

# Bootloader and Startup

## Feature Overview and Configuration Guide

### The AlliedWare Plus™ Bootloader

Every switch has a startup process. The end result of the startup is that the unit is running a specific version of the operating system software, with the features configured according to a specific startup configuration file.

The startup process goes through two main phases:

- First, the switch boots up off a dedicated bootloader software image, which initializes core functionality of the unit.
- Then, the bootloader launches the main operating software image, and passes control over to this operating system.

The bootloader is the executable code responsible for setting up the system and loading the operating system software.

The bootloader is the software that runs the unit when it first powers up, performing basic initialization and executing the product software release. As part of the startup process of the switch, the bootloader allows you various options before running the product operating system software.

## Products and software version that apply to this guide

This guide applies to all AlliedWare Plus products, running version **5.4.4** or later.

However, not all features in this guide are supported on all products. To see whether a product supports a particular feature or command, see the following documents:

- The [product's Datasheet](#)
- The [AlliedWare Plus Datasheet](#)
- The product's [Command Reference](#)

These documents are available from the above links on our website at [alliedtelesis.com](http://alliedtelesis.com).

Feature support may change in later **versions**. For the latest information, see the above documents.

## Content

The AlliedWare Plus™ Bootloader .....	1
Products and software version that apply to this guide .....	2
The Startup Process.....	3
Diagnostic Menu .....	3
Bootloader Menu.....	5
Security Level .....	5
Boot options .....	8
Startup Sequence .....	13

# The Startup Process

As AlliedWare Plus begins its startup process; there are two options that allow you to access either the diagnostic menu, or the bootloader menu. The following prompt is displayed when these options are temporarily available:

```
Bootloader 3.0.0-devel loaded  
Press <Ctrl+B> for the Boot Menu
```

You can now enter one of the following two options to determine how the startup process proceeds:

- Enter **Ctrl+D** to display the diagnostic menu.
- Enter **Ctrl+B** to display the bootloader menu.

## Diagnostic Menu

Enter **Ctrl+D** during startup to access the bootloader diagnostic menu, and provide options for performing various hardware tests. This can be useful as a tool for confirming a suspected hardware problem at the direction of network engineering personnel. When you enter **Ctrl+D**, the stage 1 diagnostics menu is displayed:

**Output 1: Stage 1 diagnostics menu**

```
Press <Ctrl+B> for the Boot Menu

Bootup Stage 1 Diagnostics Menu:

0. Restart
1. Full RAM test
2. Quick RAM test
4. Bootloader ROM checksum test
-----
7. Bootup stage 2 diagnostics menu
-----
8. Quit to U-Boot shell
9. Quit and continue booting
Enter selection ==>
```

The options in the stage 1 diagnostics menu allow you to initiate the following bootloader tests:

- **RAM:** any/all SDRAM installed in the system.
- **NVS:** any/all non-volatile (battery backed) SRAM installed in the system.
- **Checksum:** the bootloader checksum ROM memory for error detection.

For example, enter “2” to select a Quick RAM test:

```
Quick RAM test - press Q to quit, S to skip when failing
Writing pattern ..... .
Checking pattern ..... .
Writing complemented pattern ..... .
Checking complemented pattern ..... .
Pass 1 total errors 0
```

Enter “7” to display the stage 2 diagnostics menu:

```
Entering stage 2...
Epi3: Station address is: 00:0c:25:03:90:c1
Net: BCM_ethernet

Bootup Stage 2 Diagnostics Menu:

0. Restart
2. Test FLASH (Filesystem only)
4. Erase FLASH (Filesystem only)
-----
8. Quit to U-Boot shell
9. Quit and continue booting

Enter selection ==>
```

The options in the stage 2 diagnostics menu allow you to initiate the following tests:

- **Flash:** the user file system area of Flash. The bootloader is stored in a protected area of Flash that is not accessed by the user file system.
- **Flash Erase:** the bootloader erases the user file system area of Flash only.
- **SD (and SDHC) Card slot:** the Card slot.

Once any required tests are completed from the diagnostics menu, enter “9” to quit the diagnostic menu and continue the switch boot-up process.

## Bootloader Menu

Enter **Ctrl+B** during startup to access the bootloader menu where boot options can be set. The boot options shown are explained in detail under this example.

```
Boot Menu:

WARNING: The bootloader is not currently password protected.
-----
B. Boot backup software
-----
S. Security Level
-----
0. Restart
1. Perform one-off boot from alternate source
2. Change the default boot source (for advanced users)
3. Update Bootloader
4. Adjust the console baud rate
5. Special boot options
6. System information
7. Restore Bootloader factory settings
-----
9. Quit and continue booting

Enter selection ==>
```

## Security Level

The Security Level option enables you to configure how accessible the bootloader is to users. There are three levels of security.

The first level is the default level. By default, there is no protection on the bootloader menu. Anyone who has physical access to the switch can connect a terminal to the console port, reboot the switch, and type **Ctrl+B** at startup to access the bootloader menu.

The next level of security enables a password for access to the menu. If the user types **Ctrl+B** at bootup, they will need to enter the password before being able to access the following menu items in the bootloader menu:

- Perform one-off boot from alternate source
- Change the default boot source (for advanced users)
- Update bootloader
- Special boot options (which accesses the **skip startup script** option)
- Developer menu
- Configure protected mode

Therefore, the following will still be accessible without knowing the password:

- The **Ctrl+D** diagnostics

And the following items in the bootloader menu:

- Adjust the console baud rate
- System information
- Restore Bootloader factory settings (which does not clear password protection)

The next level of security is equivalent to the second one, except that there is no longer any access to the **skip startup script** option and to the **special boot options** section of the bootloader menu, even if the user knows the password.

Instead, there is a new **completely erase Flash** item in the bootloader menu, that now becomes the only option a user has for recovering the switch if the Admin password is lost.

To use this **security level** menu item, proceed as follows:

1. Type 's' to choose the **security level** option:

```
Enter selection ==> s
```

2. You will receive the following menu:

```
Security Settings menu:
```

```
The security Level is currently set to 1 (None)
```

```
-----  
0. Return to previous menu  
1. Set security Level to 2 (Password Protected)  
2. Set security Level to 3 (Locked Down)
```

```
Enter selection ==>
```

3. Type '2' to choose **security level 3**:

```
Enter selection ==> 2
```

4. You will receive the following output:

```
WARNING: This option will set the security level to three(3) .
```

```
Once the password has been set, some bootloader menu items  
will require authentication.
```

```
Press Y to proceed, or any other key to return to the previous menu ==>
```

5. Type 'y' to proceed:

```
Press Y to proceed, or any other key to return to the previous menu ==> y
```

6. Follow the instructions to set a password:

```
Enter new password: *****
```

```
Retype new password:*****
```

**7.** You will receive the following output:

```
Password successfully updated
```

```
Security Level set to 3 (Locked Down)
```

```
Security Settings menu:
```

```
The security Level is currently set to 3 (Locked Down)
```

- ```
-----  
0. Return to previous menu  
1. Set security Level to 1 (None)  
2. Change Password
```

```
Enter selection ==>
```

**8.** Type '0' to return to the main bootloader menu:

**Note:** Once you have chosen security level 3, the only way to return to a lower security level is to completely erase flash and NVS. So, if, in the menu above, you type 1, to go back to security level 1

```
Enter selection ==> 1
```

**9.** You will receive the following output:

```
WARNING: This option will reset the security level to One.  
which will DESTROY the entire contents of the FLASH file system  
Press Y to proceed, or any other key to return to the previous menu ==>
```

**10.** Press 'Y', and the Flash and NVS memory will be cleared.

## Boot options

A powerful feature of AlliedWare Plus is the ability to boot from a variety of sources.

With AlliedWare Plus the switch can boot directly from sources such as a USB stick, SD card or network server. This provides a very flexible system, with multiple options to upgrade software releases and for system recovery.

Details of the bootloader menu options are as follows:

1. Perform one-off boot from alternate source.

Enter 1 in the top-level menu to provide the following one-off boot options:

```
Enter selection ==> 1

Select device:

0. Return to previous menu
-----
1. Flash      (flash:)
3. TFTP       (tftp://)
4. YMODEM     (ymodem:)
6. USB        (usb:)

Enter selection ==>
```

You can select a one-off boot from Flash, USB storage device, SD (or SDHC) card, network server (TFTP), or ymodem. The selected option will be used for the next restart (only) of the switch. If you select to boot from TFTP, the bootloader prompts the user for the required network address details.

**Note:** These settings are specific to the bootloader. They are not related in any way to what may be configured by the main software release.

```
Run DHCP to populate defaults ..... [N]:
Enter IP address for this device ..... []: 10.52.18.20 10
Enter subnet mask ..... []: 255.255.254.0
Enter gateway IP ..... []: 10.52.18.1
Enter TFTP server IP ..... []: 10.52.18.144
Enter filename ..... []: x610-5.4.4-3.5.rel
Loading tftp://10.52.18.144/x610-5.4.4-3.5.rel...
```

When the switch is booted up using the ‘one-off’ selected source for the software release, it provides the option to copy the release just used to Flash for further/permanent use:

```
login: manager
Password: *****
The system has been booted using the one off boot/recovery
mechanism.
Bootup has successfully completed.
Write this release to flash? (y/n):
```

## 2. Change the default boot source (for advanced users)

```
Boot Menu:

WARNING: The bootloader is not currently password protected.
-----
B. Boot backup software
-----
S. Security Level
-----
0. Restart
1. Perform one-off boot from alternate source
2. Change the default boot source (for advanced users)
3. Update Bootloader
4. Adjust the console baud rate
5. Special boot options
6. System information
7. Restore Bootloader factory settings
-----
9. Quit and continue booting

Enter selection ==>
```

Entering **2** in the top-level menu provides the option to set the boot source permanently.

```
Enter selection ==> 2

NOTE: These settings are specific to the Bootloader.
They are not related in any way to what may be configured
by the 'boot system' command in the main software release.

Select device:

0. Return to previous menu
-----
1. Flash      (flash:)
3. TFTP       (tftp://)
4. YMODEM     (ymodem:)
6. USB        (usb:)
-----
9. Boot from default (determined by main CLI)

Enter selection ==> 1
```

The same boot source options are provided as with the one-off selection, but this time every restart of the switch will result in the unit booting from the selected source.

## 3. Update bootloader

This option allows for the bootloader code to be updated. It is not detailed here, as it is envisioned that this would rarely need to be done, and only at the request of (and with support from) Allied Telesis Technical Support.

#### 4. Adjust the console baud rate

```
Boot Menu:

WARNING: The bootloader is not currently password protected.
-----
B. Boot backup software
-----
S. Security Level
-----
0. Restart
1. Perform one-off boot from alternate source
2. Change the default boot source (for advanced users)
3. Update Bootloader
4. Adjust the console baud rate
5. Special boot options
6. System information
7. Restore Bootloader factory settings
-----
9. Quit and continue booting

Enter selection ==>
```

On IE200-6 Series switches, we do not recommend changing the baud rate. If you use this option to change the baud rate, that change does not apply until the switch has booted up. It does not actually change the baud rate for the bootloader. The bootloader always runs at 9600. Therefore, if you change the baud rate on IE200-6 Series switches, you lose the ability to control the bootloader. The baud rate of the console session is set here to match the terminal program being used for management of the switch when connected directly to the asynchronous port. The switch's default value is 9600. The baud rate selected can be set as the 'new' default for future use if preferred.

```
Select baud rate:

0. Return to previous menu
-----
1. 9600
2. 19200
3. 38400
4. 57600
5. 115200
6. 230400 (Setting can't be made permanent)
7. 460800 (Setting can't be made permanent)

Enter selection ==> 1
```

Change your terminal program baud rate to 9600 and press enter... if for some reason you are unable to do this, power cycle the device and the existing baud rate will be restored.

Use this baud rate by default? (Y/N) ==> n

## 5. Special boot options

Boot Menu:

WARNING: The bootloader is not currently password protected.

B. Boot backup software

S. Security Level

0. Restart

1. Perform one-off boot from alternate source

2. Change the default boot source (for advanced users)

3. Update Bootloader

4. Adjust the console baud rate

5. Special boot options

6. System information

7. Restore Bootloader factory settings

9. Quit and continue booting

Enter selection ==>

The special boot options allow for system recovery in the event of a forgotten password or to the default configuration.

Special boot options menu:

0. Return to previous menu

1. Skip startup script (Use system defaults)

Enter selection ==>

## 6. System information

Boot Menu:

WARNING: The bootloader is not currently password protected.

B. Boot backup software

S. Security Level

0. Restart

1. Perform one-off boot from alternate source

2. Change the default boot source (for advanced users)

3. Update Bootloader

4. Adjust the console baud rate

5. Special boot options

6. System information

7. Restore Bootloader factory settings

9. Quit and continue booting

Enter selection ==>

The system information option provides some details on the hardware platform in use, such as CPU, memory, hardware (MAC) address and so on.

```
Enter selection ==> 6

System information:

System (Detected values)
-----
CPU:
    Type .....: MIPS32_4KC
Memory:
    Total installed ....: 256 MB
Flash:
    Total installed ....: 64 MB
-----
Product information
-----
Compatible software ...: 14 (r14)
Serial .....: NONE
Manufacture date ....: 01/IE2002000
Product .....: 409
Product name .....: IE200-6GT
Revision .....: A
First MAC address ....: 00:0c:25:03:9a:72
-----
Boot software information
-----
Version .....: 3.0.0-devel / 1.0_22
Build time .....: Apr 8 2014 - 15:40:41
Built by .....: bheineman
Build host .....: imgbuild01.atg.lc
Build key .....: IE200
Compatible products:
    409 .....: IE200-6GT
    410 .....: IE200-6GP
    411 .....: IE200-6GPW
-----
Press any key to continue...
```

## 7. Restore bootloader factory settings

This option allows the bootloader to be set back to factory defaults.

**Caution**

**This option erases any settings that may have been configured by this menu**

**Are you sure? (Y/N) ==>**



The bootloader menu provides a powerful set of options for flexibility in the way software releases are upgraded on the switch, and system recovery is performed.

## Startup Sequence

Once the bootloader has performed its system initialization, it passes control to the main Operating System image, which then begins its startup sequence. The startup sequence for a device running AlliedWare Plus under normal circumstances will be as seen below. This sequence will be seen when everything loads and runs as expected.

```
AlliedWare Plus (TM) 5.4.4 11/14/14 13:00:27
Bootloader 1.1.0 loaded
Press <Ctrl+B> for the Boot MenuReading flash:x610-5.4.4-3.5.rel...
Verifying release... OK
Booting...
Starting base/first... [ OK ]


```

```
Allied Telesis Inc.
AlliedWare Plus (TM) v5.4.4
Original release filename: x610-5.4.4-3.5.rel
Built: Fri Nov 14 13:00:27 NZDT 2013 by: maker@awpmaker05-d1

Mounting virtual filesystems... [ OK ]
Mounting static filesystems... [ OK ]
Mounting flash... [ OK ]
Checking NVS filesystem... [ OK ]
Mounting NVS filesystem... [ OK ]
Starting base/dbus... [ OK ]
Starting base/klogd... [ OK ]
Starting base/loopback... [ OK ]
Starting base/sysctl... [ OK ]
Starting base/syslog... [ OK ]
Starting base/appmond... [ OK ]
Starting base/portmapper... [ OK ]
Starting base/cron... [ OK ]
Starting hardware/openhpi... [ OK ]
Starting hardware/timeout... [ OK ]
Starting base/autofs... [ OK ]
Starting base/inet... [ OK ]
Starting base/modules... [ OK ]
Received event baseboard.found
Received event hardware.done
Starting network/startup... [ OK ]
Starting hardware/openhpiolog... [ OK ]
Starting network/trigger... [ OK ]
Starting network/election.timeout... [ OK ]
Starting network/stackd... [ OK ]
Received event network.enabled

Initializing HA processes:
auth, bgpd, cntrd, epsr, hostd, hsl, imi
irdpd, lacp, loopprot, mstp, nsm, openhpid, ospfd
pdmd, pimd, ripd, ripngd, rmon, vrrpd

Received event network.initialized
Received event vcs.elected-master
09:39:40 awplus VCS[997]: Member 1 (0015.7793.20c3) has become the Active Master

Assigning Active Workload to HA processes:
authd, bgpd, epsrd, hsl, irdpd, lacpd, loopprot
mstpd, nsm, ospfd, pdmd, pimd, ripd, ripngd
rmond, vrrpd, imi

Received event network.activated
Loading default configuration
.
done!
Received event network.configured
```

**Note:** To enter the bootloader or diagnostic menus, **Ctrl+B** or **Ctrl+D** must be entered when prompted before the software modules start loading.

The example output below shows the startup sequence for a SwitchBlade x8100 running VCStack Plus™.

```
Verifying release... OK
Booting...
Starting base/first...
Mounting virtual filesystems... [ OK ] [ OK ]

Allied Telesis Inc.
AlliedWare Plus (TM) v5.4.4
Current release filename: SBx81CFC960-5.4.4-3.5.rel
Original release filename: SBx81CFC960-5.4.4-3.5.rel
Built: Thu Dec 19 21:30:52 NZDT 2013
Mounting static filesystems... [ OK ]
Checking flash filesystem... [ OK ]
Mounting flash filesystem... [ OK ]
Checking for last gasp debug output... [ OK ]
Checking NVS filesystem... [ OK ]
Mounting NVS filesystem... [ OK ]
Starting base/setup-eth... [ OK ]
Starting base/dbus... [ OK ]
Starting base/syslog... [ OK ]
Starting base/lif_ok... [ OK ]
Starting base/loopback... [ OK ]
Starting base/poe_done... [ OK ]
Starting base/sysctl... [ OK ]
Starting base/portmapper... [ OK ]
Starting base/reboot-stability... [ OK ]
Checking system reboot stability... [ OK ]
Starting base/cron... [ OK ]
Starting base/appmond... [ OK ]
Starting hardware/openhpi... [ OK ]
Starting hardware/timeout... [ OK ]
Starting base/inet... [ OK ]
Starting base/modules... [ OK ]
Starting network/startup... [ OK ]
Starting base/external-media... [ OK ]
Starting network/stackd... [ OK ]
Starting network/election.timeout... [ OK ]
Starting network/internal-tftpd... [ OK ]
Starting network/internal-bootp... [ OK ]
07:49:46 awplus-2.5 chassis[2105]: Card 2.6 (AT-SBx81CFC960) has joined the chassis
Received event network.enabled
Initializing HA processes:
cntrd, hostd, nsm, atmfd, auth, bgpd, epsr, exfx, hsl, imi, imiproxyd, irdpd, lacp, lldpd, loopprot, mstp, ospf6d, ospfd, pdmd, pim6d, pimd, ripd, ripngd, rmon, sflowd, udldd, vrrpd
Received event network.initialized
07:49:52 awplus-2.5 chassis[2105]: Waiting for all chassis cards to initialize...
07:50:12 awplus-2.6 HPI: HOTSWAP Pluggable 2.6.4 hotswapped in: AT-StackOP
07:50:13 awplus-2.6 HPI: HOTSWAP Pluggable 2.6.1 hotswapped in: AT-StackOP
07:50:17 awplus-2.5 HPI: HOTSWAP Pluggable 2.5.1 hotswapped in: AT-StackOP
07:50:17 awplus-2.5 HPI: HOTSWAP Pluggable 2.5.4 hotswapped in: AT-StackOP
07:50:50 awplus-2.5 chassis[2105]: Card 2.1 (AT-SBx81XS6) has joined the stack
07:50:51 awplus-2.5 chassis[2105]: Card 2.3 (AT-SBx81GT24) has joined the stack
07:50:51 awplus-2.5 chassis[2105]: Card 2.2 (AT-SBx81GP24) has joined the stack
07:50:51 awplus-2.5 chassis[2105]: Card 1.5 (AT-SBx81CFC960) has joined the stack
07:50:51 awplus-2.5 chassis[2105]: Card 1.6 (AT-SBx81CFC960) has joined the stack
07:50:51 awplus-1.6 HPI: HOTSWAP Pluggable 1.6.4 hotswapped in: AT-StackOP
07:51:02 awplus-2.5 chassis[2105]: Card 1.1 (AT-SBx81GT24) has joined the stack
07:51:03 awplus-2.5 chassis[2105]: Card 1.3 (AT-SBx81XS6) has joined the stack
07:51:04 awplus-2.5 chassis[2105]: Card 1.4 (AT-SBx81GP24) has joined the stack
07:51:20 awplus-2.5 chassis[2105]: Card 2.5 (AT-SBx81CFC960) has become the Active CFC
07:51:22 awplus-2.5 chassis[2105]: Stack Virtual MAC is 0000.cd37.0c22
Received event vcs.elected-master
done!
Received event network.configured
```

There are three possible status results displayed for each module loaded:

- **OK** means that the module has loaded correctly.
- **INFO** means that an error occurred, but the device is usable.
- **ERROR** means that an error occurred and device operation may be affected.

Additional specific information accompanies an INFO or ERROR status result. For example, if a corrupt release file was set as the startup release, the following error message would be seen:

```
Bootloader 3.0.0-devel loaded
Press <Ctrl+B> for the Boot Menu
Reading filesystem...
Error: Release filename is invalid (should be x610-5.4.4-3.5.rel)
Error: There is no backup release file set
Error: Boot failed. Please recover the system using the Boot Menu
Restarting...Bootloader 3.0.0-devel loaded
Press <Ctrl+B> for the Boot Menu
```

Whether an error message results in a case of the device being unusable will depend on the specific error and message, so will need to be dealt with on a case by case basis. If a software release has been corrupted, as shown on startup, a new release may need to be loaded.