5.8.4 Ipconfig Utility Facts

You can use **ipconfig /all** to troubleshoot IP configuration problems. The following table describes how the output for this command changes, based on how IP settings are configured and for specific problem situations:

Condition	ipconfig /all Output
Static IP Configuration	If the workstation is configured with static IP information, the following conditions will exist: - The DHCP Enabled line will show No. - The DHCP Server line will not be shown.
DHCP Configuration	If the workstation has received configuration information from a DHCP server, the following conditions will exist: - The DHCP Enabled line will show Yes. - The DHCP Server line will show the IP address of the DHCP server that sent the configuration information.
Rogue DHCP Server	A *rogue DHCP server* is an unauthorized DHCP server on the network. Symptoms of a rogue DHCP server include: - Conflicting IP addresses on the network - Duplicate IP addresses on the network - Incorrect IP configuration information on some hosts To identify a rogue DHCP server using **ipconfig**, verify the DHCP server address. If this address is not the address of your DHCP server, you have a rogue DHCP server. When you have a rogue DHCP server on the network, some hosts will likely receive configuration information from the correct DHCP server and others from the rogue DHCP server.
Incorrectly Configured DHCP Server	Your DHCP server can send out various IP configuration values, like the IP address and mask. If network hosts are configured with incorrect IP values (such as incorrect default gateway or DNS server addresses), first verify that the workstations are contacting the correct DHCP server. If the correct server is being used, go to the DHCP server to verify that it is sending out correct configuration information.
APIPA Configuration	If the workstation used APIPA to set configuration information, the following conditions will exist: - The DHCP Enabled line will show Yes. - The DHCP Server line will not be shown. - The IP address will be in the range of 169.254.0.1 to 169.254.255.254, with a mask of 255.255.0.0. - The Default Gateway line will be blank. - The DNS Servers line will not include any IPv4 addresses. When APIPA is used, the workstation sets its own IP address and mask. It does not automatically configure default gateway or DNS server values. When APIPA is being used: - Communication is restricted to hosts within the same subnet (there is no default gateway set). - Hosts can communicate with other hosts that have used APIPA. If some hosts are still using an address assigned by the DHCP server (even if the DHCP server is down), those hosts will not be able to communicate with the APIPA hosts. - Name resolution will not be performed (there are no DNS server addresses configured).
Alternate Configuration	If the workstation has been configured using an alternate configuration, the following conditions will exist: - The DHCP Enabled line will show Yes. - The DHCP Server line will not be shown. - The IP address and subnet mask will be values other than the APIPA values. - Default gateway and DNS server addresses will be configured using the alternate configuration values.
Duplicate MAC Addresses	The MAC address is a 12-digit hexadecimal number (48 bits). This address is unique, so you should not have duplicate addresses on your network. However, it is possible for two hosts to have the same MAC address, due to spoofing, a mistake during manufacturing, or if users choose a self-assigned address instead of the vendor-assigned hardware address. This last one is more common when using main frame systems that communicate via MAC addresses rather than protocol addresses (IP addresses). An Ethernet switch keeps a table of which MAC addresses are attached to which ports. It uses the source address of frames it receives during the normal operation of the network to make the table. When the switch receives a frame, the source MAC is read and compared with the current table, and then added alongside whichever switch port it was received on. Therefore, if there are

	two hosts with the same MAC address, then the switch will update it's MAC table every time it receives a frame from either host. Reaching either host will be inconsistent and cause other problems as well.

Exhausted DHCP scope means that all of the addresses within the DHCP scope were depleted. As a consequence, a legitimate user is denied an IP address requested through DHCP and is not able to access the network. This situation is usually caused by an attack called DHCP starvation. This attack might be a DoS mechanism or be used together with a malicious rogue server attack to redirect traffic to a malicious computer ready to intercept traffic.

If the workstation has received configuration information from the wrong DHCP server or has configured itself using APIPA, you may need to contact the DHCP server again once the DHCP problems have been resolved. Use the following commands:

- **ipconfig /release** to stop using the current dynamic IP configuration parameters.
- **ipconfig /renew** to retry the DHCP server request process to obtain IP configuration parameters.

To display the TCP/IP configuration on a Linux computer, use the **ifconfig** command.