
APPLICATION NOTE

Title: **PXELINUX issues with Avaya IP Phone Environments**

Issue: **1.0**

Date: **June 21, 2002**

Author: **Rick Scheidegger**
Tel nr. (720) 444-4453
rscheidegger@avaya.com
Highlands Ranch, CO USA

Patricia DeCock
Tel nr. (720) 444-4479
pdecock@avaya.com
Highlands Ranch, CO USA

Network Integration Lab

Network Consulting Services

1.0 Overview

PXELINUX allows LINUX machines to take advantage of Intel's PXE (Pre eXecution Environment) functionality. This functionality allows a machine to boot over an ethernet connection from a kernel on a pxe LINUX server. This note explains the issues discovered in an environment that consists of one RedHat 7.3 server running PXELINUX and TFTP services, one RedHat 7.3 server running DHCP services as well as Avaya 46xx IP Phones.

2.0 Environment

RedHat 7.3 server (PXE Server)

kernel 2.4.18-3

pxe-0.1-24.rpm

tftp-server-0.28-2.rpm

RedHat 7.3 server (DHCP Server)

kernel 2.4-18.4

dhcp-2.0p15-8

Avaya 4606 IP Phone

Wildpackets Etherpeek for Windows 4.1 (Software based sniffer)

Avaya Boottest v1.0 utility

- BootTest is designed to validate the boot environment for Avaya IP Phones. BootTest tests whether you have a DHCP and TFTP server set up according to the Avaya LAN Administrator 1.6 document. It is available via the web at this location, <http://support.avaya.com/Boot-Test/>.

3.0 Procedure

Three test scenarios were created for this environment, all of which were requesting DHCP information.

Booting a Windows 2000 Pro PC

Booting an Avaya 4606 IP Phone

Running Avaya BootTest v1.0 utility

Preparation for each of these tests required the three steps below

1 - PXE Server

- PXE daemon is started
- Turned on debugging for pxe daemon and tailed the PxeServiceLog.txt file to monitor activity
- tailed /var/log/messages to monitor system activities
- started tcpdump and redirected output to a file
- created a real-time “while true” looping script to monitor the pxe daemon and provide time stamps so we could see when the pxe daemon died
- Ensured tftp server package was installed and Avaya firmware code available in tftpboot directory.



2 - DHCP Server

- Configured dhcpd.conf file to include SSON(Site Specific Option Number) 176 for support of Avaya IP phones
- Ensured dhcpd daemon was started

3 - Etherpeek

- Started capture of data to/from the PXE server.

Collected Data for typical DHCP offer (Windows 2000 Pro)

Etherpeek packet capture of a DHCP offer for typical DHCP client PC:

```
Flags:          0x00
Status:         0x00
Packet Length: 346
Timestamp:      10:54:43.691731 06/24/2002
```

Ethernet Header

```
Destination:    FF:FF:FF:FF:FF:FF  Ethernet Broadcast
Source:         00:60:08:CB:16:DE
Protocol Type:  0x0800  IP
```

IP Header - Internet Protocol Datagram

```
Version:        4
Header Length:  5 (20 bytes)
Type of Service: %00000000
Precedence:     Routine, Normal Delay, Normal Throughput, Normal Reliability
Total Length:   328
Identifier:     0
Fragmentation Flags: %010 Do Not Fragment Last Fragment
Fragment Offset: 0 (0 bytes)
Time To Live:   64
Protocol:       17  UDP
Header Checksum: 0x7EDB
Source IP Address: 135.122.51.80
Dest. IP Address: 255.255.255.255  IP Broadcast
No IP Options
```

UDP - User Datagram Protocol

```
Source Port:    67  Bootstrap (BOOTP Server)
Destination Port: 68  Bootstrap Protocol Client
Length:         308
Checksum:       0x2E08
```

BootP - Bootstrap Protocol

```
Operation:      2  Boot Reply
Hardware Address Type: 1  Ethernet (10Mb)
Hardware Address Length: 6 bytes
```



```

Hops: 0
Transaction ID: 2973058399
Seconds Since Boot Start: 0
Flags: 0x0000
IP Address Known By Client: 0.0.0.0 IP Address Not Known By Client
Client IP Addr Given By Srvr: 135.122.51.210
Server IP Address: 135.122.51.80
Gateway IP Address: 0.0.0.0
Client Hardware Address: 00:90:27:43:E7:A7
Unused: 0x000000000000000000000000
Server Host Name:
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Boot File Name:
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
DHCP - Dynamic Host Configuration Protocol
DHCP Magic Cookie: 0x63825363
Message TypeDHCP Option
  Option Code: 53 Message Type
  Option Length: 1
  Address: 5.54.4.135
UnknownDHCP Option
  Option Code: 122
  Option Length: 51
  Option Data:
P3...T`.....s 50 33 04 00 00 54 60 01 04 FF FF FF 00 0F 0C 73
d.avaya.com...z3 64 2E 61 76 61 79 61 2E 63 6F 6D 03 04 87 7A 33
...z..... 01 06 04 87 7A 1D 02 FF 00 00 00 00 00 00 00 00
... 00 00 00
Pad DHCP Option
  Pad Option Data:
.... 00 00 00 00

```

As shown, one can see that this is a typical DHCP offer packet with minimal information being broadcast. The packet size, as determined by Etherpeek, is 346 bytes.

- Below is the information logged to the **PxeServiceLog.txt** (pxe debug file).

LoadParsingDlls: 1 Parsing Dlls specified in Registry.



0: PxeParser.

TCP INFO DHCP Socket bound to: Port=67, IP=0-0-0-0
Socket INFO BINL Socket No, 6, bound to: Port=4011, IP=0-0-0-0
Joined Mcast IP: 224-0-1-2
Waiting for another packet from client
Received DHCP Packet with 321 Bytes on port 67
PxeService: Packet #1 was NOT handled by any parsers
Waiting for another packet from client

The pxe server received a DHCP Offer broadcast from the DHCP server and handled the associated packet (#1) and returned to the “Waiting for another packet from client” state.

- Below is the transaction as it was logged by the tcpdump utility

10:54:45.318421 135.122.51.80.bootps > 255.255.255.255.bootpc: xid:0xb135455f
Y:135.122.51.210 S:135.122.51.80 ether 0:90:27:43:e7:a7 [[bootp] (DF)

Collected DHCP offer data for an Avaya 4606 IP Phone

- Etherpeek packet capture of a DHCP offer for typical DHCP client PC:

```
Flags:          0x00
Status:         0x00
Packet Length: 462
Timestamp:     10:56:15.532952 06/24/2002
```

Ethernet Header

```
Destination:   FF:FF:FF:FF:FF:FF  Ethernet Broadcast
Source:        00:60:08:CB:16:DE
Protocol Type: 0x0800  IP
```

IP Header - Internet Protocol Datagram

```
Version:       4
Header Length: 5 (20 bytes)
Type of Service: %00000000
Precedence: Routine, Normal Delay, Normal Throughput, Normal Reliability
Total Length:  444
Identifier:    0
Fragmentation Flags: %010 Do Not Fragment Last Fragment
Fragment Offset: 0 (0 bytes)
Time To Live:  64
Protocol:     17  UDP
Header Checksum: 0x7E67
Source IP Address: 135.122.51.80
```



Dest. IP Address: 255.255.255.255 *IP Broadcast*

No IP Options

UDP - User Datagram Protocol

Source Port: 67 *Bootstrap (BOOTP Server)*
Destination Port: 68 *Bootstrap Protocol Client*
Length: 424
Checksum: 0x7878

BootP - Bootstrap Protocol

Operation: 2 *Boot Reply*
Hardware Address Type: 1 *Ethernet (10Mb)*
Hardware Address Length: 6 bytes
Hops: 0
Transaction ID: 2375417856
Seconds Since Boot Start: 0
Flags: 0x0000
IP Address Known By Client: 0.0.0.0 *IP Address Not Known By Client*
Client IP Addr Given By Srvr: 135.122.51.201
Server IP Address: 135.122.51.80
Gateway IP Address: 0.0.0.0
Client Hardware Address: 00:04:0D:00:56:89
Unused: 0x00000000000000000000
Server Host Name:

..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Boot File Name:

..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

DHCP - Dynamic Host Configuration Protocol

DHCP Magic Cookie: 0x63825363

Message TypeDHCP Option

Option Code: 53 *Message Type*
Option Length: 1
Address: 2.54.4.135

UnknownDHCP Option

Option Code: 122
Option Length: 51
Option Data:

P3...T`..... 50 33 04 00 00 54 60 01 04 FF FF FF 00 03 04 87
 z3....z....sd.av 7A 33 01 06 04 87 7A 1D 02 0F 0C 73 64 2E 61 76
 aya.comB.co9510n 61 79 61 2E 63 6F 6D 42 10 63 6F 39 35 31 30 6E



```

csr                               63 73 72
UnknownDHCP Option
  Option Code:                    101
  Option Length:                  100
  Option Data:
73_2.LMCIPADD=13 37 33 5F 32 B0 6C 4D 43 49 50 41 44 44 3D 31 33
5.122.51.126,135 35 2E 31 32 32 2E 35 31 2E 31 32 36 2C 31 33 35
.122.51.155,135. 2E 31 32 32 2E 35 31 2E 31 35 35 2C 31 33 35 2E
122.51.157,135.1 31 32 32 2E 35 31 2E 31 35 37 2C 31 33 35 2E 31
22.51.130,MCPORT 32 32 2E 35 31 2E 31 33 30 2C 4D 43 50 4F 52 54
=1719,TFTPSVR=1 3D 31 37 31 39 2C 54 46 54 50 53 52 56 52 3D 31
35.1                    33 35 2E 31
Requested IP AddressDHCP Option
  Option Code:                    50  Requested IP Address
  Option Length:                  50
  Value:                          775237934
MessageDHCP Option
  Option Code:                    56  Message
  Option Length:                  49
  Value:                          11348
POP3 ServersDHCP Option
  Option Code:                    70  POP3 Servers
  Option Length:                  84
  Address:                        80.61.255.0

```

As shown, one can see that this DHCP offer includes more information than the typical packet. This packet includes information on the SSON 176, contained under the Unknown DHCP option, and is larger in size, approximately 462 bytes as determined by Etherpeek. This packet did cause the pxe daemon to die.

- Below is the information logged to the **PxeServiceLog.txt** (pxe debug file).

LoadParsingDlls: 1 Parsing Dlls specified in Registry.

0: PxeParser.

TCP INFO DHCP Socket bound to: Port=67, IP=0-0-0-0

Socket INFO BINL Socket No, 6, bound to: Port=4011, IP=0-0-0-0

Joined Mcast IP: 224-0-1-2

Waiting for another packet from client

Received DHCP Packet with 548 Bytes on port 67

What is important to notice here is that the packet was received by the pxe service, but it was not processed. Pxe did not go back to the “Waiting for another packet from client” state. At this point it was verified that the pxe daemon had died.

- Below is the transaction as it was logged by the tcpdump utility



10:56:17.163977 135.122.51.80.bootps > 255.255.255.255.bootpc:
 xid:0x8d960000 Y:135.122.51.201 S:135.122.51.80 ether 0:4:d:0:56:89 [[bootp] (DF)

Collected Avaya BootTest application DHCP offer

Etherpeek packet capture of a DHCP offer for the Avaya BootTest Application:

Flags: 0x00
 Status: 0x00
 Packet Length: 462
 Timestamp: 11:14:18.135849 06/24/2002

Ethernet Header

Destination: FF:FF:FF:FF:FF:FF *Ethernet Broadcast*
 Source: 00:60:08:CB:16:DE
 Protocol Type: 0x0800 *IP*

IP Header - Internet Protocol Datagram

Version: 4
 Header Length: 5 (20 bytes)
 Type of Service: %00000000
Precedence: Routine, Normal Delay, Normal Throughput, Normal Reliability
 Total Length: 444
 Identifier: 0
 Fragmentation Flags: %010 *Do Not Fragment Last Fragment*
 Fragment Offset: 0 (0 bytes)
 Time To Live: 64
 Protocol: 17 *UDP*
 Header Checksum: 0x7E67
 Source IP Address: 135.122.51.80
 Dest. IP Address: 255.255.255.255 *IP Broadcast*

No IP Options

UDP - User Datagram Protocol

Source Port: 67 *Bootstrap (BOOTP Server)*
 Destination Port: 68 *Bootstrap Protocol Client*
 Length: 424
 Checksum: 0xEC0C

BootP - Bootstrap Protocol

Operation: 2 *Boot Reply*
 Hardware Address Type: 1 *Ethernet (10Mb)*
 Hardware Address Length: 6 bytes
 Hops: 0
 Transaction ID: 1131741184
 Seconds Since Boot Start: 4096
 Flags: 0x8000 *Broadcast*
 IP Address Known By Client: 0.0.0.0 *IP Address Not Known By Client*
 Client IP Addr Given By Srvr: 135.122.51.213



```

Server IP Address:          135.122.51.80
Gateway IP Address:       0.0.0.0
Client Hardware Address:  38:2A:00:00:DE:5A
Unused:                   0x000008E62000005260000
Server Host Name:
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Boot File Name:
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

DHCP - Dynamic Host Configuration Protocol

```

DHCP Magic Cookie:          0x63825363
Message TypeDHCP Option
  Option Code:              53 Message Type
  Option Length:           1
  Address:                  2.54.4.135
UnknownDHCP Option
  Option Code:              122
  Option Length:           51
  Option Data:
P3...T`..... 50 33 04 00 00 54 60 01 04 FF FF FF 00 03 04 87
z3....z....sd.av 7A 33 01 06 04 87 7A 1D 02 0F 0C 73 64 2E 61 76
aya.comB.co9510n 61 79 61 2E 63 6F 6D 42 10 63 6F 39 35 31 30 6E
csr                63 73 72
UnknownDHCP Option
  Option Code:              101
  Option Length:           100
  Option Data:
73_2.lMCIPADD=13 37 33 5F 32 B0 6C 4D 43 49 50 41 44 44 3D 31 33
5.122.51.126,135 35 2E 31 32 32 2E 35 31 2E 31 32 36 2C 31 33 35
.122.51.155,135. 2E 31 32 32 2E 35 31 2E 31 35 35 2C 31 33 35 2E
122.51.157,135.1 31 32 32 2E 35 31 2E 31 35 37 2C 31 33 35 2E 31
22.51.130,MCPORT 32 32 2E 35 31 2E 31 33 30 2C 4D 43 50 4F 52 54
=1719,TFTPSRVR=1 3D 31 37 31 39 2C 54 46 54 50 53 52 56 52 3D 31
35.1                33 35 2E 31
Requested IP AddressDHCP Option
  Option Code:              50 Requested IP Address
  Option Length:           50
  Value:                    775237934
MessageDHCP Option
  Option Code:              56 Message

```



```
Option Length: 49
Value: 11348
POP3 ServersDHCP Option
Option Code: 70 POP3 Servers
Option Length: 84
Address: 80.61.255.0
```

As shown, one can see that this DHCP offer includes nearly identical information as the packet captured when the 4606 phone booted. The only differences are related to IP/MAC addresses of the particular client. The size as reported by Etherpeek is also 462 bytes. This packet also caused the pxe daemon to die.

- Below is the information logged to the **PxeServiceLog.txt** (pxe debug file).

LoadParsingDlls: 1 Parsing Dlls specified in Registry.

0: PxeParser.

TCP INFO DHCP Socket bound to: Port=67, IP=0-0-0-0

Socket INFO BINL Socket No, 6, bound to: Port=4011, IP=0-0-0-0

Joined Mcast IP: 224-0-1-2

Waiting for another packet from client

Received DHCP Packet with 548 Bytes on port 67

What is important to notice here is that the packet was also received by the pxe service, but it was not processed. Again pxe did not go back to the “Waiting for another packet from client” state. At this point it was verified that the pxe daemon had died.

- Below is the transaction as it was logged by the tcpdump utility

```
11:14:53.299341 135.122.51.80.bootps > 255.255.255.255.bootpc: xid:0x43750000
Y:135.122.51.213 S:135.122.51.80 ether 38:2a:0:0:de:5a [[bootp] (DF)
```

4.0 Observations

After capturing this information, it is apparent that the DHCP Offer sent from the DHCP server is causing the pxe daemon to die. The differences in the packets may be attributed to the SSON 176 option information. To ensure consistency these tests were also conducted using a Windows 2000 DHCP server as well as multiple versions of Avaya IP Phones , 4630, 4624 and 4612

5.0 Conclusions

The differences causing pxe to die are uncertain, but may be related to the size of the packet, the information in the packet or some other undertermined cause. It is safe to say that the Avaya IP phones are not sending information to the pxe server causing it to die, but the DHCP environment,



in which an Avaya IP Phone operates, appears to be a cause. The obvious course to resolve this issue is for RedHat to determine why these DHCP offer packets are causing their process to die. RedHat would not need an Avaya IP phone configuration to duplicate this, but could use the Avaya BootTest utility to debug their pxe daemon.