

Check Point Software Technologies LTD.

Understanding a DHCP Environment

By: Joe DiPietro

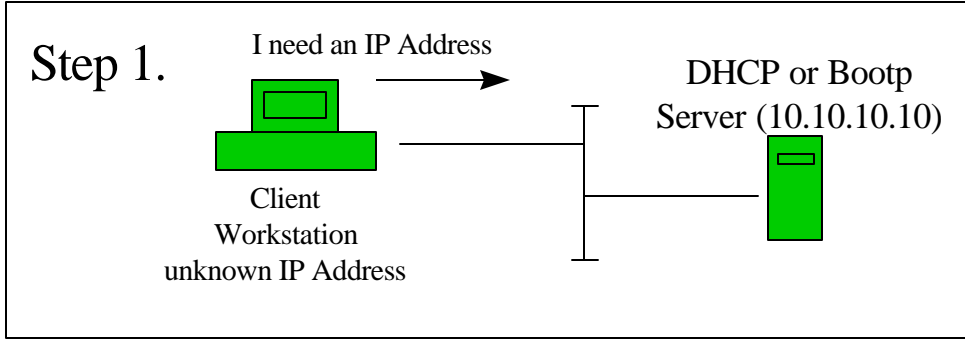
Date: 1/17/97

Subject: DHCP/Bootp Environments

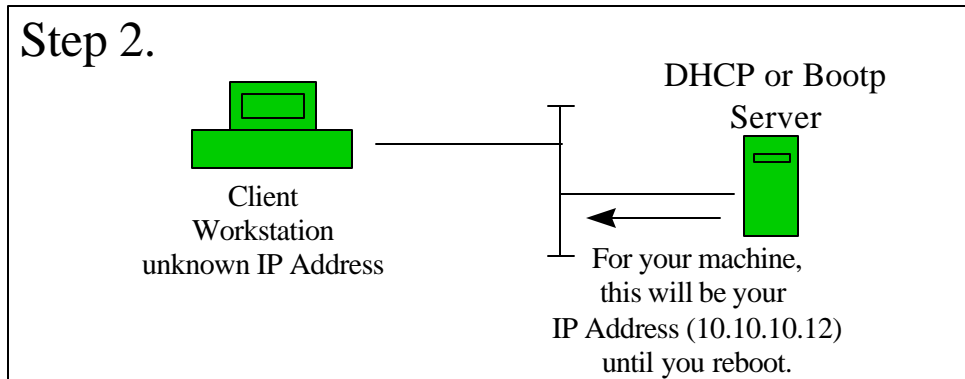
Goal: To describe how Checkpoint's Firewall-1 handles a Dynamically Assigned IP Address Environment.

This document is to give a broad understanding of DHCP and how Checkpoint can seamlessly integrate into this environment.

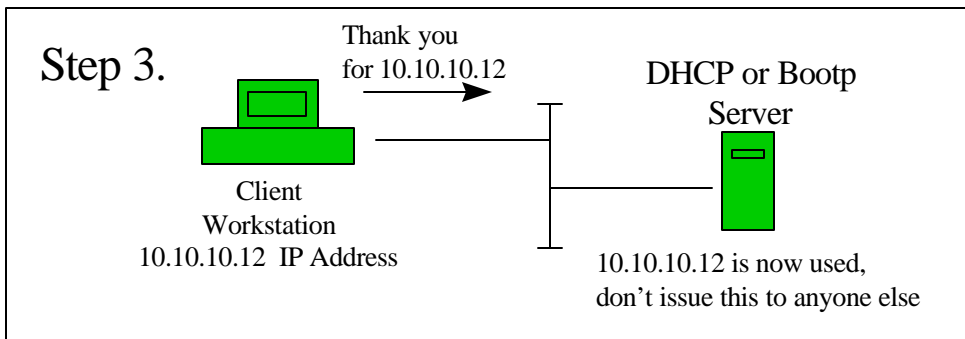
The basic concept of DHCP is to dynamically issue IP Addresses to a Client PC. The diagram looks like the following:



The Client machine asks for an IP Address.

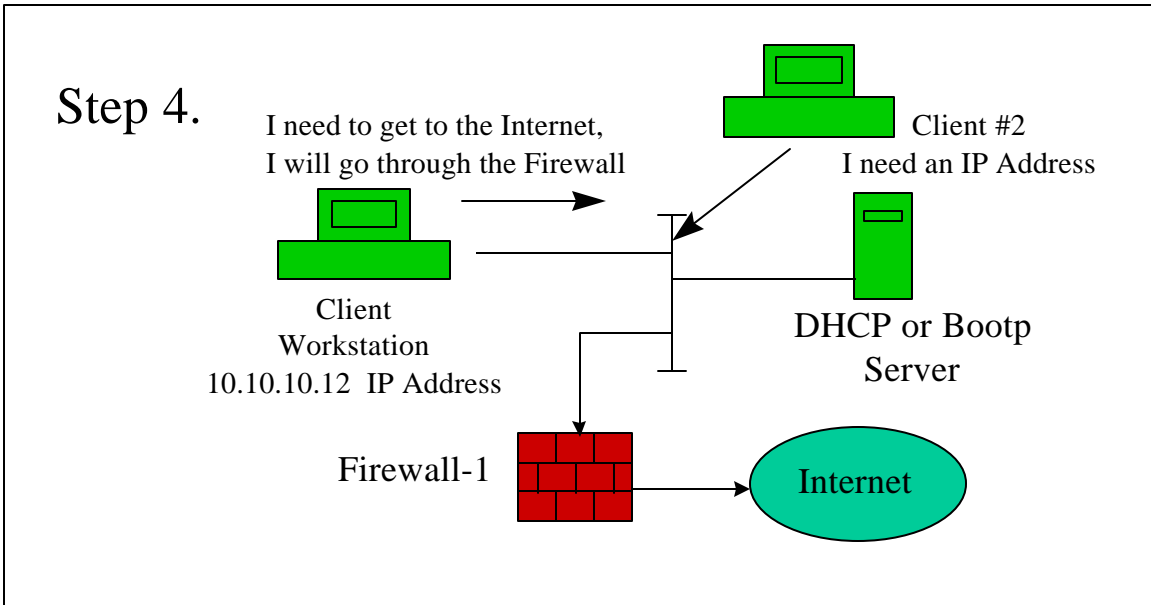


The Bootp or DHCP server will issue the IP Address out of a pool of IP Addresses, or give a specific IP Address to that particular machine. In the case of the Bootp Protocol, the Ethernet Address of the client workstation identifies to the Bootp Server what Specific IP Address is to be given to that machine. Each machine must be given a unique IP Address.



The final step is the Client machine now receives an IP address, so that it can now communicate with other devices on the network.

How does the Firewall handle this situation?



The Firewall does not know who has the address of 10.10.10.12. It could be the first client workstation that was assigned that address, or it could be client #2 who is asking for an IP Address at this point. Therefore, there are two ways to handle this situation depending on what your security needs are. If the goal is to allow all Internal users to get Web access to the Internet without any Authentication, this rule below on the firewall would handle this situation.

1. Define a rule that allows the Internal Network access to the Internet for Web traffic only.

<u>Source</u>	<u>Destination</u>	<u>Service</u>	<u>Action</u>	<u>Track</u>
internal-network	any	http	accept	long

where the above components are defined as follows:

“internal-network” - this component is a group of three subnets
 - net10 which is 10.10.10.0
 - net11 which is 10.10.11.0
 - net12 which is 10.10.12.0

“any” - this component is defined as any address, including all of the IP address in the Internet

“http” - this component is the service that web browsers use to surf the Internet

“accept” - this allows the firewall to accept this communication and pass it out to the Internet

“long” - this will log all the transactions that the client machine communicates to the Internet

The second security goal might be to authenticate the individual users (Joe, Ken, and Scott) that are on the client machine. This would be the case if you would want to give FTP access to the Internet for example. Now we can add another rule like the following:

<u>Source</u>	<u>Destination</u>	<u>Service</u>	<u>Action</u>	<u>Track</u>
internal-network	any	http	accept	long
managers@ internal-network	any	ftp	user-authentication	long

where the above components for rule 2 are defined as follows:

managers - a group of users that contains the following users

- Ken
- Joe
- Scott

“internal-network” - this component is a group of three subnets

- net10 which is 10.10.10.0
- net11 which is 10.10.11.0
- net12 which is 10.10.12.0

“any” - this component is defined as any address, including all of the IP address in the Internet

“ftp” - this component is the service for the file transfer protocol (ftp)

“user-authentication” - this allows the firewall to identify the particular user, independent of what client workstation they are working on.

“long” - this will log all the transactions that the client machine communicates to the Internet

The key to this rule is to use the user-authentication feature. This allows the firewall to make the username to IP address binding for any client workstation, at the time the user wants to communicate to the Internet. This completes the security requirement for the users to be identified, independent of what IP address they happen to be at this particular instance in time.

This is just a sample of how Checkpoint’s Firewall-1 can handle this and many other environments.