GLOSSARY

802.11b/g/n - The number 802.11 is the IEEE (Institute of Electrical and Electronics Engineers) term for the wireless signal on a land area network (WLAN). The letters that follow indicate the levels of strength. The following lists the maximum throughputs for b and g:

- b = 11 Mb/s
- g = 54 Mb/s

n is the most recent protocol:

- n = well over 50 Mb/s

AFP (Apple Filing Protocol) - Similar to SMB/CIFS and NFS, AFP is a protocol used for requests over a network. Requests could mean accessing shared files, volumes, and devices (such as printers). AFP is used for Apple-based systems, Mac OS 9 and X.

DHCP (Dynamic Host Configuration Protocol) - A computer requires an identity when it connects to a network, otherwise access to the Internet as well as company or home servers will not be possible. That identity is called an IP (Internet Protocol) address, which may be enabled manually (Static IP) in the operating system network settings or assigned by a network management device, such as a DHCP device. Though a generic term, the device could be a server or an active switch, as found in business environments; or, a cable or DSL modem offered by an Internet provider. The LaCie product has the ability to assign IP addresses dynamically, which means it can be configured as a DHCP server. An example of an IP address is 192.168.10.1

DHCP Server Range Start IP/Range End IP - The range of addresses that a DHCP server may assign to the attached systems.

DLNA™ (Digital Living Network Alliance) - A standard (based on UPnP) widely embraced by consumer electronic manufacturers to allow entertainment devices within the home to share movies, music, and photos across a home network.

DNS (Domain Name System or Domain Name Server) - All email and web addresses are domain names. Every web site and email account has a specific place within a server that has a unique IP address (such as 192.168.54.25, IPv4; or 2001:db8:1f70::999:de8:7648:6e8, IPv6). However, when we launch a favorite browser to buy a new hard drive or send an email, we do not type lengthy, hard to remember numerical addresses. Instead, we use company names, www.lacie.com, or email addresses, sales@lacie.com. The domain names in these examples are “lacie.com” or ”@lacie.com”. The server manages the tie between the IP address it requires for a network identity and the domain name for communication.

DSL (Digital Subscriber Line) - Broadband data transmitted digitally over telephone wires. The local telephone company provides a service that includes Internet, telephone, and, for some, cable television. For access to the Internet, telephone companies generally provide an adapter or DSL modem for connection to a computer via Ethernet.

Dynamic DNS - This moves DNS hosting a bit further as it provides access to domain names hosted on servers with varying (hence, dynamic) IP addresses. This means that web sites are not forced to maintain a single IP address, but can be managed within a network that uses DHCP to assign an identity. The Dynamic DNS host is smart enough to read the domain name and find the IP address to which it belongs. Dynamic DNS is a great tool for accessing home network servers, such as the LaCie product, from anywhere outside the home.

Dynamic Port Forwarding - Allows applications to use SOCKS servers on local ports for network communication and Internet access. This can be very convenient as it will avoid having to configure port forwarding each time an application is used. The SOCKS is configured on a server to route traffic while the application, such as a web browser, is assigned a SOCKS in its preferences.

External Port - This port deals with requests outside the LAN, working with the NAT (network address translation) to convert external IP addresses and port numbers to addresses that will be accepted inside the network.

Firewall - One or more programs that act in concert with the gateway server to protect the computers and systems within a network.

Frame - A frame comprises all the data that is sent between network points, including the addressing and network protocol information.

FTP (File Transfer Protocol) - A protocol used to transfer and exchange files over networks that use TCP/IP. With FTP, one person can copy files into a folder within an FTP server for others to access. Permissions are generally set so that anyone seeking to access the files must enter a username and password.

FTP Server - A server that acts as the "host" for FTP transfers and exchanges. A server, such as the LaCie product, can enable FTP access to files stored on its volume(s). The LaCie product can act as an FTP server, allowing the user, or friends and family, to access its files or volumes by Internet hyperlinks. The base addresses are: ftp://IP-address, such as ftp://192.168.15.24; and ftp://username:password@<ip or machine name>/.

Gateway - See Network Gateway

HTTP (Hypertext Transfer Protocol) - The most common protocol for the World Wide Web (the "www" in web addresses). HTTP is a command that aids in defining the messaging for Web servers and browsing, initiating the request to a particular address.

HTTPS (Hypertext Transfer Protocol Secure) - A secure level of HTTP that uses SSL protocol for encryption and identification. Very often seen with online financial websites or when making a purchase on the Internet.

HTTPS Certificate - A digital certificate verifies the identity of a web site or user. When a user logs onto the site, the browser will automatically accept the certificate and indicate that the site is secure (often graphically represented by a lock). HTTPS certificates may be purchased and/or generated from many online vendors.

ICMP (Internet Control Message Protocol) - Another level of address communication, along with TCP and UDP. However, this level is generally not used to send and receive messages between servers or computers. ICMP is implemented mostly for error messages, such as a Web site being unavailable, or the popular ping feature used to search for other IP addresses on a network.

Internal Port - This port deals with requests inside the LAN, such as accessing files or sending emails.

Internet Provider - Broadband Internet service is available with a cable modem provided by the local cable provider. The cable modem is linked to the computer via an Ethernet cable.

IP Address (Internet Protocol) - Each computer must have at least one unique identity to engage in a form of network communication. The IP address has multiple layers that allow a computer to send and receive data, whether looking for web sites on the Internet from home or sending e-mail to a colleague at work.

IPv4 - The most common form of network addressing used today, IPv4 is 32-bit. The format is easily recognizable as xxx.xxx.xxx.xxx, where each "x" only represents the maximum digits in each field between periods. An IPv4 address can be 192.168.1.1 or 84.22.291.652. The maximum number of combinations reaches well over four billion. Even so, due to a world that has become dependent on Internet communication, IPv4 addressing is becoming difficult to maintain.

IPv6 - To combat the seeming inevitability of IPv4 addressing reaching its worldwide limit, IPv6 now offers much larger 128-bit addressing. Examples of the longer length are often seen as xxxx:xxxx:xxx:xxxx:xxx:xxxx:xxxx:xxxx, where "x" can be a letter or a number. However, it is not necessary to use four digits in all eight fields and the address can be truncated when heavily populated with zeros. IPv6 is flexible in understanding the address even when cutting back on leading zero digits or using a double colon to remove them altogether. The address below is an example of the same network identity in all its permutations:

2001:0f34:0000:0000:0000:0000:2002:04fe

2001:f34:000:000:000:000:2002:4fe

2001:f34:00:00:00:00:2002:4fe

2001:f34:0:0:0:0:2002:4fe

2001:f34::2002:4fe

Note that the double colons can be used to replace whole fields that contain only zeros.

ISP (Internet Service Provider) - The service that has installed a cable or DSL modem in a home or business for access to the Internet.

iTunes™ Server - iTunes libraries can be shared over a local network via a computer, network disk, or network device that acts as the iTunes Server. The protocol is used to detect libraries on the computer, network disk, or network device and stream playlists to anyone who requests them. The function must also be enabled on each computer that runs iTunes.

iTunes™ Scan Interval - Periodic scans of the shared music libraries for updates. For example, a LaCie network device automatically performs an iTunes once every 24 hours.

LAN (Local Area Network) - A network within a small or limited geography, such as an office, a school, or a home.

MAC Address (Media Access Control) - A unique identifier assigned by the manufacturer of a computer's network interface card. Though it has a different naming structure, a MAC address works with the IP address for network communication. There are many layers of network communication but, as an oversimplification, the MAC address supports the hardware aspect while the IP deals with the software implementation. An IP address can change while a MAC address is almost always fixed. A MAC address can generally be found in the operating system network settings, also referred to as an ethernet address, hardware address, adapter address, or physical address. The naming structure can be listed in two ways:

MM:MM:MM:SS:SS:SS or MM-MM-MM-SS-SS-SS

The "M" half of the address represents code used to identify the manufacturer of the network interface while the "S" half is a serial number. For example, a common manufacturer "M" prefix is, 00A0C9 since it represents Intel®. A full MAC address example is 00:23:df:99:5e:2a, with 00:23:df pointing to Apple as the manufacturer.

MAC Address Cloning - Internet service providers (ISP) may limit the amount of network connections by counting MAC addresses. Upon seeing more than an arbitrary number of MAC addresses on your home network, access will be denied to additional devices. MAC address cloning enables a router or network device to create a single MAC address for the ISP to see while it manages the computers that are attached via Ethernet or Wi-Fi.

NAT (Network Address Translation) - A router will take addresses that come from public servers and translate them to addresses that are acceptable to the private network. This is helpful for reducing the number of IP addresses on a network or directing welcome traffic into a private network while dismissing unwanted visitors.

NAT-PMP (Network Address Translation-Port Mapping Protocol) - Taking port forwarding a step further, this allows users in a private network to automate network address translation by port number. Addresses outside the private network include a port number that mark them as acceptable. NAT-PMP converts "good" traffic into acceptable IP address within the system.

Netmask - Also known as the subnetwork. A subnet address is part of the IP address information, generally placing a network geography onto one or more computers. That is, everyone with a certain subnet address is hosted or attached to a specific server. A subnet mask has an address listing similar in form to IPv4. A common subnet mask (as it is called in the operating system preferences) is: 255.255.255.0.

Network Gateway - Capable of operating in software, hardware, or a combination of the two, a network gateway assists in enabling communication between networks with different protocols. Often, the network gateway is the Internet access device (such as a broadband router) provided by the ISP. An example would be one network that is using TCP/IP, while a second runs AppleTalk and a third, UDP. The network gateway assures that the translation process between them is transparent to the user.

NTP Server (Network Time Protocol) - A protocol used to synchronize the time for computers that reside on the same network. Public NTP servers are also available on the Internet.

Port Forwarding - Since a port number is part of a network address, it is possible to target specific IP addresses by their port numbers. This way, remote computers or devices with IP addresses can shake hands with a particular address on a LAN. A real world example is a Playstation®3 being used for an online game. That particular game may demand a specific IP address and port number for its network communication.

Port Number - Another layer of network addressing that works with protocols such as TCP/IP or UDP/IP. A port number is represented by a number ranging from 0 to 65535. Under normal conditions, a user does not have to worry about port numbers for network communication since they remain layers in the addressing protocol. However, for advanced use, some port numbers may have to be managed or specifically opened due to the demands of hardware, software, or firewalls. For example, it may be necessary to open Port 80 in order to play a video game online.

Print Server - A network device that is connected to one or more printers and to client computers over a local network. It can accept print jobs from the computers and send them to the appropriate printer(s).

Proxy Server - A special server that aids in client-client, client-server, and/or server-server communications. A common example is a web server that acts as the portal for a company's traffic to the Internet. Each client has the server IP address listed as the proxy server in their network settings in order to access the Internet or use email.

Remote Access - Accessing data or managing a server or workstation from a separate system or network. The remote access feature on your LaCie product includes the creation of a hostname (essentially, a unique web address name, such as www.lacieNAS.dyndns.org) that will enable easy management and access to data stored on the device from a separate network.

SAMBA - Another name for SMB. See SMB/CIFS

SMB/CIFS (Server Message Block/Common Internet File System) - There are many protocols that a network must implement to assure proper communication between systems, servers, and devices (such as printers). In normal operation, a computer requests a shared file or device managed by a server and the server responds to the demand. SMB/CIFS (also called “Samba”) is a protocol that targets the level in which applications will ask to share a file or device. SMB/CIFS is compatible with Linux, Mac, and Windows, meaning that all three operating systems may reside on the same shared network of servers and devices.

SMTP Server (Simple Mail Transfer Protocol) - A networking and Internet standard for email communication via IP addressing. SMTP is used for outgoing mail, often using port 25.

SOCKS (for Sockets) - A protocol that enables client-client and/or client-server communication via a proxy server. For example, two co-workers want to exchange information but one is blocked due to a firewall. Using the SOCKS Internet protocol, a proxy server will allow them to communicate.

SSID (Server Set Identifier) - The network name of the wireless access point. While an SSID contains no built-in security protocol, it can act as a password when kept hidden from outside traffic.

Static IP (Internet Protocol) - As opposed to DHCP, where the IP address on a computer may change based upon how the server or router manages network identities, a static IP rarely varies.

Static Port Forwarding - Configuring port forwarding to handle traffic through an IP address that does not change. A static address must be configured on a system in order to properly configure static port forwarding.

TCP/IP (Transport Control Protocol/Internet Protocol) - TCP is another layer of communication between the Internet and, within companies or organizations, the Intranet. The TCP breaks down the information that is being sent then puts it back together on the receiving end. The IP layer makes certain that the packets reach the correct address.

Time Machine™ - A backup utility for computers using Mac OS X. Using incremental backups, Time Machine offers a simple interface to back up Apple computers on network or desktop attached storage devices. Users can retrieve single or numerous files that have been periodically saved.

TKIP (Temporal Key Integrity Protocol) - An enhanced version of WEP security, TKIP was created to strengthen hardware that was only compatible with WEP. It adds additional security encryption to the existing WEP.

TLS (Transport Layer Security) - An encryption protocol for Internet communication that is stronger than SSL.

UDP/IP (User or Universal Datagram Protocol/Internet Protocol) - An alternative network protocol to TCP that does not have the ability to reorder or assemble packages of data sent via the Internet. UDP generally sends the message packets and relies upon the user software to put them in order. UDP is good for cutting back on processing with smaller files, since there is little to reassemble at the destination address. IP makes certain that the correct address receives the data.

UPnP™/IGD (Universal Plug and Play/Internet Gateway Device) - UPnP enables devices to share media and data on a network. UPnP devices are “plug-and-play” since they automatically announce their address and supported services once connected to a network. Other systems on the network that recognize those services may immediately begin sharing media with the device. UPnP is very popular with gaming systems such as the Playstation 3 or the Xbox.

WLAN (Wireless Land Area Network) - Similar to a LAN but within the network of a wireless access point.

WEP (Wired Equivalent Privacy) - A security protocol for WLANs. Encrypting data over radio waves, WEP is a security standard that was ported from LAN to WLAN. WEP is not the strongest level of protection for a wireless network since it does not include all layers of network addressing. WEP will protect the data and physical layers of an address.

WEP Key - The security code for a Wi-Fi access point using WEP. It is a series of hexadecimal digits (0-9 and A-F).

WEP Key ID - WEP encryption allows four keys. The user and the wireless access point start with the base WEP Key, then add one of the four WEP Key IDs to extend the characters and strengthen security.

WPA (Wi-Fi Protected Access) - A slightly stronger wireless security protocol than WEP.

WPA2 (Wi-Fi Protected Access 2) - Higher level of wireless security than WPA.

WPA PSK (Wi-Fi Protected Access, Pre-Shared Key) - A “key”, or password, that is shared between a wireless access point and the members of the WLAN. In this case, the PSK uses WPA encryption for security.