



# IBNT Lab Guide

Introduction to Basic Networking Technologies

Labs powered by





*Introduction to Basic  
Networking Technologies  
(IBNT) Lab Guide*



25 Century Blvd., Ste. 500, Nashville, TN 37214 | [Boson.com](http://Boson.com)

To perform the labs referenced in this book, please download the Boson NetSim Network Simulator, navigate to the appropriate lab in the lab menu in the Boson NetSim, and load the lab. To learn more about the Boson NetSim or to purchase and download the software, please visit [www.boson.com/netsim](http://www.boson.com/netsim).

Copyright © 2016 Boson Software, LLC. All rights reserved. Boson, Boson NetSim, Boson Network Simulator, and Boson Software are trademarks or registered trademarks of Boson Software, LLC. Catalyst, Cisco, and Cisco IOS are trademarks or registered trademarks of Cisco Systems, Inc. in the United States and certain other countries. Media elements, including images and clip art, are the property of Microsoft. All other trademarks and/or registered trademarks are the property of their respective owners. Any use of a third-party trademark does not constitute a challenge to said mark. Any use of a product name or company name herein does not imply any sponsorship of, recommendation of, endorsement of, or affiliation with Boson, its licensors, licensees, partners, affiliates, and/or publishers.

<b>Module 3: IP Addressing</b> .....	<b>7</b>
Lab 3.1 – TCP/IP Settings .....	8
Lab Tasks .....	10
Lab Solutions .....	12
Lab 3.2 – Notations .....	22
Lab Tasks .....	22
Lab Solutions .....	26
Lab 3.3 – IPv6 Address Spaces .....	34
Lab Tasks .....	34
Lab Solutions .....	36
<b>Module 4: Routing</b> .....	<b>41</b>
Lab 4.1 – Routing Basics.....	42
Lab Tasks .....	44
Lab Solutions .....	46
Lab 4.2 – Using NetSim .....	58
Lab Tasks .....	59
Lab 4.3 – Configuration Demo I.....	64
Lab Tasks .....	66
Lab Solutions .....	68
Lab 4.4 – Configuration Demo II .....	72
Lab Tasks .....	75
Lab Solutions .....	77
<b>Module 5: Upper-Layer Protocols</b> .....	<b>83</b>
Lab 5.1 – DHCP.....	84
Lab Tasks .....	85
Lab Solutions .....	86
Lab 5.2 – DNS .....	92
Lab Tasks .....	93
Lab Solutions .....	95

Content in these labs is available in the full version of the curriculum. Please visit [www.boson.com](http://www.boson.com) for more information.



# Module 3

---

**Lab 3.1** – TCP/IP Settings

**Lab 3.2** – Notations

**Lab 3.3** – IPv4 Address Spaces

## Lab 3.1 – TCP/IP Settings

### Objective

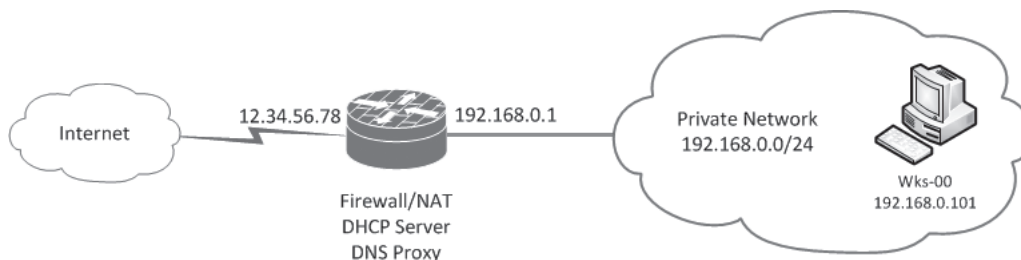
This lab corresponds to Module 3: IP Addressing, of Boson’s Introduction to Basic Networking Technologies (IBNT) tutorial. In this lab, you will review and analyze Transmission Control Protocol/Internet Protocol (TCP/IP) settings on a Windows computer.

### Overview

To be able to communicate on an Internet Protocol (IP) network, a computer must be configured with certain TCP/IP settings. Some of those settings are configured automatically by default or by using Dynamic Host Configuration Protocol (DHCP), and some settings must be configured manually by an administrator by using the graphical user interface (GUI) or command-line tools.

### Lab Topology

The topology diagram below shows the configuration of the network used in this lab:



To complete this lab, you need a computer running a version of Windows supported by Microsoft; this computer is labeled Wks-00 in the topology diagram. The computer must be equipped with at least one network interface card (NIC) and be connected to the Internet. The tasks in this lab are based on the assumption that you have high-speed Internet access through a broadband router that also functions as a firewall, a network address translator (NAT), a DHCP server, and a Domain Name System (DNS) proxy. It is assumed that the router’s NIC connected to your private network is assigned the IP address 192.168.0.1 and that the router’s NIC connected to the Internet is configured automatically by your Internet service provider (ISP).

The IP addresses shown in the topology diagram might differ from the IP addresses on your network. The router’s public address in this diagram, 12.34.56.78, is fictitious. Wks-00 is assumed to be your computer’s name, and 192.168.0.101 is assumed to be your computer’s IP address. The actual name and IP address can be different. If your private network is configured somewhat differently, you should still be able to complete this lab, but the information that you observe on your computer’s screen may not always exactly match the information specified in this lab guide.



The commands you will need to perform the tasks in this lab, along with their syntax and descriptions, are shown in the Command Summary table below. All tasks in this lab involve running commands from a Command Prompt window.

## Command Summary

Command	Description
<b>arp -a</b>	displays the computer's Address Resolution Protocol (ARP) cache
<b>arp -d</b>	clears the ARP cache
<b>arp -d <i>ip-address</i></b>	deletes the ARP cache entry for the host specified by <i>ip-address</i>
<b>arp -s <i>ip-address mac-address</i></b>	adds a static entry for an unused IP address to the ARP cache
<b>ipconfig</b>	displays the computer's basic TCP/IP settings
<b>ipconfig /all</b>	displays the computer's detailed TCP/IP settings
<b>netsh interface ipv4 add neighbors <i>NIC IP MAC</i></b>	adds a static entry for a used IP address to the ARP cache; <i>NIC</i> is the name of the NIC as it appears in the output of the <b>ipconfig</b> command
<b>ping <i>name-or-ip-address</i></b>	verifies connectivity to the host with the specified name or IP address

### Security warning:

Some commands require elevation; that is, a standard user does not have the authority to execute certain commands. By default, all users, including local administrators, on a computer running any version of Windows starting with Windows Vista operate as standard users. Therefore, to successfully run the commands that require elevation, you must run those commands in an elevated Command Prompt window. To open an elevated Command Prompt window, right-click the **Command Prompt** shortcut on the Start menu or Start screen (depending on the version of Windows) and select **Run as administrator**. Depending on the type of user account that you are using, you will be required to respond to the User Account Control prompt by either selecting an administrative user account and entering its password or simply clicking **Yes**.

## Lab Tasks

### Task 1: Display and Review Basic TCP/IP Settings

1. Display your computer's basic TCP/IP settings.
2. How many network interfaces does your computer have? \_\_\_\_\_
3. What is the computer's IP version 4 (IPv4) address? \_\_\_\_\_
4. What is the computer's subnet mask? \_\_\_\_\_
5. How is that mask presented in binary notation? \_\_\_\_\_
6. How is that mask presented in prefix length notation? \_\_\_\_\_
7. What does this mask mean? \_\_\_\_\_
8. What is the IPv4 address of your private network? \_\_\_\_\_
9. What is the computer's IPv4 default gateway address? How does the computer use this address? \_\_\_\_\_  
\_\_\_\_\_
10. What is the computer's link-local IPv6 address on the physical NIC? What can this address be used for? \_\_\_\_\_
11. What other IPv6 addresses does your computer's physical NIC have? \_\_\_\_\_
12. What IPv6 addresses does your computer's Teredo interface have? Explain the purpose of each address. \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

### Task 2: Display and Review Detailed TCP/IP Settings

1. Display your computer's detailed TCP/IP settings.
2. What is the MAC address of your computer's physical NIC? \_\_\_\_\_
3. Is DHCP enabled on your computer's physical NIC? \_\_\_\_\_

4. Is there a DHCP server on your network? If so, what is its IP address and which device is it? \_\_\_\_\_  
\_\_\_\_\_
5. What is the DHCP lease duration on your computer's physical NIC? \_\_\_\_\_
6. Is there a DNS server on your home network? If so, what is its IP address and which device is it? \_\_\_\_\_  
\_\_\_\_\_

### **Task 3: Display and Review the ARP Cache**

For computers to be able to communicate with one another, they must know one another's IP addresses. Computers that are located on the same network segment must also know one another's MAC addresses. ARP is a protocol that enables computers to automatically infer one another's MAC addresses from IP addresses. When a computer learns another computer's MAC address, it temporarily stores the IP address-to-MAC address mapping in a special area of memory known as the ARP cache.

1. Display your computer's ARP cache.
2. Clear your computer's ARP cache.
3. Populate your computer's ARP cache with dynamic entries.
4. Add a static entry to your computer's ARP cache.
5. Remove the static entry from your computer's ARP cache.

## Lab Solutions

### Task 1: Display and Review Basic TCP/IP Settings

1. To display your computer's basic TCP/IP settings, you should open a Command Prompt window and issue the **ipconfig** command. Sample output is shown below:

```
C:\Users\User1>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : hitronhub.home
    IPv6 Address. . . . . : fd00:bc4d:fb91:1ea2:2cf7:5235:998a:975d
    Temporary IPv6 Address. . . . . : fd00:bc4d:fb91:1ea2:a00d:2465:b32c:75b0
    Link-local IPv6 Address . . . . . : fe80::2cf7:5235:998a:975d%3
    IPv4 Address. . . . . : 192.168.0.101
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Tunnel adapter isatap.hitronhub.home:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : hitronhub.home

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2001:0:5ef5:79fb:38ac:38bc:9c12:5078
    Link-local IPv6 Address . . . . . : fe80::38ac:38bc:9c12:5078%5
    Default Gateway . . . . . :
```

2. The command returns the computer's basic TCP/IP settings for each NIC. The sample output shown above indicates that the computer has one physical NIC and two virtual NICs for IPv6 transition technologies.

The sample output also indicates that the physical NIC is named Ethernet. Its settings include an IPv4 address, a subnet mask, a default gateway address, three IPv6 addresses, and a connection-specific DNS suffix.

One virtual NIC is for the Intra-site Automatic Tunnel Addressing Protocol (ISATAP) transition technology. It is named `isatap.hitronhub.home`. It does not have any settings and is in the **Media disconnected** state because this private network is not configured to support ISATAP.

The other virtual NIC is for the Teredo technology. It is named Teredo Tunneling Pseudo-Interface. Its settings include two IPv6 addresses, a default gateway address, and a connection-specific DNS suffix. The two latter settings do not have any values, because they are not configured by default.

3. The sample output indicates that the computer's IPv4 address is 192.168.0.101.
4. The sample output indicates that the computer's subnet mask is 255.255.255.0.

5. In binary notation, this mask is presented as follows:

255.255.255.0 = 11111111 11111111 11111111 00000000

6. In prefix-length notation, the mask is presented as /24.
7. This mask means that the first (that is, the leftmost) 24 bits, or three octets, in the computer's IP address, 192.168.0, represent a network ID or subnet ID and that the fourth octet, 101, represents a host ID.
8. Based on your computer's IPv4 address and subnet mask, the IPv4 address of this private network is 192.168.0.0/24. The host ID portion in a network address must consist of all 0s in binary notation.
9. The default gateway address in the sample output is 192.168.0.1. This is the address of the router on the private network. The computer will direct all Internet-bound traffic to this address, and the router will forward the traffic to the Internet.
10. All versions of Windows starting with Windows Vista support both IPv4 and IPv6. At startup, your computer automatically generated a link-local IPv6 address for its physical NIC. In the sample output, the physical NIC is assigned the following link-local IPv6 address:

FE80::2CF7:5235:998A:975D%3

This address can be used to communicate with other IPv6 or dual-stack devices on the local network segment, or link. In particular, once a computer has assigned itself a link-local address, it can discover whether there are any routers on the local link and use them to configure additional, routable IPv6 addresses for itself.

The percent sign followed by a decimal number appended to this address indicate a zone index. UNIX and Linux operating systems (OSs) use alphanumeric names of the network connections instead of numeric indexes. Each NIC on an IPv6 or dual-stack computer is always automatically assigned a link-local IPv6 address. In addition, certain virtual NICs for transition technologies are automatically created on dual-stack computers and are also assigned link-local IPv6 addresses. Thus most computers have multiple NICs (physical or virtual) that are assigned link-local IPv6 addresses. When an application needs to send something to a destination defined by a link-local IPv6 address, the usual routing based on routing prefixes does not work, because all link-local IPv6 addresses have the same prefix, FE80::/64. In such situations, the zone indexes are used for disambiguation to specify the NIC through which an outgoing communication must be transmitted.

11. In the sample output, the two other IPv6 addresses on the physical NIC both start with the FD00::/8 prefix, which means that they are unique local addresses. They are similar to IPv4 private addresses; they can be used only on private networks. The following is the first IPv6 address in the sample output:

```
FD00:BC4D:FB91:1EA2:2CF7:5235:998A:975D
```

The first 64 bits, or four blocks of four hexadecimal digits each, constitute a network ID:

```
FD00:BC4D:FB91:1EA2
```

The computer must have learned this prefix from the router. The last 64 bits constitute an interface ID. Note that the interface ID in this unique local address is the same as the interface ID in the link-local address:

```
2CF7:5235:998A:975D
```

The following is the second unique local IPv6 address in the sample output:

```
FD00:BC4D:FB91:1EA2:A00D:2465:B32C:75B0
```

This is a temporary address. Note that it has the same network ID as the first unique local address but a different interface ID. In certain situations, a computer can generate random interface IDs and form temporary routable addresses. The temporary addresses have limited lifespans and are periodically changed in order to protect your privacy. The use of temporary addresses somewhat obfuscates the exact origin of the IPv6 network traffic produced by your computer. As a result, it is more difficult for other hosts on the network to track your activities on the network.

12. The Teredo virtual NIC in the sample output is configured with the following two IPv6 addresses:

```
2001:0:5EF5:79FB:38AC:38BC:9C12:5078  
FE80::38AC:38BC:9C12:5078%5
```

A Teredo virtual NIC is automatically created on a computer that is connected to the Internet through a NAT. The first IPv6 address on this NIC is global, and the second address is link-local. Note that the interface ID is the same in both addresses. The link-local address is automatically configured first and is used to discover a Teredo server on the Internet. It can also be used to communicate with other Teredo clients on the local link. Some organizations maintain public Teredo servers on the Internet. The global address is automatically configured after the client receives a response from a Teredo server. This address can be used to communicate with IPv6 and dual-stack hosts on the IPv6 Internet and with dual-stack hosts on the IPv4 Internet.

## Task 2: Display and Review Detailed TCP/IP Settings

1. To display your computer's detailed TCP/IP settings, you should open a Command Prompt window and issue the **ipconfig /all** command. Sample output is shown below:

```
C:\Users\User1>ipconfig /all

Windows IP Configuration

Host Name . . . . . : wks-00
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : hitronhub.home

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : hitronhub.home
Description . . . . . : Microsoft Hyper-V Network Adapter
Physical Address. . . . . : 00-15-5D-00-03-06
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : fd00:bc4d:fb91:1ea2:2cf7:5235:998a:975d(Preferred)
Temporary IPv6 Address. . . . . : fd00:bc4d:fb91:1ea2:a00d:2465:b32c:75b0(Preferred)
Link-local IPv6 Address . . . . . : fe80::2cf7:5235:998a:975d%3(Preferred)
IPv4 Address. . . . . : 192.168.0.101(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, January 19, 2016 15:37:32
Lease Expires . . . . . : Tuesday, January 26, 2016 15:37:33
Default Gateway . . . . . : 192.168.0.1
DHCP Server . . . . . : 192.168.0.1
DHCPv6 IAID . . . . . : 50337117
DHCPv6 Client DUID. . . . . : 00-01-00-01-1D-6F-A4-A6-00-15-5D-00-03-06
DNS Servers . . . . . : 192.168.0.1
NetBIOS over Tcpi. . . . . : Enabled

Tunnel adapter isatap.hitronhub.home:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : hitronhub.home
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

Tunnel adapter Teredo Tunneling Pseudo-Interface:

Connection-specific DNS Suffix . :
Description . . . . . : Teredo Tunneling Pseudo-Interface
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:0:5ef5:79fb:38ac:38bc:9c12:5078(Preferred)
Link-local IPv6 Address . . . . . : fe80::38ac:38bc:9c12:5078%5(Preferred)
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 134217728
DHCPv6 Client DUID. . . . . : 00-01-00-01-1D-6F-A4-A6-00-15-5D-00-03-06
NetBIOS over Tcpi. . . . . : Disabled
```

Detailed TCP/IP settings include the basic settings and additional information, such as MAC addresses, DNS server addresses, and whether DHCP is enabled. If DHCP is enabled, the settings can also include the address of the DHCP server and the DHCP lease interval.

2. The MAC address of the computer's physical NIC in the sample output shown above is 00-15-5D-00-03-06. A MAC address is often also referred to as a physical address.



3. Yes. DHCP is enabled on the physical NIC in the sample output.
4. Yes. The sample output indicates that there is a DHCP server on the network. Its IP address is 192.168.0.1. This is the private address of the broadband router that connects your private network to the Internet. The router includes a built-in DHCP server.
5. The DHCP lease duration in the sample output is one week. You can determine that by comparing the **Lease Obtained** and **Lease Expires** dates in the output.
6. As stated in the Lab Topology section, the environment for this lab does not include a full-fledged DNS server. However, the sample output indicates that there is an entity that functions as a DNS server and that its IP address is 192.168.0.1. This is the private address of the broadband router, which also acts as a DNS proxy.

### Task 3: Display and Review the ARP Cache

1. To display your computer's ARP cache, you should open a Command Prompt window and issue the **arp -a** command. Sample output is shown below:

```
C:\Users\User1>arp -a

Interface: 192.168.0.101 --- 0x3
 Internet Address      Physical Address      Type
 192.168.0.1          bc-4d-fb-91-1e-a2    dynamic
 192.168.0.255        ff-ff-ff-ff-ff-ff    static
 224.0.0.22           01-00-5e-00-00-16    static
 224.0.0.251          01-00-5e-00-00-fb    static
 224.0.0.252          01-00-5e-00-00-fc    static
 239.255.255.250      01-00-5e-7f-ff-fa    static
```

The exhibit contains one dynamic mapping for the IP address 192.168.0.1 and five static mappings for special IPv4 addresses. 192.168.0.255 is the local broadcast address, and the four other addresses are reserved multicast addresses that are used for various special purposes, such as automatic communications with multicast-enabled routers, discovery of other devices on the local network segment, and name resolution on the local network segment. Dynamic mappings are transient, whereas static mappings are permanent. Being transient refers to two factors: the duration of time that a mapping remains in the cache and the fact that the MAC address in a mapping can change if the IP address is reassigned to another device. Being permanent does not necessarily mean that a mapping stays in the cache forever; rather, it means that the IP address will always be mapped to the same MAC address. Generally, static mappings can be added to the cache manually. However, the static mappings in the sample output from the **arp -a** command are created automatically; they map special, reserved IPv4 addresses to special, reserved MAC addresses.



- To clear your computer's ARP cache, you should issue the **arp -d** command.

**Security warning:** This command must be run in an elevated Command Prompt window.

Sample output is shown below:

```
C:\windows\system32>arp -a
Interface: 192.168.0.101 --- 0x3
  Internet Address      Physical Address      Type
  224.0.0.22           01-00-5e-00-00-16    static
```

The sample output shown above indicates that all the previously cached mappings except one have been removed.

- To populate your computer's ARP cache with dynamic entries, you can use the Ping command-line tool. A computer's ARP cache is automatically populated with dynamic entries when the computer attempts to communicate with other hosts on the local network segment. Some communications occur automatically and thus cause the corresponding dynamic ARP entries to be added automatically. For example, you can wait for a few minutes and then run the **arp -a** command again to confirm that the same dynamic entry for address 192.168.0.1 that was cached earlier has been added automatically again along with the same static entries that appear in the output in step 1.

Other entries will be automatically added when you initiate communications with other hosts. Assuming that, in addition to your current computer and the broadband router, your private network also contains another device and that device's IP address is 192.168.108, you can issue the **ping 192.168.0.108** command and then issue the **arp -a** command.

*(continued on next page)*

(continued from previous page)

The **ping 192.168.0.108** command will cause your computer to initiate communications with a host whose IP address is 192.168.0.108. The **arp -a** command will display the ARP cache, which will include a mapping of the IP address 192.168.0.108 to the host's MAC address. The following exhibit illustrates how the contents of the ARP cache change as a result of running the **ping 192.168.0.108** command:

```
C:\Users\User1>arp -a

Interface: 192.168.0.101 --- 0x3
Internet Address      Physical Address      Type
192.168.0.1          bc-4d-fb-91-1e-a2    dynamic
192.168.0.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250      01-00-5e-7f-ff-fa    static

C:\Users\User1>ping 192.168.0.108

Pinging 192.168.0.108 with 32 bytes of data:
Reply from 192.168.0.108: bytes=32 time=1ms TTL=128
Reply from 192.168.0.108: bytes=32 time<1ms TTL=128
Reply from 192.168.0.108: bytes=32 time<1ms TTL=128
Reply from 192.168.0.108: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.108:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\User1>arp -a

Interface: 192.168.0.101 --- 0x3
Internet Address      Physical Address      Type
192.168.0.1          bc-4d-fb-91-1e-a2    dynamic
192.168.0.108        00-15-5d-00-03-09    dynamic
192.168.0.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250      01-00-5e-7f-ff-fa    static
```

- You should issue the **arp -s ip-address mac-address** command to add static entries to the ARP cache. They persist until the computer is restarted or the NIC is reinitialized. For an IP address that is currently not being used on the local network segment, you can add a static mapping by using a command similar to **arp -s 192.168.0.101 01-02-03-04-05-06**.

**Security warning:** This command must be run in an elevated Command Prompt window.

Sample output is shown below:

```
C:\windows\system32>arp -s 192.168.0.101 01-02-03-04-05-06
C:\windows\system32>arp -a
Interface: 192.168.0.101 --- 0x3
  Internet Address      Physical Address      Type
  192.168.0.1           bc-4d-fb-91-1e-a2    dynamic
  192.168.0.101        01-02-03-04-05-06    static
  192.168.0.108        00-15-5d-00-03-09    dynamic
  192.168.0.255        ff-ff-ff-ff-ff-ff    static
  224.0.0.22           01-00-5e-00-00-16    static
  224.0.0.251         01-00-5e-00-00-fb    static
  224.0.0.252         01-00-5e-00-00-fc    static
  239.255.255.250     01-00-5e-7f-ff-fa    static
```

The Arp command-line tool cannot modify an existing dynamic mapping or add a static mapping for an IP address that is in use on the network. To add a static mapping for an IP address of an existing device, you can use a Netsh command similar to **netsh interface ipv4 add neighbors Ethernet 192.168.0.108 11-22-33-44-55-66**.

**Warning:** This command must be run in an elevated Command Prompt window.

*(continued on next page)*

(continued from previous page)

Sample output is shown below:

```
C:\Windows\system32>arp -s 192.168.0.108 11-22-33-44-55-66
The ARP entry addition failed: Access is denied.

C:\Windows\system32>arp -d 192.168.0.108

C:\Windows\system32>arp -a

Interface: 192.168.0.101 --- 0x3
Internet Address      Physical Address      Type
192.168.0.1           bc-4d-fb-91-1e-a2    dynamic
192.168.0.101        01-02-03-04-05-06    static
192.168.0.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251         01-00-5e-00-00-fb    static
224.0.0.252         01-00-5e-00-00-fc    static
239.255.255.250     01-00-5e-7f-ff-fa    static

C:\Windows\system32>arp -s 192.168.0.108 11-22-33-44-55-66
The ARP entry addition failed: Access is denied.

C:\Windows\system32>netsh interface ipv4 add neighbors Ethernet 192.168.0.108 11-22-33-44-55-66

C:\Windows\system32>arp -a

Interface: 192.168.0.101 --- 0x3
Internet Address      Physical Address      Type
192.168.0.1           bc-4d-fb-91-1e-a2    dynamic
192.168.0.101        01-02-03-04-05-06    static
192.168.0.108        11-22-33-44-55-66    static
192.168.0.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251         01-00-5e-00-00-fb    static
224.0.0.252         01-00-5e-00-00-fc    static
239.255.255.250     01-00-5e-7f-ff-fa    static
```

In this command, **Ethernet** is the name of the network connection for which you are adding a static entry. If the connection's name contains spaces—for example, in some versions of Windows, the default name for a network connection is Local Area Connection—it should be enclosed in double quotation marks.

5. Although, technically, the static entry that you have added in the previous step is valid, it is, in fact, incorrect because it maps the IP address of an existing device to a fictitious MAC address. Therefore, you should remove that entry by running the **arp -d 192.168.0.108** command.

**Security warning:** This command must be run in an elevated Command Prompt window.

Sample output is shown below:

```
C:\windows\system32>arp -d 192.168.0.108
C:\windows\system32>arp -a
Interface: 192.168.0.101 --- 0x3
  Internet Address      Physical Address      Type
  192.168.0.1           bc-4d-fb-91-1e-a2    dynamic
  192.168.0.101         01-02-03-04-05-06    static
  192.168.0.255         ff-ff-ff-ff-ff-ff    static
  224.0.0.22            01-00-5e-00-00-16    static
  224.0.0.251           01-00-5e-00-00-fb    static
  224.0.0.252           01-00-5e-00-00-fc    static
  239.255.255.250       01-00-5e-7f-ff-fa    static
```

## **Certification Candidates**

Boson Software's ExSim-Max practice exams are designed to simulate the complete exam experience. These practice exams have been written by in-house authors who have over 30 years combined experience writing practice exams. ExSim-Max is designed to simulate the live exam, including topics covered, question types, question difficulty, and time allowed, so you know what to expect. To learn more about ExSim-Max practice exams, please visit [www.boson.com/exsim-max-practice-exams](http://www.boson.com/exsim-max-practice-exams) or contact Boson Software.

## **Organizational and Volume Customers**

Boson Software's outstanding IT training tools serve the skill development needs of organizations such as colleges, technical training educators, corporations, and governmental agencies. If your organization would like to inquire about volume opportunities and discounts, please contact Boson Software at [orgsales@boson.com](mailto:orgsales@boson.com).

## **Contact Information**

E-Mail: support@boson.com  
Phone: 877-333-EXAM (3926)  
615-889-0121  
Fax: 615-889-0122  
Address: 25 Century Blvd., Ste. 500  
Nashville, TN 37214





B o s o n . c o m

8 7 7 . 3 3 3 . 3 9 2 6      s u p p o r t @ b o s o n . c o m

© Copyright 2016 Boson Software, LLC. All rights reserved.