclosure Paper Version 1.0

Prepared by:

Erin Huber
Xerox Corporation
800 Phillips Road
Webster, New York 14580

©2013 Xerox Corporation. All rights reserved. Xerox and the sphere of connectivity design are trademarks of Xerox Corporation in the United States and/or other countries.

Other company trademarks are also acknowledged.

Document Version: 1.0 (August 2013).





- 1. INTRODUCTION..... 5**
- 1.1. Purpose.....5
- 1.2. Target Audience5
- 1.3. Disclaimer5
- 2. DEVICE DESCRIPTION 6**
- 2.1. Security-relevant Subsystems.....8
 - 2.1.1. Physical Partitioning 8
 - 2.1.2. Security Functions allocated to Subsystems.....9
- Controller.....10**
 - 2.1.3. Purpose.....10
 - 2.1.4. Memory Components10
 - 2.1.5. External Connections11
 - 2.1.6. USB Ports.....12
- 2.3 Fax Module (WorkCentre 3615 only).....12
 - 2.3.1. Purpose.....12
 - 2.3.2. Hardware12
- 2.4. Scanner (WorkCentre 3615 only)13
 - 2.4.1. Purpose.....13
 - 2.4.2. Hardware13
- 2.5. Marking Engine (also known as the Image Output Terminal or IOT).....14
 - 2.5.1. Purpose.....14
 - 2.5.2. Hardware14
 - 2.5.3. Control and Data Interfaces.....14
- 2.6. System Software Structure14
 - 2.6.1. Open-source components14
 - 2.6.2. OS Layer in the Controller14
 - 2.6.3. Network Protocols.....15
- 2.7. Logical Access.....16
 - 2.7.1. Network Protocols.....16
 - 2.7.2. Wireless Support16
 - 2.7.2.1. 802.11 Infrastructure Mode.....16
 - 2.7.2.2. 802.11 Ad Hoc Mode.....16
 - 2.7.3. IPSec16
 - 2.7.4. Ports.....17
 - 2.7.4.1. Port 23, Telnet.....17
 - 2.7.4.2. Port 25, SMTP.....17
 - 2.7.4.3. Port 53, DNS17
 - 2.7.4.4. Port 68, DHCP18
 - 2.7.4.5. Port 80, HTTP.....18
 - 2.7.4.6. Port 88, Kerberos18
 - 2.7.4.7. Ports 137, 138, 139, NETBIOS.....19
 - 2.7.4.8. Ports 161, 162, SNMP.....19



2.7.4.9. Port 389, LDAP.....20

2.7.4.10. Port 427, SLP.....20

2.7.4.11. Port 443, SSL/HTTPS20

2.7.4.12. Port 445, SMB/CIFS.....20

2.7.4.13. Port 515, LPR20

2.7.4.14. Port 546, DHCPv6.....20

2.7.4.15. Port 631, IPP.....20

2.7.4.16. Port 636, sLDAP20

2.7.4.17. Port 3003, http/SNMP reply21

2.7.4.18. Port 5200, UPnP/SSDP.....21

2.7.4.19. Port 5353, Multicast DNS.....21

2.7.4.20. Port 8018, WSD.....21

2.7.4.21. Port 9100, raw IP21

2.7.5. IP Filtering21

3. SYSTEM ACCESS..... 22

3.1. Authentication Model.....22

3.2. Login and Authentication Methods.....22

3.2.1. System Administrator Login22

3.2.2. User authentication (WorkCentre 3615 only)22

3.3. System Accounts23

3.3.1. Printing23

3.3.2. Network Scanning (WorkCentre 3615 ONLY).....23

3.4. Diagnostics23

4. SECURITY ASPECTS OF SELECTED FEATURES 24

4.1. Port Control for USB ports24

4.2. Encrypted Partitions24

4.3. Clear Device Memory.....24

5. RESPONSES TO KNOWN VULNERABILITIES 25

5.1. Security @ Xerox (www.xerox.com/security).....25

6. APPENDICES 26

6.1. Appendix A – Abbreviations.....26

6.2. Appendix B – Supported MIB Objects28

6.3. Appendix C –Standards30

6.4. Appendix E – References31



1. Introduction

The Phaser 3610 printer and the WorkCentre 3615 multifunction system are among the latest versions of Xerox devices for general office use.

1.1. Purpose

The purpose of this document is to disclose information for the Phaser and WorkCentre products with respect to device security. Device Security, for this paper, is defined as how image data is stored and transmitted, how the product behaves in a networked environment, and how the product may be accessed, both locally and remotely. Please note that the customer is responsible for the security of their network and the printers and multifunction devices do not establish security for any network environment.

The purpose of this document is to inform Xerox customers of the design, functions, and features of the Phaser and WorkCentre products relative to Information Assurance (IA).

This document does NOT provide tutorial level information about security, connectivity, PDLs, or WorkCentre products features and functions. This information is readily available elsewhere. We assume that the reader has a working knowledge of these types of topics. However, a number of references are included in the Appendix.

1.2. Target Audience

The target audience for this document is Xerox field personnel and customers concerned with IT security.

1.3. Disclaimer

The information in this document is accurate to the best knowledge of the authors, and is provided without warranty of any kind. In no event shall Xerox Corporation be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this document including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox Corporation has been advised of the possibility of such damages.

2. Device Description

The WorkCentre 3615 consists of an input document handler and scanner, marking engine including paper path, controller, and user interface.

The Network Controller is located on the left rear side of the machine in WorkCentre 3615 products.



The Phaser 3610 consists of a marking engine including paper path, controller, and user interface.



2.1. Security-relevant Subsystems

2.1.1. Physical Partitioning

The security-relevant subsystems of the product are partitioned as shown in Figure 2-1.

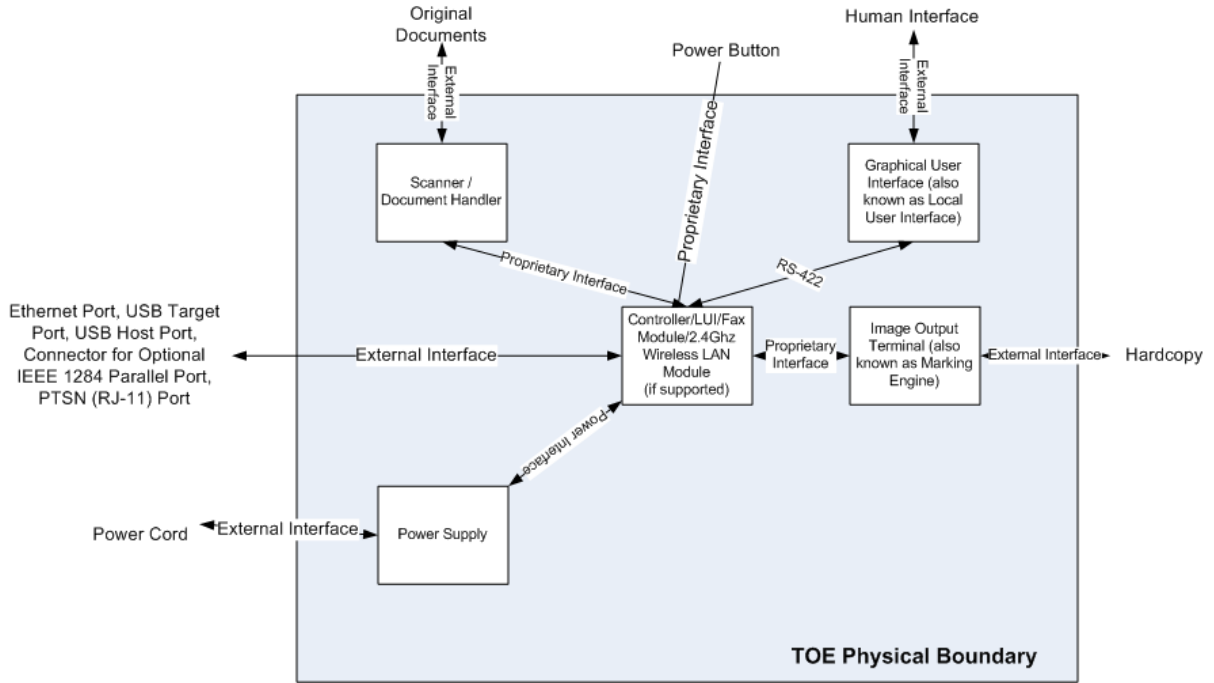


Figure 2-1 System functional block diagram

2.1.2. Security Functions allocated to Subsystems

| Security Function | Subsystem |
|-------------------------------------|--|
| Image Overwrite | Controller Local User Interface |
| System Authentication | Controller Local User Interface |
| Network Authentication | Controller Local User Interface |
| Cryptographic Operations | Controller |
| User Data Protection – SSL | Controller |
| User Data Protection – IP Filtering | Controller |
| User Data Protection – IPSec | Controller |
| Network Management Security | Controller |
| Fax Flow Security | Fax Module Controller Local User Interface |
| Security Management | Controller Local User Interface |

Table 1 Security Functions allocated to Subsystems

Controller

2.1.3. Purpose

The controller provides both network and direct-connect external interfaces, and enables copy, print, email, network scan and Embedded FAX functionality (print only for the Phaser 3610).

The controller also incorporates a proprietary web server that exports a Web User Interface (WebUI) through which users can submit jobs and check job and machine status, and through which system administrators can remotely administer the machine.

[WorkCentre 3615 only] The controller contains the image path, which uses proprietary hardware and algorithms to process the scanned images into high-quality reproductions. Scanned images may be temporarily buffered in DRAM to enable electronic pre-collation, sometimes referred to as scan-once/print-many. When producing multiple copies of a document, the scanned image is processed and buffered in the DRAM in a proprietary format. The buffered bitmaps are then read from DRAM and sent to the Image Output Terminal (IOT) for marking on hardcopy output. For long documents, the production of hardcopy may begin before the entire original is scanned, achieving a level of concurrency between the scan and mark operations.

The controller operating system is VxWorks v6.3. The controller works with the User Interface (UI) assembly to provide system configuration functions. The device can be configured to require a System Administrator PIN be entered at the UI in order to access device settings.

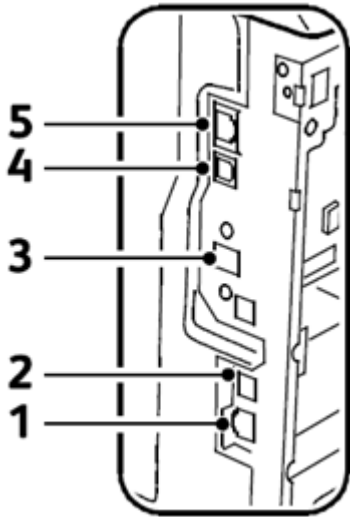
2.1.4. Memory Components

| Volatile Memory | | | | |
|---|-------|-----------------------|---|---------------------|
| Type (SRAM, DRAM, etc) | Size | User Modifiable (Y/N) | Function or Use | Process to Sanitize |
| SDRAM | 512MB | N | Executable code, Printer control data [MIOP] | Remove power |
| Additional Information: | | | | |
| Non-Volatile Memory | | | | |
| Type (Flash, EEPROM, etc) | Size | User Modifiable (Y/N) | Function or Use | Process to Sanitize |
| Flash | 8MB | Via Diagnostics | Firmware | None – No PII |
| EEPROM | 1MB | Via Diagnostics | Control setpoints, configuration settings (MIB) | None – No PII |
| Flash | 8MB | | | |
| Flash | 8MB | | | |
| Additional Information: All memory listed above contains code for execution and configuration information. No user or job data is permanently stored in this location. | | | | |

Table 2 Controller memory components

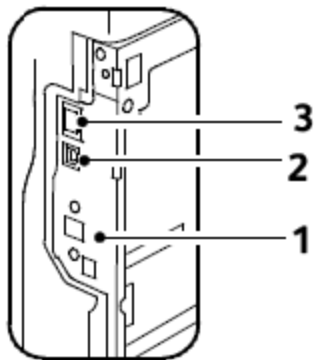
2.1.5. External Connections

2.2.3.1 WorkCentre 3615



| | Interface | Description / Usage |
|---|--|--|
| 1 | Extension Telephone Socket (EXT), RJ11 | Allows connection of telephone |
| 2 | FAX line 1, RJ-11 | Supports FAX Modem T.30 protocol only |
| 3 | Wireless adapter | 2.4 Ghz Wireless. The device supports an Infrastructure mode and an Ad Hoc mode. |
| 4 | USB 2.0 Target Port | Direct-connect printing |
| 5 | Network Port | 10/100/1000 Network connectivity |

2.2.3.2 Phaser 3610



| | Interface | Description / Usage |
|---|---------------------|--|
| 1 | Wireless adapter | 2.4 Ghz Wireless. The device supports an Infrastructure mode and an Ad Hoc mode. |
| 2 | USB 2.0 Target Port | Direct-connect printing |
| 3 | Network Port | 10/100/1000 Network connectivity |

2.1.6. USB Ports

The WorkCentre 3615 contains a host connector for a USB flash drive, enabling printing from USB and scanning to USB.

Autorun is disabled on this port. No executable files will be accepted by the port.

Both ports can be disabled by an Admin via the WebUI.

| USB | |
|-----------------------|------------------------------------|
| USB port and location | Purpose |
| USB 2.0 Host port | Printing from USB, scanning to USB |
| USB 2.0 Target port | Direct-connect printing |

Table 3 USB Ports

2.3 Fax Module (WorkCentre 3615 only)

2.3.1. Purpose

The embedded FAX service uses the embedded fax module to send and receive images over the telephone interface.

2.3.2. Hardware

The fax module is built into the Main Controller processor card. The fax module does not have its own processor and local memory but uses the Main processor and internal memory. The card contains a fax-only modem that supports the T.30 protocol. If anything other than the T.30 protocol is detected, the modem will disconnect. Internal logical interfaces maintain separation between Fax and network.

| Volatile Memory Description | | | | |
|--|------------------------------------|---|---|------------------------|
| Type (SRAM, DRAM, etc) | Size | User Modifiable (Y/N) | Function or Use | Process to Clear: |
| None | n/a | n/a | n/a | n/a |
| Additional Information: | | | | |
| Non-Volatile Memory Description | | | | |
| Type (Flash, EEPROM, etc) | Size | User Modifiable (Y/N) | Function or Use | Process to Clear: |
| Internal optional SD card | Fax jobs stored on 570MB partition | Yes – Directly by saving/ deleting files. | All permanent user and device history data, All temporary and stored image data | Manual Image Overwrite |
| Additional Information: This partition is encrypted using AES 256bit encryption. The only overwrite method available on the WorkCentre 3615 is Manual Image Overwrite. Manual Image Overwrite is invoked from the device LUI. It consists of a single pass using the F character. | | | | |

Table 4 Fax Module memory components

2.4. Scanner (WorkCentre 3615 only)

2.4.1. Purpose

The purpose of the scanner is to provide mechanical transport of hardcopy originals and to convert hardcopy originals to electronic data.

2.4.2. Hardware

The scanner converts the image from hardcopy to electronic data. A document handler moves originals into a position to be scanned. The scanner provides enough image processing for signal conditioning and formatting. The scanner does not store scanned images. All other image processing functions are in the main controller.

Marking Engine (also known as the Image Output Terminal or IOT)

2.5.1. Purpose

The Marking Engine performs copy/print paper feeding and transport, image marking and fusing. Images are not stored at any point in these subsystems.

2.5.2. Hardware

The marking engine is comprised of paper supply trays and feeders, paper transport, laser scanner (WorkCentre 3615 only), xerographics, and paper output.

2.5.3. Control and Data Interfaces

Images and control signals are transmitted from the main controller to the marking engine across a proprietary interface.

2.6. System Software Structure

2.6.1. Open-source components

Open-source components in the connectivity layer implement high-level protocol services. The security-relevant connectivity layer components are:

- Apache Xerces2
- NetBSD Project
- netsnmp library
- Open1x
- Open SLP
- libupnp
- wpa_supplicant
- ldns
- uIP
- Info-zip
- TWAIN sample Data Source
- libzip library
- Java Sample code
- NetBSD Project
- FreeType2
- GCC
- CUPS
- libjpeg
- TWAIN 2.0 DSM library
- libxml2 library
- Expat XML parser
- Unicode
- cURL library
- Kerberos v1.3.5
- Raphael
- pixman
- lua library
- Little CMS library
- cairo graphics library
- iText
- Open LDAP v2.1.15
- OpenSSL library v0.9.8h
- libtiff
- libpng
- zlib v1.2.3
- NSIS
- CxImage

2.6.2. OS Layer in the Controller

The OS layer includes the operating system, network and physical I/O drivers. The controller operating system is VxWorks v6.8.

The crypto library for IPSec is provided by the OpenSSL Toolkit.

IP Filtering is also provided as a loadable kernel module.

2.6.3. Network Protocols

Figure 2- is an interface diagram depicting the protocol stacks supported by the device, annotated according to the DARPA model.

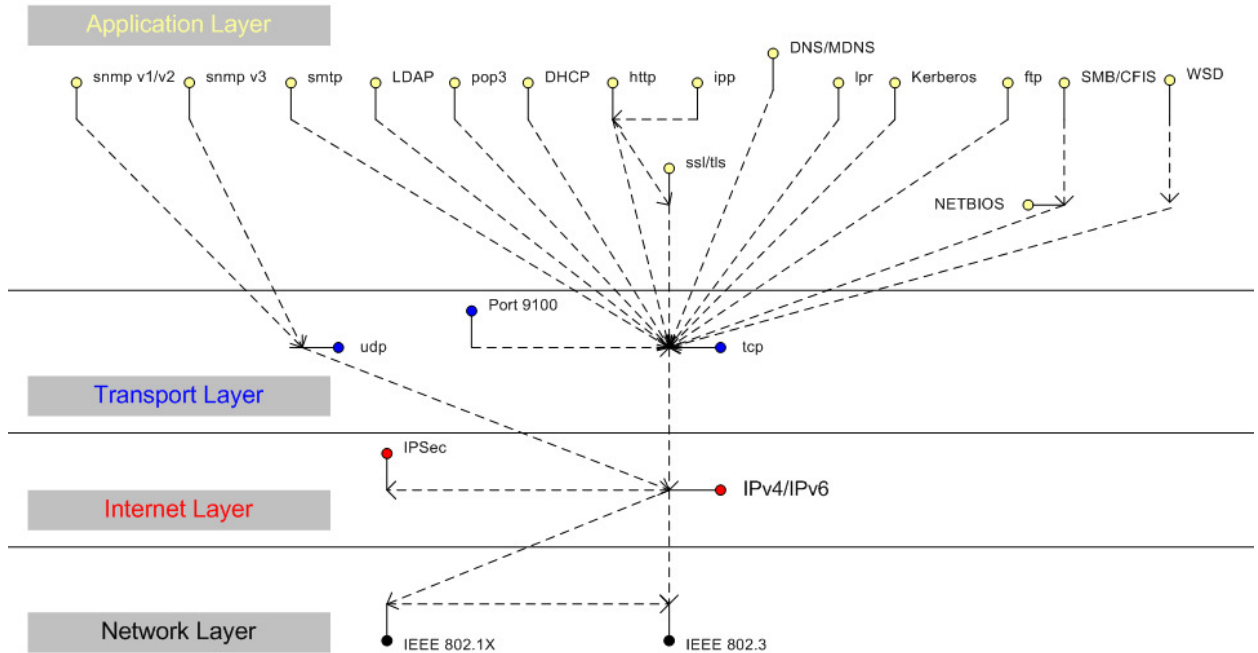


Figure 2-4 IPv4/IPv6 Network Protocol Stack

2.7. Logical Access

2.7.1. Network Protocols

The supported network protocols are listed in Appendix C and are implemented to industry standard specifications (i.e. they are compliant to the appropriate RFC) and are well-behaved protocols. There are no 'Xerox unique' additions to these protocols.

2.7.2. Wireless Support

The WorkCentre 3615 contains a 2.4 Ghz Wireless LAN module. The device supports an Infrastructure mode and an Ad Hoc mode. The Ad Hoc mode is enabled by default and is active if no wired connection exists. The wireless feature can be enabled, disabled and configured from the device LUI or the CWIS Properties tab.

2.7.2.1. 802.11 Infrastructure Mode

In Infrastructure mode, there is at least one wireless Access Point and one wireless client. The wireless client uses the wireless Access Point to access the resources of a traditional wired network. The wired network can be an organization intranet or the Internet, depending on the placement of the wireless Access Point.

The supported Authentication types for Infrastructure Mode are WPA-Personal, WPA-Enterprise, WPA2-Personal, and WPA2 –Enterprise. The supported encryption types are TKIP and AES. (only with optional SD card)

2.7.2.2. 802.11 Ad Hoc Mode

In Ad Hoc mode, wireless clients communicate directly with each other without the use of a wireless Access Point. One of the wireless clients takes over the responsibility of the wireless Access Point. All wireless clients must be explicitly configured to use ad hoc mode. There can be a maximum of nine members in an ad hoc 802.11 wireless network.

The supported Authentication types for Ad Hoc mode are Open System and Shared Key. The supported encryption key types are WEP64 and WEP128.

2.7.3. IPSec

The device supports IPSec tunnel mode. The print channel can be secured by establishing an IPSec association between a client and the device. A shared secret is used to encrypt the traffic flowing through this tunnel. SSL must be enabled in order to set up the shared secret.

When an IPSec tunnel is established between a client and the machine, the tunnel will also be active for administration with SNMPv2 tools (HP Open View, etc.), providing security for SNMP SETs and GETS with an otherwise insecure protocol. SNMP Traps may not be secure if either the client or the device has just been rebooted. IP Filtering can be useful to prevent SNMP calls from non-IPSec clients.

Once an IPSec channel is established between two points, it stays open until one end reboots or goes into power saver,. Only network clients and servers will have the ability to establish an IPSec tunnel with the machine. Thus device-initiated operations (like scanning) cannot assume the existence of the tunnel unless a print job (or other client initiated action) has been previously run since the last boot at either end of the connection.

2.7.4. Ports

The following table summarizes all potential open ports and subsequent sections discuss each port in more detail.

| Default Port # | Type | Service name |
|----------------|---------|---|
| 23 | TCP | Telnet |
| 25 | TCP | SMTP |
| 53 | UDP | DNS |
| 68 | UDP | BOOTP/DHCP |
| 80 | TCP | HTTP |
| 88 | UDP/TCP | Kerberos |
| 137 | UDP | NETBIOS- Name Service |
| 138 | UDP | NETBIOS-Datagram Service; SMB/CIFS filing |
| 139 | TCP | NETBIOS; SMB/CIFS filing |
| 161 | UDP | SNMP |
| 162 | UDP | SNMP trap |
| 389 | UDP | LDAP |
| 427 | TCP/UDP | SLP |
| 443 | TCP | SSL/HTTPS |
| 445 | TCP | SMB/CIFS |
| 515 | TCP | LPR |
| 546 | UDP | DHCPv6 |
| 631 | TCP | IPP |
| 636 | TCP | sLDAP |
| 3003 | TCP | HTTP/SNMP reply |
| 5200 | TCP | UPnP/SSDP |
| 5353 | UDP | Multicast DNS |
| 6000 | UDP | SetIP Utility |
| 7000 | UDP | LTP Utility |
| 8018 | TCP | WSD |
| 9100 | TCP | Raw IP |

Table 75 Network Ports

Please note that there is no FTP port in this list. FTP is only used to export scanned images and to retrieve Scan Job Templates, and will open port 21 on the remote device. An FTP port is never open on the controller itself.

2.7.4.1. Port 23, Telnet

When enabled, Telnet can be used to configure some network and printer port settings. Telnet is disabled by default and can be configured on the Properties tab of the Web UI.

2.7.4.2. Port 25, SMTP

This unidirectional port is open only when Scan to E-mail is exporting images to an SMTP server or when email alerts are being transmitted. SMTP messages & images are transmitted to the SMTP server from the device. The port can be configured on the Properties tab of the Web UI.

2.7.4.3. Port 53, DNS

Designating a DNS server will allow the device to resolve domain names. This can be configured via the WebUI.

2.7.4.4. Port 68, DHCP

This port is used only when performing DHCP, and is not open all of the time. To permanently close this port, DHCP must be explicitly disabled. This is done in User Tools via the Local User Interface or via the TCP/IP page in the Properties tab on the WebUI.

2.7.4.5. Port 80, HTTP

The embedded web pages communicate to the machine through a set of unique APIs and do not have direct access to machine information:

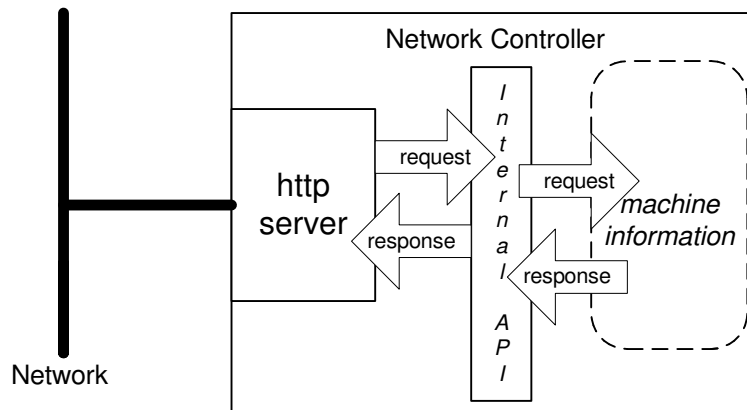


Figure 2-6 HTTP

The HTTP port can only access the HTTP server residing in the controller. The embedded HTTP server is Apache. The purpose of the HTTP server is to:

- Give users information of the status of the device;
- View the job queue within the device and delete jobs;
- Allow users to download print ready files and program Scan to File Job Templates;
- Allow remote administration of the device. Many settings that are on the Local UI are replicated in the device's web pages. Users may view the properties of the device but not change them without logging into the machine with administrator privileges.

The HTTP server can only host the web pages resident on the device. It does not and cannot act as a proxy server to get outside of the network the device resides on. Hence the server cannot access any networks (or web servers) outside of the customer firewall.

When the device is configured with an IP address, it is as secure as any device inside the firewall. The web pages are accessible only to authorized users of the network inside the firewall.

This service (and port) may be disabled in User Tools via the Local User Interface or via the TCP/IP page in the Properties tab on the Web UI. Please note that when this is disabled, IPP Port 631 is also disabled.

HTTP may be secured by enabling Secure Sockets Layer.

2.7.4.6. Port 88, Kerberos

This port is only open when the device is communicating with the Kerberos server to authenticate a user, and is only used only to authenticate users in conjunction with the Network Scanning feature. To disable this port, authentication must be disabled, and this is accomplished via the Local User Interface.

This version of software has Kerberos 5.1.1 with DES (Data Encryption Standard) and 64-bit encryption. The Kerberos code is limited to user authentication, and is used to authenticate a user with a given Kerberos server

as a valid user on the network. Please note that the Kerberos server (a 3rd party device) needs to be set up for each user. Once the user is authenticated, the Kerberos software has completed its task. This code will not and cannot be used to encrypt or decrypt documents or other information.

This feature is based on the Kerberos program from the Massachusetts Institute of Technology (MIT). The Kerberos network authentication protocol is publicly available on the Internet as freeware at <http://web.mit.edu/kerberos/www/>. Xerox has determined that there are no export restrictions on this version of the software. However, there are a few deviations our version of Kerberos takes from the standard Kerberos implementation from MIT. These deviations are:

- 1) The device does not keep a user's initial authentication and key after the user has been authenticated. In a standard Kerberos implementation, once a user is authenticated, the device holds onto the authentication for a programmed timeout (the usual default is 12 hours) or until the user removes it (prior to the timeout period). In the Xerox implementation, all traces of authentication of the user are removed once they have been authenticated to the device. The user can send any number of jobs until the user logs off the system, either manually or through system timeout.
- 2) The device ignores clock skew errors. In a standard implementation of Kerberos, authentication tests will fail if a device clock is 5 minutes (or more) different from the Kerberos server. The reason for this is that given enough time, someone could reverse engineer the authentication and gain access to the network. With the 5-minute timeout, the person has just 5 minutes to reverse engineer the authentication and the key before it becomes invalid. It was determined during the implementation of Kerberos for our device that it would be too difficult for the user/SA to keep the device clock in sync with the Kerberos server, so the Xerox instantiation of Kerberos has the clock skew check removed. The disadvantage is that this gives malicious users unlimited time to reverse engineer the user's key. However, since this key is only valid to access the Network Scanning features on a device, possession of this key is of little use for nefarious purposes.
- 3) The device ignores much of the information provided by Kerberos for authenticating. For the most part, the device only pays attention to information that indicates whether authentication has passed. Other information that the server may return (e.g. what services the user is authenticated for) is ignored or disabled in the Xerox implementation. This is not an issue since the only service a user is being authenticated for is access to an e-mail directory. No other network services are accessible from the Local UI.

Xerox has received an opinion from its legal counsel that the device software, including the implementation of a Kerberos encryption protocol in its network authentication feature, is not subject to encryption restrictions based on Export Administration Regulations of the United States Bureau of Export Administration (BXA). This means that it can be exported from the United States to most destinations and purchasers without the need for previous approval from or notification to BXA. At the time of the opinion, restricted destinations and entities included terrorist-supporting states (Cuba, Iran, Libya, North Korea, Sudan and Syria), their nationals, and other sanctioned entities such as persons listed on the Denied Parties List. Xerox provides this information for the convenience of its customers and not as legal advice. Customers are encouraged to consult with legal counsel to assure their own compliance with applicable export laws.

2.7.4.7. Ports 137, 138, 139, NETBIOS

For print jobs, these ports support the submission of files for printing as well as support Network Authentication through SMB. Port 137 is the standard NetBIOS Name Service port, which is used primarily for WINS. Port 138 supports the CIFS browsing protocol. Port 139 is the standard NetBIOS Session port, which is used for printing. Ports 137, 138 and 139 may be configured in the Properties tab of the device's web page.

2.7.4.8. Ports 161, 162, SNMP

These ports support the SNMPv1, SNMPv2c, and SNMPv3 protocols. Please note that SNMP v1 does not have any password or community string control. SNMPv2 relies on a community string to keep unwanted people from changing values or browsing parts of the MIB. This community string is transmitted on the network in clear text so anyone sniffing the network can see the password. Xerox strongly recommends that the customer change the community string upon product installation. SNMP is configurable, and may be explicitly enabled or disabled in the Properties tab on the WebUI.

SNMP traffic may be secured if an IPSec tunnel has been established between the agent (the device) and the manager (i.e. the user's PC).

The device supports SNMPv3, which is an encrypted version of the SNMP protocol that uses a shared secret. Secure Sockets Layer must be enabled before configuring the shared secret needed for SNMPv3.

2.7.4.9. Port 389, LDAP

This is the standard LDAP port used for address book queries in the Scan to Email, and for LDAP authentication into the Active Directory feature.

2.7.4.10. Port 427, SLP

When activated, this port is used for service discovery and advertisement. The device will advertise itself as a printer and also listen for SLP queries using this port. It is not configurable. This port is explicitly enabled / disabled in the Properties tab of the device's web pages.

2.7.4.11. Port 443, SSL/HTTPS

This is the default port for Secure Sockets Layer communication. This port can be configured via the device's web pages. SSL must be enabled before setting up either SNMPv3 or IPSec. SSL must also be enabled in order to use any of the Web Services (Automatic Meter Reads, or Network Scanning Validation Service).

SSL should be enabled so that the device can be securely administered from the web UI. When scanning, SSL can be used to secure the filing channel to a remote repository.

SSL uses X.509 certificates to establish trust between two ends of a communication channel. When storing scanned images to a remote repository using an https: connection, the device must verify the certificate provided by the remote repository. A Trusted Certificate Authority certificate should be uploaded to the device in this case.

To securely administer the device, the user's browser must be able to verify the certificate supplied by the device. A certificate signed by a well-known Certificate Authority (CA) can be downloaded to the device, or the device can generate a self-signed certificate. In the first instance, the device creates a Certificate Signing Request (CSR) that can be downloaded and forwarded to the well-known CA for signing. The signed device certificate is then uploaded to the device. Alternatively, the device will generate a self-signed certificate. In this case, the generic Xerox root CA certificate must be downloaded from the device and installed in the certificate store of the user's browser.

The device supports only server authentication.

2.7.4.12. Port 445, SMB/CIFS

This port is used by the SMB/CIFS protocol for exporting scanned images and associated data if NetBIOS is not supported by the repository OS. The port is only open when the files are being stored to the server.

2.7.4.13. Port 515, LPR

This is the standard LPR printing port, which only supports IP printing. It is a configurable port, and may be explicitly enabled or disabled in the Properties tab on the Web UI.

2.7.4.14. Port 546, DHCPv6

This port is used only when performing DHCPv6, and is not open all of the time. To permanently close this port, DHCPv6 must be explicitly disabled. This is done via the TCP/IP page in the Properties tab on the Web UI.

2.7.4.15. Port 631, IPP

This port supports the Internet Printing Protocol. It may be explicitly enabled or disabled in the Properties tab on the Web UI. This is disabled when the http server is disabled.

2.7.4.16. Port 636, sLDAP

This is the standard LDAP port when using SSL for address book queries in the Scan to Email feature.

2.7.4.17.Port 3003, http/SNMP reply

This port is used when the http server requests device information. The user displays the Web User Interface (WebUI) and goes to a page where the http server must query the device for settings (e.g. Novell network settings). The http server queries the machine via an internal SNMP request (hence this port can only open when the http server is active). The machine replies back to the http server via this port. It sends the reply to the loopback address (127.0.0.0), which is internally routed to the http server. This reply is never transmitted on the network. Only SNMP replies are accepted by this port, and this port is active when the http server is active (i.e. if the http server is disabled, this port will be closed). If someone attempted to send an SNMP reply to this port via the network, the reply would have to contain the correct sequence number, which is highly unlikely, since the sequence numbers are internal to the machine.

2.7.4.18.Port 5200, UPnP/SSDP

This port is used by SSDP and UPnP. It can be disabled in the Properties tab on the Web UI.

2.7.4.19.Port 5353, Multicast DNS

Designating a Multicast DNS server will allow the device to resolve domain names over a multicast protocol. This port can be disabled in the Properties tab on the Web UI.

2.7.4.20.Port 8018, WSD

This port is used for WSD print and scan. This is a configurable port, and may be disabled in the Properties tab of the device's web pages.

2.7.4.21.Port 9100, raw IP

This allows downloading a PDL file directly to the interpreter. This port has limited bi-directionality (via PDL back channel) and allows printing only. This is a configurable port, and may be disabled in the Properties tab of the device's web pages.

2.7.5. IP Filtering

The devices contain a static host-based firewall that provides the ability to prevent unauthorized network access based on an IP address or IP address range. Filtering rules can be set by the SA using the WebUI.

3. System Access

3.1. Authentication Model

The authentication model allows for the following:

- Network Authentication: Provides access to the walk-up user services. User network credentials are used to authenticate the user at the network domain controller.
- Authorization: Provides two levels of access to the CentreWare Internet Services and to the Local User Interface: system administrator and all users.

3.2. Login and Authentication Methods

There are a number of methods for different types of users to be authenticated. In addition, the connected versions of the product also log into remote servers. A description of these behaviors follows.

3.2.1. System Administrator Login

The device can be configured to require a 4 digit PIN to access the Tools via the Local UI. This PIN is stored in the controller NVM and is inaccessible to the user. Xerox strongly recommends that this PIN be changed from its default value immediately upon product installation. The same PIN is used to access the Administration screens in the Web UI.

3.2.2. User authentication (WorkCentre 3615 only)

Users may authenticate to the device using Kerberos, or LDAP Domain authentication protocols. Once the user is authenticated to the device, the user may proceed to use the walk-up user services to which they have access.

The WebUI allows an SA to set up a default authentication domain.

Kerberos Authentication (Windows only)

This is an option that must be enabled on the device, and is used in conjunction with all walk-up user services. The authentication steps are:

- 1) A User enters a user name and password at the device in the Local UI. The device sends an authentication request to the Kerberos Server.
- 2) The Kerberos Server responds with the encrypted credentials of the user attempting to sign on.
- 3) The device attempts to decrypt the credentials using the entered password. The user is authenticated if the credentials can be decrypted.
- 4) The user may then add recipient addresses by accessing the Address Book on the LDAP server. Please see the User Manual for details. Each addition is a separate session to the LDAP server.

LDAP authentication (Windows only)

This is an option that must be enabled on the device, and is used in conjunction with all walk-up user services. The authentication steps are:

- 1) A User enters a user name and password at the device in the Local UI. The device sends an authentication request to the LDAP Server.
- 2) The LDAP Server responds with the encrypted credentials of the user attempting to sign on.
- 3) The device attempts to decrypt the credentials using the entered password. The user is authenticated if the credentials can be decrypted.
- 4) The user may then add recipient addresses by accessing the Address Book on the LDAP server. Please see the User Manual for details. Each addition is a separate session to the LDAP server.

3.2.2.1. DDNS

The implementation in the device does not support any security extensions.

3.3. System Accounts

3.3.1. Printing

The device may be set up to connect to a print queue maintained on a remote print server. The login name and password are sent to the print server in clear text. IPSec should be used to secure this channel.

3.3.2. Network Scanning (WorkCentre 3615 ONLY)

Network Scanning may require the device to log into a server. The instances where the device logs into a server are detailed in the following table. Users may also need to authenticate for scanning. This authentication is detailed in subsequent sections.

3.3.2.1. Device log on

| Scanning feature | Device behavior |
|------------------|---|
| Scan to Network | The device logs in to the scan repository as set up by the SA via CWIS. |
| Scan to E-mail | <p>The device logs into an SMTP Server as set up by the SA via CWIS. It will only log into the Server when a user attempts to use the scan-to-email feature. At the time the LDAP server must be accessed, the device will log into the LDAP server.</p> <p>The device uses simple authentication on the SMTP server. A network username and password must be assigned to the device. The device logs in as a normal user, with read only privileges. User credentials are not used for this authentication step, and are never transmitted over the network.</p> |

Table 8 Device Log On for Scanning Features

Please note that when the device logs into any server the device username and password are sent over the network in clear text unless SSL has been enabled or IPSec has been configured to encrypt the traffic.

3.4. Diagnostics

To access onboard diagnostics from the local user interface, Xerox service representatives must use a unique key button press combination. This PIN is the same for all product configurations and cannot be changed.

4. Security Aspects of Selected Features

4.1. Port Control for USB ports

As the USB ports on the device can be used to plug in a USB drive from which files may be printed and also be used to scan documents to a USB drive, depending on the environment or data processed by the device, this may be a security issue. When configured by the System Administrator, USB ports may be turned off to enhance security.

4.2. Encrypted Partitions

The secure partitions of the optional SD Card are encrypted using the AES algorithm with a 256-bit key. The key is generated dynamically on each boot, and is kept only in volatile memory. Encryption is enabled by default and cannot be disabled.

4.3. Clear Device Memory

A manual overwrite function is available to clear the device memory at any time. With digital media there is no residual charge left behind when information is erased. Performing one overwrite cycle will remove all data.

5. Responses to Known Vulnerabilities

5.1. Security @ Xerox (www.xerox.com/security)

Xerox maintains an evergreen public web page that contains the latest security information pertaining to its products. Please see www.xerox.com/security.

6. APPENDICES

6.1. Appendix A – Abbreviations

| | |
|--------------------|--|
| API | Application Programming Interface |
| ASIC | Application-Specific Integrated Circuit. This is a custom integrated circuit that is unique to a specific product. |
| CAT | Customer Administration Tool |
| CSE | Customer Service Engineer |
| DADF/DADH | Duplex Automatic Document Feeder/Handler |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name Server. A centralized database that maps host names to static IP addresses. |
| DDNS | Dynamic Domain Name Server. Maps host names to dynamic static IP addresses. |
| DRAM | Dynamic Random Access Memory |
| EEPROM | Electrically erasable programmable read only memory |
| EGP | Exterior Gateway Protocol |
| GB | Gigabyte |
| HP | Hewlett-Packard |
| HTTP | Hypertext transfer protocol |
| IBM | International Business Machines |
| ICMP | Internet Control Message Protocol |
| IETF | Internet Engineering Task Force |
| IFAX | Internet Fax |
| IIT | Image Input Terminal (the scanner) |
| IT | Information Technology |
| IOT | Image Output Terminal (the marking engine) |
| IP | Internet Protocol |
| IPSec | Internet Protocol Security |
| LAN | Local Area Network |
| LDAP | Lightweight Directory Access Protocol |
| LDAP Server | Lightweight Directory Access Protocol Server. Typically the same server that is used for email. It contains information about users such as name, phone number, and email address. It can also include a user's login alias. |
| LED | Light Emitting Diode |
| LPR | Line Printer Request |
| LUI | Local User Interface |
| MAC | Media Access Control |
| MIB | Management Information Base |
| n/a | not applicable |
| NOS | Network Operating System |
| NVRAM | Non-Volatile Random Access Memory |
| NVM | Non-Volatile Memory |
| PCL | Printer Control Language |
| PDL | Page Description Language |
| PIN | Personal Identification Number |
| PWBA | Printed Wire Board Assembly |



| | |
|--------------|--|
| RFC | Required Functional Capability |
| SA | System Administrator |
| SNMP | Simple Network Management Protocol |
| SRAM | Static Random Access Memory |
| SSDP | Simple Service Discovery Protocol |
| SSL | Secure Sockets Layer |
| TCP | Transmission Control Protocol |
| UI | User Interface |
| URL | Uniform Resource Locator |
| UDP | User Datagram Protocol |
| WebUI | Web User Interface – the web pages resident in the WorkCentre Pro. These are accessible through any browser using the machine's IP address as the URL. |
| XCFI | Xerox Common Management Interface |



6.2. Appendix B – Supported MIB Objects

NOTES :

- (1) The number of objects shown per MIB group represents the number of objects defined by the IETF standard for that MIB group. It does not represent the instantiation of the MIB group which may contain many more objects.
- (2) Some MIB objects defined within Input and Output groups of the Printer MIB (RFC 1759) have a MAX-ACCESS of RW. However, the Printer MIBv2 defines a MIB-ACCESS of RO for these MIB objects within the Input and Output groups and all machines assessed support RO access. Therefore, RO access to these MIB objects is considered IETF compliant.
- (3) It is assumed that mandatory IETF string-related MIB objects shall contain meaningful data; not blank strings
- (4) The "(C)" notation indicates that the previously stated item is a true caveat condition. The "(I)" notation indicates that the previous stated item should be regarded as information only.
- (5) MIB objects that CANNOT be populated with meaningful data (e.g. a machine may not have paper level sensors, hence, can only support "0" or "-3 for more than 1 sheet" for prtInputCurrentLevel) will be considered a caveat, denoted as "(C)".
- (6) The Printer MIB requires a few groups from RFC 1213 and RFC 1514 to be supported. Therefore, this assessment will indicate that these groups are "supported" as long as the basic MIB structures have been implemented.

| SNMP version / Network Transport support | WorkCentre |
|--|------------|
| SNMPv1 (RFC 1157) | supported |
| SNMPv2P (RFCs 140x) | supported |
| SNMPv2C (RFCs 190x) | supported |
| SNMPv3 (RFCs 1902, 2572, 2574) | supported |
| SNMP over UDP (IP) | supported |

| RFC 1759 - Printer MIB Group | WorkCentre |
|--|--|
| RFC 1213 - System group | supported |
| RFC 1213 - Interface group | supported |
| RFC 1514 - Storage group | supported |
| RFC 1514 - Device group | supported |
| General group [7 objects] | supported |
| Covers group [3 objects] | supported |
| Localization group [4 objects] | supported (only US English language supported) |
| System Resources group [4 objects] | supported |
| Input group [12 objects] | supported |
| Extended Input group [7 objects] - OPTIONAL | supported |
| Input Media group [4 objects] - OPTIONAL | supported |
| Output group [6 objects] | supported |
| Extended Output group [7 objects] - OPTIONAL | supported |
| Output Dimensions group [5 objects] OPTIONAL | supported |
| Output Features group [6 objects] - OPTIONAL | supported |
| Marker group [15 objects] | supported |
| Marker Supplies group [9 objects] - OPTIONAL | supported |
| Marker Colorant group [5 objects] - OPTIONAL | supported |
| Media Path group [11 objects] | supported |
| Channels group [8 objects] | supported |
| Interpreter group [12 objects] | supported |
| Console group [4 objects] | supported |
| Console Display Buffer group [2 objects] | supported |
| Alert Table group [8 objects] | supported |
| Alert Time group [1 object] - OPTIONAL | supported |

| RFC 1514 – Host Resources MIB group | WorkCentre |
|-------------------------------------|------------|
| System group [7 objects] | supported |
| Storage group [8 objects] | supported |
| Devices group [6 objects] | supported |

| RFC 1514 – Host Resources MIB group | WorkCentre |
|-------------------------------------|---------------|
| Processor Table [2 objects] | supported |
| Network Interface Table [1 object] | Not supported |
| Printer Table [2 objects] | supported |
| Disk Storage Table [4 objects] | supported |
| Partition Table [5 objects] | Not supported |
| File System Table [9 objects] | supported |

| RFC 1213 - MIB-II for TCP/IP group | WorkCentre |
|--|---|
| System group [7 objects] | supported |
| Interfaces group [23 objects] | supported |
| Address Translation group [3 objects] | supported, but this group has been DEPRECATED by the IETF |
| IP group [42 objects] | supported |
| ICMP group [26 objects] | supported |
| TCP group [19 objects] | supported |
| UDP group [6 objects] | supported |
| EGP group [20 objects] | not applicable because Exterior Gateway Protocol not supported by machine |
| Transmission group [0 objects] | not applicable because the group has not yet been defined by the IETF |
| SNMP group [28 objects] | supported |
| System Object Resources Table/objects per RFC 1907 [8 objects] | supported |

| Additional Capabilities / Application Support | WorkCentre |
|--|--|
| ability to change GET, SET, TRAP PDU community names | supported |
| Printer MIB traps | supported = printerV1Alert, printerV2Alert |
| SNMP Generic Traps | supported = coldStart, warmStart, authenticationFailure |
| Vendor-specific Traps | supported = xcmJobV1AlertNew, xcmJobV2AlertNew for job monitoring alerts |
| set trap destination address(es) for any 3rd party Net Mgmt apps. | supported via Web UI |
| polling for IETF status objects using any 3rd party Net Mgmt apps. | supported |
| walking IETF MIB tree structure using any 3rd party Net Mgmt app. (e.g. HP OpenView, etc.) / shareware program | supported |
| New type 2 enumerations from next generation Host Resources MIB supported | optional, not supported because Host Resources MIBv2 has NOT entered the standards track |
| New type 2 enumerations from next generation Printer MIB supported | supported |
| New Printer MIBv2 objects implemented | optional, not support because Printer MIBv2 has NOT entered the standards track |

Table 9 Supported MIB Objects

6.3. Appendix C –Standards

Controller Software

| Function | RFC/Standard |
|---|------------------------------------|
| Internet Protocol | 950 |
| Internet standard subnetting procedure | 919 |
| Broadcasting internet datagrams | 922 |
| Transmission Control Protocol (TCP) | 793 |
| User Datagram Protocol | 768 |
| Standard for the transmission of IP datagrams over Ethernet networks | 894 |
| Standard for the transmission of IP datagrams over IEEE802 networks | 1042 |
| ICMP – ICMP Echo, ICMP Time, ICMP Echo Reply, and ICMP Destination Unreachable message. | 792 |
| Reverse Address Resolution Protocol (RARP) | 903 |
| Bootstrap Protocol (BOOTP) | 951 |
| Clarifications and Extensions for the Bootstrap Protocol (BOOTP) | 1542 |
| X.500 Distinguished Name RFC references | 1779, 2253, 2297, 2293 |
| SLP | 2608 |
| Dynamic Host Configuration Protocol (DHCP) | 2131 |
| DHCP Options and BOOTP Vendor Extensions | 2132 |
| X.509 Certificate RFC references | 2247, 2293, 2459, 2510, 2511, 3280 |
| Hyper Text Transfer Protocol version 1.1 (HTTP) | 2616 |
| Line Printer Daemon (LPR/LPD) | 1179 |
| File Transfer Protocol (FTP) | 959 |
| SNMPv1 | 1157 |
| SNMPv2 | 1901, 1905, 1906, 1908, 1909 |
| Structure of Management Information (SMI) for SNMPv1 | 1155, 1212 |
| Structure of Management Information (SMI) for SNMPv2 | 1902, 1903, 1904 |
| IETF MIBs: | |
| MIB II | 1213 |
| Host Resources | 1514 |
| RFC 1759 (Printer), Printer MIB V2 | 1759 |
| SNMP Traps | 1215 |
| Document Printing Application (DPA) | 10175 |

Table 10 Controller Software

Printing Description Languages

PostScript
PCL5 (PCL5e and PCL5c)
PCL6 (PCL XL)
Portable Document Format
Tagged Image File Format
XML Paper Specification
IBM/Epson

6.4. Appendix E – References

| | |
|-----------------|---|
| Kerberos FAQ | http://www.cmf.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html |
| IP port numbers | http://www.iana.org/assignments/port-numbers |