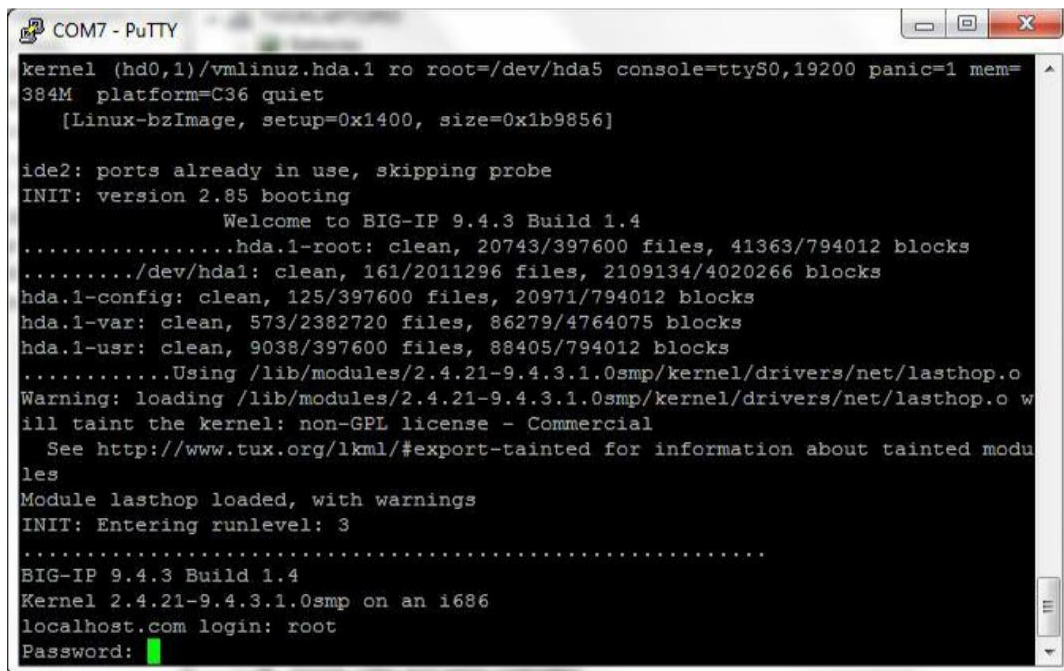


Big IP F5 v9.4.3 Devices

Using SSH, Telnet or direct console connection

For this procedure you will be using the Command Line Interface (CLI) of your Big IP F5 device using an SSH client (such as OpenSSH or Putty), Telnet or through the console port. We would recommend using either SSH (for remote connections) or using a direct connection to the console port. Telnet provides no encryption of the communications and therefore your authentication credentials and configuration would be vulnerable if a malicious user were to monitor your connection.

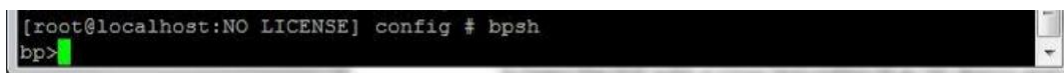
1. Connect to the Big IP F5 using your favorite SSH client, Telnet or a direct console connection.
2. Certain Big IP devices will be capable of dual booting so make sure that you have selected the correct version for the following instructions.



```
COM7 - PuTTY
kernel (hd0,1)/vmlinuz.hda.1 ro root=/dev/hda5 console=ttyS0,19200 panic=1 mem=
384M platform=C36 quiet
[Linux-bzImage, setup=0x1400, size=0x1b9856]

ide2: ports already in use, skipping probe
INIT: version 2.85 booting
      Welcome to BIG-IP 9.4.3 Build 1.4
.....hda.1-root: clean, 20743/397600 files, 41363/794012 blocks
...../dev/hda1: clean, 161/2011296 files, 2109134/4020266 blocks
hda.1-config: clean, 125/397600 files, 20971/794012 blocks
hda.1-var: clean, 573/2382720 files, 86279/4764075 blocks
hda.1-usr: clean, 9038/397600 files, 88405/794012 blocks
.....Using /lib/modules/2.4.21-9.4.3.1.0smp/kernel/drivers/net/lasthop.o
Warning: loading /lib/modules/2.4.21-9.4.3.1.0smp/kernel/drivers/net/lasthop.o w
ill taint the kernel: non-GPL license - Commercial
See http://www.tux.org/lkml/#export-tainted for information about tainted modu
les
Module lasthop loaded, with warnings
INIT: Entering runlevel: 3
.....
BIG-IP 9.4.3 Build 1.4
Kernel 2.4.21-9.4.3.1.0smp on an i686
localhost.com login: root
Password: █
```

3. Logon using your administration authentication credentials.
4. Execute the following CLI command to access the bigpipe shell: `bpsh`



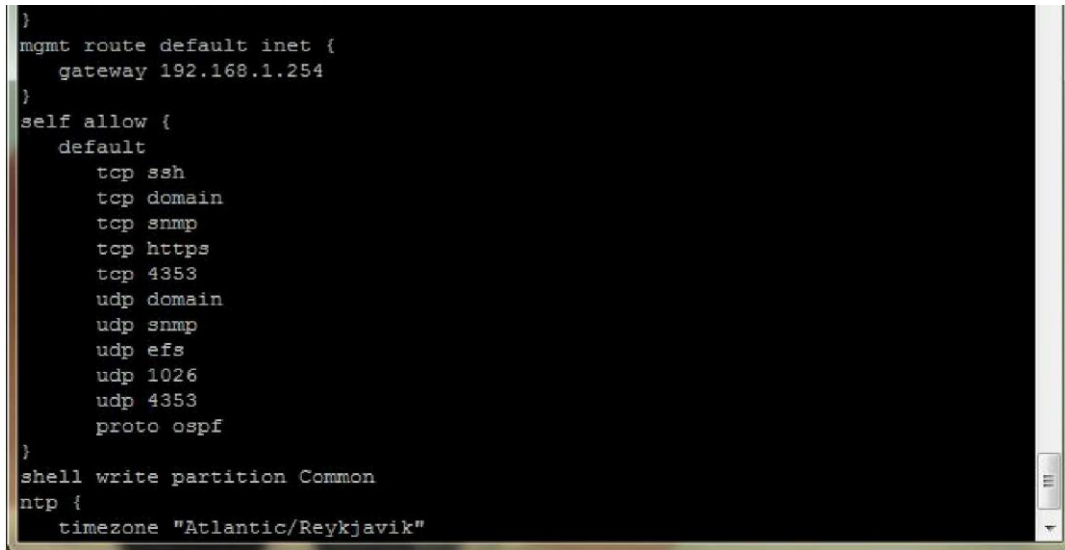
```
[root@localhost:NO LICENSE] config # bpsh
bp> █
```

5. The command prompt will change to: `bp>`
6. From the bigpipe shell run the command `export`



```
COM9 - PuTTY
bp>export
mgmt 192.168.1.245 {
  netmask 255.255.255.0
```

7. Capture the output (using cut and paste, for example).
8. Save the captured output to a text file on your local machine.

A screenshot of a terminal window with a black background and white text. The text is a network configuration snippet in a structured text format. The configuration includes a management route, a self-allow rule with various protocols and ports, a shell write partition, and an ntp section with a timezone setting.

```
}
mgmt route default inet {
    gateway 192.168.1.254
}
self allow {
    default
        tcp ssh
        tcp domain
        tcp snmp
        tcp https
        tcp 4353
        udp domain
        udp snmp
        udp efs
        udp 1026
        udp 4353
        proto ospf
}
shell write partition Common
ntp {
    timezone "Atlantic/Reykjavik"
```

9. This text file will be readable by Nipper Studio.