



AN LDAP PRIMER

This Flexible Communication Protocol Works Behind the Scenes, Making Scan to E-Mail a Seamless Process

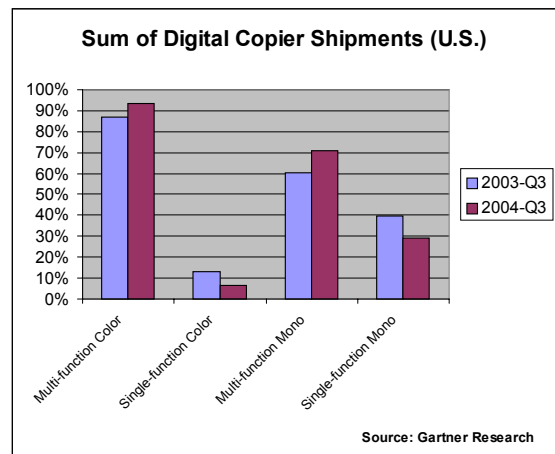
by: Denine Phillips, Tech-Write, LLC

“One of the primary reasons network scanning was incorporated within an MFP platform was to enable organizations to improve document workflow on an enterprise level,” says Ken Weilerstein, research vice president at Gartner (Stamford, CT). “And, with more than half of all copiers being sold as a multifunctional system, not just a single-function copier, it’s critical that dealers get a good feel for what’s going on in terms of their customers’ workflow.”

Indeed, network scanning, particularly the ability to *scan-to-email*, has simplified the conversion of paper-based documents into shared electronic data. Today digital copiers, high-end fax systems, and even desktop network scanners have been transformed into versatile “scan-to” hubs for busy offices, both large and small.

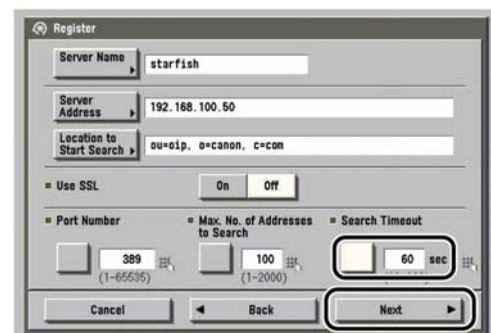
Whether placed as workgroup or departmental systems, color or monochrome, walk-up users can easily capture and distribute information that expedites communication with colleagues, customers, clients and suppliers. The bottom-line benefits include time savings (higher productivity) and lower costs, specifically streamlined workflow and reduced reliance on costly forms of communication, for instance, PSTN fax and overnight courier.

That said, it’s no wonder that inclusion of scan-to-email capabilities on the MFP platform has grown exponentially over the past few years. And, unbeknownst to many, a communication protocol called LDAP, Light-weight Directory Access Protocol, is working behind the scenes to make scan-to-email a seamless process. (For a list of LDAP-complaint, offered by Canon, Panasonic, Ricoh and Sharp, please see page 4.)



The LDAP Connection

“The beauty of LDAP is that it’s an industry standard and many products, including Canon imageRUNNER MFPs support it,” explains Nick Del Re, director of professional services, Canon U.S.A., Inc. And, he adds, “LDAP has a well-defined structure on how to query information from an LDAP-compliant directory. Examples of LDAP compliant directories include Microsoft’s Active Directory and Novell’s NDS. Canon’s Universal Send allows a user to search and retrieve e-mail addresses from an LDAP directory server. LDAP also supports various methods for communicating over the network, some send information over clear text, others encrypt data to protect information. On Canon’s MEAP platform, our Software Development Kits provide access to functions, such as LDAP over SSL (Secure Sockets Layer), to protect sensitive information, like user names and passwords, when performing authentication. SSL is the technology that is commonly used today for on-line banking via the Internet.”



Canon: LDAP Configuration Screen

How Does LDAP Work?

George Grafanakis, senior manager, product planning and marketing for Sharp Document Solutions Company of America says, "Much like HTTP (HyperText Transfer Protocol) allows computer users to access and search the World Wide Web, our LDAP-compliant Sharp MFPs allow a key operator to access and search e-mail addresses stored on one or more LDAP servers. Over a network, on a TCP/IP connection, LDAP support makes it easy for users to send e-mail without having to type an entire e-mail address through the control panel, which saves time. Grafanakis goes on to say that corporate environments typically run their own mail server and Global Address Book, so MFP users theoretically have immediate access to hundreds, possibly thousand of e-mail addresses. Of course, the Sharp MFP itself displays just a fixed number of the addresses returned after a search, a number that is based on user configuration settings.

Canon's Del Re notes that the IETF (Internet Engineering Task Force) developed the LDAP standard with specific guidelines as to how to perform a search on an LDAP directory. "The parameters of a search can be filtered down to facilitate finding information such as, e-mail address, or fax number," he says.

Is LDAP Widely Accepted?

According to Ron Albeck, senior manager, advanced imaging solutions group, Ricoh Corporation, "LDAP has gained widespread acceptance as the preferred directory access method and is supported by Microsoft, Novell, Netscape, IBM, Lotus, and many other software companies. He adds, "Ricoch Aficio MFPs that support network scanning are LDAP complaint and our document solutions, such as GlobalScan, offer secure LDAP directory look-up functionality as well. This provides the user with a fast, intuitive way to select e-mail recipients from the touch-screen display. Users are already comfortable with the copier features, we simply added the Scanner button to support



scan-to-email, scan-to-folder, scan-to-FTP, scan-to-HDD, as well as other functions."

Sharp: LDAP Implementation on MFP

How Do You Scan-to-Email?

"Scanning to e-mail, for instance via the GlobalScan system, is as easy as sending a fax," says Albeck. As he further details the process, the user presses the Scanner button, authenticates by entering a user name and password (via the QWERTY soft keyboard), if necessary, and presses the "E-mail Document" button. Entry of a "Subject" and "Document Name" is optional. Next, the user can search the Global Address Book by pressing "Lookup by Name," enter a few characters of the recipient's name and press "Search." An unlimited number of matching e-mail addresses is returned. The user simply scrolls and selects the desired addresses (see *Illustration 1*). The process is repeated to perform another search, or the "Start" button is pressed, initiating the scan. Of course, ad hoc (manual) entry of an e-mail address is possibly when communicating outside an organization, that is, to addresses not stored in the global address book.

Illustration 1



Ricoh: GlobalScan's LDAP Search Results on MFP

Why Authenticate?

No discussion of LDAP is complete without addressing authentication. Sharp's Grafanakis says, "LDAP and authentication work hand in hand. For instance, if 'device authentication' is enabled, every query of an LDAP directory server must first be 'authenticated,' which simply verifies that the MFP used to send the e-mail is a authorized device on the network. User authentication, combined with 'device authentication,' also requires the user to be identified, not just the MFP, so the operator must log in with a valid user name and password. This grants that individual access to the database of e-mail addresses in the Global Address Book, as well as access to the outbound mail server."

As Bob Curci, Panasonic's senior product marketing specialist notes, "Authentication is most commonly deployed in network scanning applications, such as scan-to-email, because you don't want confidential documents, like a P&L ledger -- that's just sitting on someone's desk -- being e-mailed anonymously. If this were to occur under authentication, the administrator could retrieve data detailing the history of scans on that particular MFP." The ability to track e-mail communication through an authentication log is cited by Lanier's product marketing manager, Dane Browning, as a major benefit to large organizations. "Authentication leaves a footprint by identifying exactly who have been using the scan-to-email function by sender, date, time and recipient."

"Authentication also prevents transmission of anonymous e-mails, something which is a concern to many companies," says Gartner's Weilerstein. "The trend is toward better management of MFPs, as well as improved security, and authentication plays a major part. For businesses we talk to, they don't want users sending untraceable e-mails that are viewed as spam by the receiver. We've been taught to delete suspicious e-mail, especially those with attachments. That's what would happen if a message were sent from an MFP without the sender being identified." Weilerstein suggests that buyers look into whether the MFP identifies the initiator to the recipient and, if so, how." He clarifies by saying, "I would not assume that an MFP capable of LDAP lookup necessarily inserts a return address for the sender."

It's important to note that most MFP users must be authenticated before accessing an LDAP server. Some high-end systems may even employ authentication by user or group, for instance employee/group A can only access walk up copier features, and employee/group B can utilize copier, printer, scanner and fax functions. Hence, authentication can be highly customizable on the MFP.

Risks to Information Security

Surprisingly, some organizations choose to not implement authentication on their network-connected MFPs. Such unrestricted access to the device has its hazards. Companies are vulnerable to potential abuse of valuable network resources and/or theft of proprietary information. Andrew in accounting could scan credit card data to his home e-mail address and Mary in marketing could print 100 color copies of her resume.

One vendor reported that approximately 60% of the scan-enabled multifunctional products his company had placed did not have the authentication feature enabled.
Source: *Digital Imaging Review*, BLI, 9/04

Admittedly, a user name and password is a basic authentication scheme, one that simply verifies that a user is who they say they are, and won't prevent the aforementioned scenarios. Authentication will, however, reduce risks by causing people who wish to undermine a business' interests to think twice.

Conclusion

With the LDAP basics covered, how do you determine if a product is LDAP compliant? Take a close look at the last page of the brochure, generally the specification page, and under "Communication protocols," along with TCP/IP, SMTP, POP3, MIME, DHCP, NDS, PKI, SNMB and MIB, you may find LDAP. Clearly, as part of a growing list of Internet protocols, LDAP has become an indispensable standard for helping build robust, interoperable MFP platforms. In turn, dealers are able to deploy scalable office solutions that meet their customers' diverse imaging and document distribution needs today, tomorrow and beyond.

###

Denine Phillips, of Tech-Write, Annandale, New Jersey, is an office technology consultant and free-lance writer. She can be reached for questions or comments via e-mail: denine.phillips@tech-write.biz, or her Web site: www.tech-write.biz.

© Copyright 2005 by Tech-Write. All Rights Reserved.

Copier-based Products / LDAP-Compliance		
	Model	Requirements
Canon*	iRC3100 / C3100N	With Optional Universal Send
	iRC5800 / C6800	With Optional Universal Send
	iR2270 / 2870 / 3570 / 4570 / iR2220N / 2220i / 3320N / 3320i / iR5020 / 5020i / 6020 / 6020i / iR8070 / 9070 / 105+ / CiR C3220	With Optional Universal Send & supported within MEAP*
	imageCLASS C2500/C3500	Standard
Panasonic	DP-190	Standard
	DP-1820 through DP-6030	With Optional Internet Fax Kit
	DP-6530 / 8130	With Optional Print Controller
Ricoh**	Aficio 1224C / 1232C Aficio 2022 / 2027 / 2035 / 2045 Aficio 2051/ 2060 / 2075 Aficio 3800 / CL7000CMF	With Optional Print/Scan Kit
	Aficio 2022SP / 2027SP Aficio 2232C / 2238C Aficio 2035e SP / 2045e SP Aficio 2060SP / 2051SP / 2075SP Aficio 2090 / 2105	Standard
Sharp	AR-M168S / M168D	With Optional AR-NB2N Network Kit
	AR-M160 / M205	With Optional AR-NB2N Network Kit (through web page only)
	AR-M162 / M207	With Optional AR-NB3 Network Kit
	AR-M237 / M277	With Optional AR-P17 Print Controller + AR- NS2 Network Scanning Kit
	AR-M350N / M450N	With Optional AR-NS2 Network Scanning Kit
	AR-M355N / M455N / M550N / M620N / M700	With Optional AR-NS3 Network Scanning Kit
	AR-BC260 / BC320	Standard
AR-C330	With Optional AR-PE3 EFI Controller	

* LDAP is supported within Canon's MEAP platform. MEAP is an application development platform that allows the creation of embedded applications for Canon multifunctional peripheral devices. That is, custom applications can be created to execute on the device itself.

** Ricoh's Embedded Software Architecture™ SDK (Software Development Kit) offers System Integrators and Value-added Resellers the opportunity to customize Ricoh, Savin, Gestetner and Lanier MFPs and LPs (laser printers) to meet special document workflow requirements, including support for LDAP.

Additional Resources

For detailed information on a specific version of LDAP, go to www.google.com and enter the RFC (Requests for Comments) number, as follows...

- RFC 1487 [LDAPv1 (July, 1993)]
- RFC 1777 [LDAPv2 (March, 1995)]
- RFC 2251 [LDAPv3 (March, 1999)]