PURE IP ARCHITECTURE

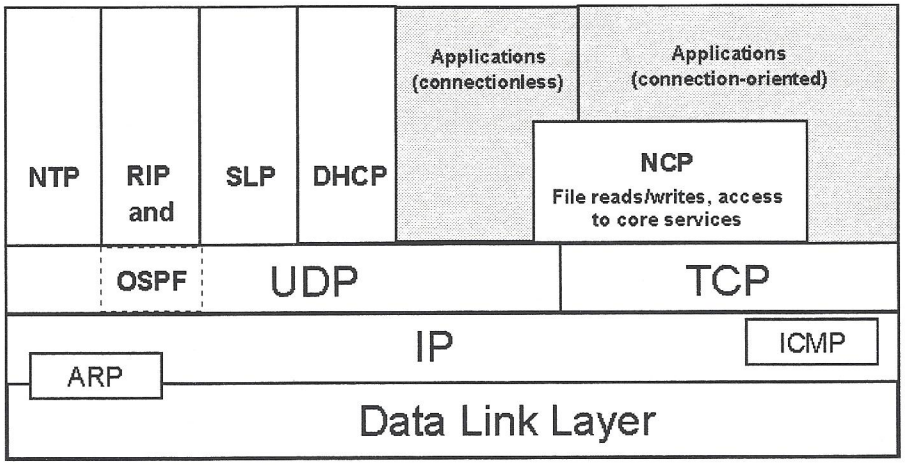
by Laura Chappell
Senior Protocal Analyst, Imagitech, Inc.

I've waited years for Pure IP ... in fact, when I saw that first NCP packet directly over UDP, I nearly cried... ok, ok, I'm a sucker for a new protocol implementation. Now that it's here (or almost here), it's time to start prepping for the communications analysis that must occur to understand this protocol set thoroughly. When you understand the elements and how they relate to each other, you can define troubleshooting and optimization techniques that fit your communication system.

This article is built in three parts (staying with that modular theme, eh?)... Part 1 focuses on the new protocol architecture offered by NetWare® 5. Part 2 examines a typical connection sequence and compares a DHCP client connection sequence with an SLP client connection sequence. Part 3 provides step-by step instructions on how to update your LANalyzer® for Windows* decodes to handle Pure IP communications (and other TCP/IP-related protocols).

Note: As always, you can access our lab trace files on our web site (www.imagitech.com) to see more details on the Pure IP communication system.

Figure 1: Pure IP Architecture



Pure IP Architecture

When you first look at the Pure IP architecture, shown in Figure 1, you'll notice that all your standard TCP/IP stack 'favorites' are there – ARP, ICMP, IP, UDP, TCP, SNMP, etc. There may be some protocols you're not as familiar with, however.

Pure IP Client Connection Sequences: DHCP or SLP?

A Pure IP client has two distinct options when connecting to a Pure IP server. If the client has a locally assigned IP address, it will use SLP to locate the Preferred Tree. If the client is using DHCP to obtain an IP address, the client will also use DHCP to locate the Preferred Tree and Server.

Client has a Locally Assigned IP Address

Figure 2 shows a summary of the boot sequence for a Pure IP client that is bilingual (supports NCP over both IPX and IP). The client attempts to locate a server using the IPX-based SAP method. Since my network does not have any servers that support IPX anymore, the client times out waiting for a response.

- Packet 29—Duplicate IP address test (10.99.99.99)
- Packet 30—Internet Group Management Protocol multicast
- Packets 31-34—SLP requests to find

Figure 2: Client Connection through SLP.

No.	Source	Destination	Layer	Size	Summary
1	002078102EC3	FFFFFFFFFFFF	sap	0064	Query Nearest Directory Server
29	002078102EC3	FFFFFFFFFFFF	arp	0064	Req by 10.99.99.99 for 10.99.99.99
...					
30	002078102EC3	01005E000116	ip	0064	Protocol= IGMP
31	002078102EC3	FFFFFFFFFFFF	slp	0080	Function=SrvReq; XID=16659
32	002078102EC3	01005E000123	slp	0080	Function=SrvReq; XID=16658
33	002078102EC3	01005E000116	slp	0087	Function=SrvReq; XID=16660
34	002078102EC3	01005E000116	slp	0090	Function=SrvReq; XID=16661
35	00104B30C44A	FFFFFFFFFFFF	arp	0064	Req by 10.0.0.1 for 10.99.99.99
36	002078102EC3	00104B30C44A	arp	0064	Reply 10.99.99.99=002078102EC3
37	00104B30C44A	002078102EC3	slp	0096	Function=SrvRply; XID=16661
38	002078102EC3	FFFFFFFFFFFF	dhcp	0594	Req INFORM
39	002078102EC3	01005E000123	slp	0080	Function=SrvReq; XID=16658
40	002078102EC3	01005E000116	slp	0087	Function=SrvReq; XID=16660
41	002078102EC3	01005E000123	slp	0080	Function=SrvReq; XID=16658
42	002078102EC3	01005E000116	slp	0087	Function=SrvReq; XID=16660
43	002078102EC3	FFFFFFFFFFFF	dhcp	0594	Req INFORM
44	002078102EC3	01005E000123	slp	0080	Function=SrvReq; XID=16658
45	002078102EC3	01005E000116	slp	0087	Function=SrvReq; XID=16660
46	002078102EC3	01005E000116	ip	0064	Protocol= IGMP
47	002078102EC3	FFFFFFFFFFFF	dhcp	0594	Req INFORM
48	002078102EC3	01005E000123	slp	0080	Function=SrvReq; XID=16658
49	002078102EC3	01005E000116	slp	0087	Function=SrvReq; XID=16660
50	002078102EC3	00104B30C44A	ncp	0064	Req Create Service Connection
51	00104B30C44A	002078102EC3	ncp	0064	Rply Create Service Connection

Directory Tree I2_TREE

- Packet 35—Server ARP for client's MAC address
- Packet 36—Client sends ARP reply
- Packet 37—SLP reply from server to client
- Packet 38—Client sends DHCP request to get more information (if DHCP supported on server)
- Packets 39-49—Retransmissions of unanswered SLP and DHCP requests
- Packet 50—Client requests NCP General Services Connection (NCP-TCP)

Note: This trace file is called CONN1.TR1 and is available for download off our web site at www. imagitech.com.

Let's take a look at packet 34. This is the SLP request for an NDS™ Tree called I2_TREE (Figure 3). The server's responses with it's own IP address (10.0.0.1) and verification that the tree exists.

Note: You must update your LANalyzer for Windows decodes in order to decode SLP packets. The updated .DLL files and the new LZFW.INI file are available at www.imagitech.com. See the section entitled "LZFW Decode Update for Pure IP" later in this article.

If the server supported DHCP, it would have replied to the client's DHCP request for information. For more details on the client "INFORM" DHCP requests, refer to the next section.

Client is Configured to Obtain an IP Address Using DHCP

If you have configured your clients to obtain an IP address automatically using DHCP, the startup sequence is quite different. In this case, the client transmits a DHCP request for an address and NetWare Tree, Server and Context information. Figure 4 shows what an "INFORM" packet looks like once the new decodes have been added to LANalyzer for Windows.

The three new DHCP Options for NetWare are defined below:

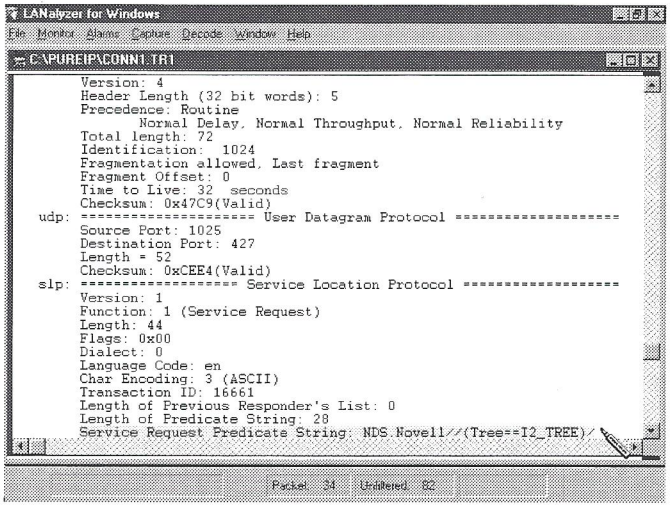


Figure 3: An SLP request includes the Service Request Predicate String identifying the desired service.

DHCP Option 85: NetWare NDS Servers

This option can specify one or more NDS servers for the client to access in order to get to the NDS database. Servers that do not provide access because they support a read-only partition should not be listed in this option reply.

DHCP Option 86: NDS Tree Name

This option provides the name of the NDS tree that the client will contact. This DHCP option reply can contain only one Tree name (up to 255 byte-length name).

DHCP Option 87: NDS Context for Client

This option provides the initial client NDS context. Since DHCP options have a maximum 255 byte length, this option may appear more than once in a packet that defines a very long context name.

Once again, in order to see these packets decode, you must update your LANalyzer for Windows decodes.

Even though IPX/SPX is a very decent, plug-and-play network protocol stack, the flexibility and robustness of Pure IP makes it worth the wait.

LZFW Decode Update for Pure IP

Now you can update LANalyzer for Windows 2.2 to support the following decodes:

- SLP
- DHCP (including the new Novell DHCP options)

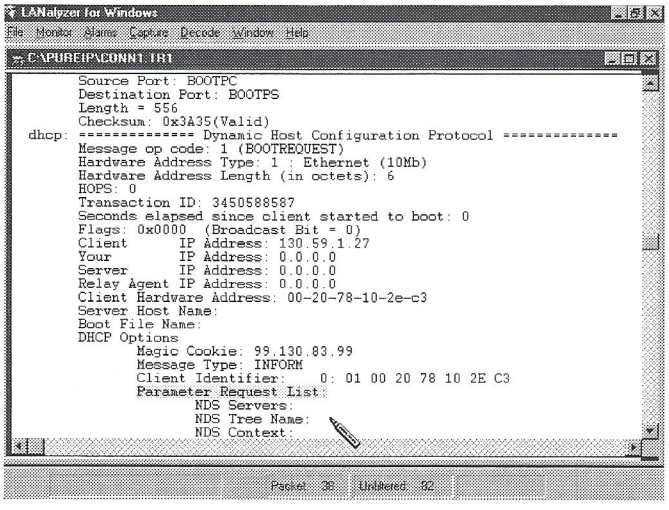


Figure 4: Clients can use DHCP to obtain NetWare Tree, NetWare Server and Context information.