ADTRAN

AOS

Implementing Auto-Config Using the CLI

Basic Configuration Guide

September 2018
61200560L1-29.2E

To the Holder of this Document

This document is intended for the use of ADTRAN customers only for the purposes of the agreement under which the document is submitted, and no part of it may be used, reproduced, modified or transmitted in any form or means without the prior written permission of ADTRAN.

The contents of this document are current as of the date of publication and are subject to change without notice.

Trademark Information

“ADTRAN” and the ADTRAN logo are registered trademarks of ADTRAN, Inc. Brand names and product names included in this document are trademarks, registered trademarks, or trade names of their respective holders.

Disclaimer of Liability

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products are given “as is”, and any liability arising in connection with such hardware or software products shall be governed by ADTRAN’s standard terms and conditions of sale unless otherwise set forth in a separately negotiated written agreement with ADTRAN that specifically applies to such hardware or software products.

To the fullest extent allowed by applicable law, in no event shall ADTRAN be liable for errors in this document for any damages, including but not limited to special, indirect, incidental or consequential, or any losses, such as but not limited to loss of profit, revenue, business interruption, business opportunity or data, that may arise from the use of this document or the information in it.

©2018 ADTRAN, Inc.
All Rights Reserved.

Revision History

Rev E	September 2018	Initial release of this document in this format. Document updated to include information about the Auto-Config search for additional configuration file names as part of the new default fallback behavior for the AOS firmware R13.4.0 release.

Table of Contents

List of Figures

List of Tables

1 Overview

This configuration guide provides an overview of the automatic self-configuration feature (referred to as Auto-Config) in the ADTRAN Operating System (AOS), and includes the Command Line Interface (CLI) configuration options available for configuring and using Auto-Config in multiple network situations. Additionally, troubleshooting information, instructions for creating an Auto-Config configuration file, and additional documentation resources are also provided.

1.1 Intended Audience

The intended audience for this information is the network administrator using and configuring the AOS device. The instructions assume familiarity with the intended use of the equipment, basic required installation and configuration skills, and knowledge of local and accepted networking practices.

1.2 Document Structure

Table 1 lists the topics contained in this document

Table 1. Topic List

1.3 Hazard and Conventional Symbols

The following Hazard symbols are used throughout this guide:

WARNING!
Warning: Service affecting. Possible risk of system failure.

CAUTION!
Caution: Indicates that a failure to take or avoid a specific action could result in a loss of data.

NOTICE!
Notice: Provides information that is essential to the completion of a task.

NOTE
Note: Information that emphasizes or supplements important points of the main text.

1.4 Related Online Documents and Resources

Refer to Table 2 for additional information for this device.

Documentation for AOS products is available for viewing and download directly from the ADTRAN Support Community website, available online at https://supportforums.adtran.com.

Table 2. Related Online Documents and Resources

Title	Description
AOS Command Reference Guide	Document outlining all available AOS commands, their variations and parameters, and their uses.
Upgrading Firmware in AOS	Configuration guide outlining the necessary steps to upgrade firmware for AOS products.

2 Auto-Config Overview

The Auto-Config feature provides an automated method for configuring a new AOS device by enabling a newly-deployed AOS device to download and apply configuration parameters automatically from a secondary configuration file, as well as to download and apply a new firmware file.

Auto-Config uses three main methods for providing a local AOS device with configuration information.The first method uses Trivial File Transfer Protocol (TFTP) to download a specific configuration file, and is typically employed in an enterprise network. The second method uses Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS) to download a specific configuration file, and is typically used in a service provider environment as an enhanced version of Auto-Config. Using the enhanced Auto-Config allows the local AOS device to redirect to a secondary server to receive additional configuration settings. The third method, Zero-Touch Provisioning, requires removing the startup configuration file on the AOS device prior to booting the device. Once the device is booted without a startup configuration file, it automatically downloads the necessary configuration settings from a host device using TFTP.

2.1 Auto-Config Attributes

There are several attributes that determine the way Auto-Config functions when it is initiated. Many of these attributes are optional and may not pertain to your specific network needs. These attributes are introduced in the following sections.

2.1.1 File Transfer Methods

The Auto-Config file transfer method specifies which of three protocols (TFTP, HTTP, or HTTPS) are used when transferring configuration files to an AOS device for the purpose of automatic configuration. By default, TFTP is used by Auto-Config for file transfer. If Auto-Config is configured to transfer files using HTTP or HTTPS, additional authentication parameters must be specified.

2.1.2 HTTP(S) Authentication Parameters

If HTTP(S) is being used for configuration file transfer, an authentication user name and password must be specified. This information must be transmitted from the local AOS device to the HTTP(S) server to allow the configuration file to download. The user name can be specified using system variables, such as: system name, serial number, description, software version, and medium access control (MAC) address.

Additionally, a specific MAC address can be used for authentication as part of the HTTP user agent header. To use this method, the MAC authentication mode must be enabled in Auto-Config, and a MAC address or interface must be specified.

2.1.3 Locating the Configuration Server Address

The configuration server is a network server or another AOS device that provides the configuration files necessary to complete Auto-Config on the AOS device being configured. The server is located using a specified static IPv4 address (or host name), or by the local AOS device using Dynamic Host Configuration Protocol (DHCP) to learn the server address. Optionally, DHCP Options 66 or 160 can also be used to specify the server address. When using either OPTION 66 or 160, the DHCP server must have the appropriate option defined in order to successfully locate the configuration server.

2.1.4 File Name Parameters

The file name refers to the name of the configuration file that is downloaded to the local AOS device and applied to its running configuration. This file must exist on the host device in order for it to be successfully downloaded. Files can be specified using a file name or a system variable. System variables represent system parameters such as: system name, serial number, description, software version, and MAC addresses. DHCP OPTION 67 can also be used to specify the file name.

If no file name is specified, Auto-Config attempts to locate additional configuration files on the server device as a fallback measure. The configuration file names searched for in such a situation include (in order of priority): a file name based on MAC addresses (**`<MAC#1>.cfg`**), a file name based on the AOS device part number (**`adtran_<Unit Part Number>.cfg`**), and the ADTRAN default file name (**`adtran_000000000000.cfg`**).

2.1.5 Applying Received Configuration Settings

When a local device retrieves configuration settings from a host device through TFTP, HTTP, or HTTPS, the new configuration settings can be applied to the local device by either appending the new information to the existing running configuration (and saved manually), or by overwriting the existing startup configuration.

2.1.6 Firmware Download Settings

Optionally, you can configure Auto-Config to download and apply new primary and secondary firmware images to the local AOS device.

2.1.7 Initiating Auto-Config

If Auto-Config is currently off or disabled on the local AOS device, there are several methods that can be used to initiate Auto-Config. You can choose to manually initiate Auto-Config using the **`auto-config`** or **`auto-config restart`** commands from either the Global Configuration mode or Enable mode, respectively. Additionally, you can configure the device's startup configuration file to include the **`auto-config`** command, in which case, when the configuration file is processed, Auto-Config initiates.

Alternatively, when an AOS device is configured to use IP SIP, and Auto-Config is configured with a SIP user that accepts check-sync events (using the **`auto-config sip-notify user`** *`<user>`* command), Auto-Config will automatically initiate when the device receives a SIP NOTIFY message with a check-sync event.

Lastly, Auto-Config can be initiated using Zero-Touch Provisioning, so called because no one directly drives the process. This method is only available on certain AOS units. Auto-Config will initiate when a device boots up with no startup configuration file present on the local file system. Not all units trigger Auto-Config when booted without a startup configuration file.

Once started, the Auto-Config process can be stopped by entering the **`no auto-config`** command from the Global Configuration mode prompt.

3 Hardware and Software Requirements and Limitations

The Auto-Config and Zero-Touch Provisioning Auto-Config features are only available on AOS products as outlined in the *AOS Feature Matrix*, available online at ADTRAN's Support Forum, https://supportforums.adtran.com.

At this time, Auto-Config can only be configured using the command line interface (CLI).

Only certain AOS devices support SIP NOTIFY check-sync events. In order for the SIP NOTIFY message to be received, the AOS device must support IP SIP messaging (this excludes switches and routers without SIP Proxy), and have it enabled in its configuration. In addition, the firewall must be provisioned to allow it to receive SIP messages from the server.

As of AOS firmware release R13.4.0, Auto-Config can attempt to locate additional configuration files on a server device if a file name is not specified. The configuration file names searched for in such a situation include (in order of priority): a file name based on MAC addresses (*<MAC#1>*.cfg), a file name based on the AOS device part number (adtran_*<Unit Part Number>*.cfg), and the ADTRAN default file name (adtran_000000000000.cfg). The priority of file types is set by default. To support the search for additional configuration files, the number of Auto-Config retry attempts must be set to either 0 (infinite) or a minimum of 3.

4 Connect to the AOS CLI

To configure Auto-Config using the CLI, connect to the AOS device using these steps:

1. Boot up the device.
2. Telnet to the device (**telnet** *<ip address>*), for example:

```
telnet 10.10.10.1
```

NOTE
If during the device's setup process you have changed the default IP address (10.10.10.1), use the configured IP address.

3. Enter your user name and password at the prompt.

NOTE
The AOS default user name is **admin** and the default password is **password**. If your device no longer has the default user name and password, contact your system administrator for the appropriate user name and password.

4. Enable your device by entering **enable** at the prompt as follows:

```
>enable
```

5. If configured, enter your Enable mode password at the prompt.
6. Enter the device's Global Configuration mode as follows:

```
#configure terminal
(config)#
```

7. From the Global Configuration mode, enter the commands necessary to configure Auto-Config using one of the following methods:
   - "Configuring Auto-Config Using the CLI" on page 13
   - "Implementing Auto-Config with Zero-Touch Provisioning" on page 19

5 Configuring Auto-Config Using the CLI

The following sections outline the steps necessary to configure Auto-Config using the CLI. Basic Auto-Config configuration includes specifying the file transfer method, the HTTP authentication method, the configuration file name, the application of the configuration information to the AOS device, and then initiating the Auto-Config process. Several additional configuration options, such as specifying a host server location, additional authentication parameters, Auto-

Config retry attempts, and whether firmware is also downloaded. These configuration options are discussed in the following sections.

5.1 Step 1: Specifying the File Transfer Method

Begin Auto-Config configuration by specifying the protocol to use when transferring the configuration file from a server to the AOS device using the **auto-config method [tftp | http [port** *<number>* **| https port** *<number>***]** command from the Global Configuration mode. By default, Auto-Config uses TFTP to transfer files. You can specify that HTTP or HTTPS is used as the file transfer method by entering the **https** or **http** keywords. By default, the HTTP port 80 and HTTPS port 443 are used if no ports are specified. Valid port range is **1** to **65535**. To specify HTTP is used for file transfers, using the default port, enter the command from the Global Configuration mode prompt as follows:

```
(config)#auto-config method http
```

To return to using TFTP as the file transfer method, enter the **auto-config method tftp** command from the Global Configuration mode prompt as follows:

```
(config)#auto-config method tftp
```

5.2 Step 2: Specify the Configuration Server Address (Optional)

The configuration server is located through DHCP using either OPTION 66 or OPTION 160, or by specifying the host name or IPv4 address. When using either OPTION 66 or 160, the DHCP server must have the appropriate option defined in order to successfully locate the configuration server.

Use the **auto-config server [dhcp [option 66 | option 160]] [***<hostname>* **|** *<ipv4 address>***]** command from the Global Configuration mode prompt to specify how Auto-Config locates the server with the configuration file. The **dhcp option 66** and **dhcp option 160** parameters specify that DHCP OPTION 66 or DHCP OPTION 160 are used, respectively. By default, Auto-Config uses DHCP OPTION 66 to locate the server. Alternatively, you can specify the host name of the server using the *<hostname>* parameter, or an IPv4 address of the server using the *<ipv4 address>* parameter. IPv4 addresses should be expressed in dotted decimal notation (for example, **10.10.10.1**).

To specify that DHCP OPTION 160 is used to locate the server, enter the command from the Global Configuration mode prompt as follows:

```
(config)#auto-config server dhcp option 160
```

5.3 Step 3: Configure Authentication for HTTP(S) File Transfer (Optional)

By default, Auto-Config uses TFTP for transferring configuration files. You can optionally choose instead to use HTTP or HTTPS for file transfers, but using either HTTP or HTTPS indicates that device authentication must occur before the file transfer is allowed. Device authentication can be achieved using either a user name and password, or the MAC address of the device, to confirm the identity of the device requesting the files. Each of these authentication methods are optional and their use depends upon your network needs.

5.3.1 Specifying an Authentication User Name and Password

A user name and password for HTTP(S) authentication can be specified using the following command:

```
(config)#auto-config authname <username> password <password>
```

NOTE
The default user name is **adtran** and the default password is **adtran**.

The user name can also be specified using the following system variables to indicate system parameters:

- **$SYSTEM_NAME** - the host name of the system
- **$SYSTEM_SERIAL_NUMBER** - the serial number of the system
- **$SYSTEM_DESCRIPTION** - the device name and software version
- **$SYSTEM_SOFTWARE_VERSION** - the running software version
- **$AUTH_MAC_ADDRESS** - MAC address for MAC authentication

In the following example, **$SYSTEM_NAME** is used to define the user name, and a password is provided:

```
(config)#auto-config authname $SYSTEM_NAME password fRiax&crOus9I#p
```

5.3.2 Using the MAC Address for HTTP(S) Authentication

Authentication for HTTP(S) file transfers can also be achieved using a MAC address. To use this method, you must first enable the MAC authentication mode in Auto-Config using the **auto-config mac-auth mode http-user-agent** command. Next, you must specify either a MAC address to include in the HTTP User Agent header, or an interface from which to use the assigned MAC address using the **auto-config mac-auth [address** *<mac address>* **| interface** *<interface> <slot/port>***]** command. MAC addresses should be expressed in the following format **xx:xx:xx:xx:xx:xx** (for example, **00:A0:C8:00:00:01**). For this command, colons are optional. Interfaces should be specified in the format *<interface type [slot/port | slot/port.subinterface id | interface id | interface id.subinterface id]>*. For example, for an Ethernet interface, use **eth 0/1**, for an Ethernet subinterface, use **eth 0/1.1**. Type **auto-config mac-auth interface ?** for a complete list of valid interfaces.

To configure Auto-Config to use a specific MAC address for authentication, enter the commands as follows:

```
(config)#auto-config mac-auth mode http-user-agent
(config)#auto-config mac-auth address 00:A0:C8:00:00:01
```

To configure Auto-Config to use the MAC address from an interface, enter the commands as follows:

```
(config)#auto-config mac-auth mode http-user-agent
(config)#auto-config mac-auth interface ethernet 0/1
```

To disable MAC address authentication, enter the following command:

```
(config)#auto-config mac-auth mode none
```

5.4 Step 4: Configure the Auto-Config HTTP Authentication Mode

Auto-Config uses two types of HTTP authentication for configuration files (in addition to HTTP(S) authentication used for file transfers): a basic mode, which uses clear text authentication, and a digest mode, which uses encrypted text authentication. Both modes can be enabled or disabled individually, and by default, both modes are enabled.

To enable either the basic or digest authentication modes, enter the **auto-config http-auth basic** or **auto-config http-auth digest** commands as follows:

```
(config)#auto-config http-auth basic
(config)#auto-config http-auth digest
```

To disable either of the authentication modes, enter the **no** form of the command as follows:

```
(config)#no auto-config http-auth basic
(config)#no auto-config http-auth digest
```

NOTE
At least one mode must be enabled at all times. An error will occur if both authentication modes are disabled.

5.5 Step 5: Specify the Configuration File Name

Once initiated, Auto-Config searches for a configuration file on the file server to provide the local AOS device. When found, the file is downloaded from the file server using the method defined in "Step 1: Specifying the File Transfer Method" on page 14. The file name can be retrieved using DHCP OPTION 67, by entering the **auto-config filename dhcp** command (default method), or the file name can be specified using the **auto-config filename** *<name>* command (including the file path is optional). Additionally, the *<name>* parameter can be defined with an exact file name or by using the following system parameters that represent system values:

- **$SYSTEM_NAME** - the host name of the system
- **$SYSTEM_SERIAL_NUMBER** - the serial number of the system
- **$SYSTEM_DESCRIPTION** - the device name and software version
- **$SYSTEM_SOFTWARE_VERSION** - the running software version
- **$AUTH_MAC_ADDRESS** - MAC address for MAC authentication

To configure the device to retrieve the file name according to the DHCP OPTION 67, enter the command as follows:

```
(config)#auto-config filename dhcp
```

NOTE
When using DHCP OPTION 67, the DHCP server must have OPTION 67 defined in order successfully locate the file name.

To define the file name using one of the system parameters, enter the command as follows:

```
(config)#auto-config filename $SYSTEM_NAME.cfg
```

To define a file name using a system parameter and include the file path, enter the command as follows:

```
(config)#auto-config filename config/adtran/$SYSTEM_NAME.cfg
```

To define a specific file name, enter the command as follows:

```
(config)#auto-config filename AUTO_CONFIG.cfg
```

To define a specific file name and include the file path, enter the command as follows:

```
(config)#auto-config filename config/adtran/AUTO_CONFIG.cfg
```

By default, Auto-Config will search for additional configuration files if no file name has been specified. These searched file names are, in order of priority, a file name based on MAC addresses (*<MAC#1>*.**cfg**), a file name based on the AOS device part number (**adtran_***<Unit Part Number>*.**cfg**), and the ADTRAN default configuration file name (**adtran_000000000000.cfg**).

5.6 Step 6: Specify Auto-Config Retry Attempts (Optional)

Use the **auto-config retry-count** *<number>* command to specify the maximum number of retries allowed to download a configuration file. Valid *<number>* range is **0** to **1000**. By default, the number of retries is set to **0**, thus allowing the feature to continuously attempt to download a configuration file until the Auto-Config feature is disabled. To set the number of retries to **100**, enter the command as follows:

```
(config)#auto-config retry-count 100
```

NOTE

For Auto-Config to be able to search for additional default configuration file names if there is a problem with a specified file name, the number of Auto-Config retry attempts must be set to either **0** (infinite) or a minimum of **3**.

5.7 Step 7: Specify If the Configuration File is Appended or Replaced

Once the configuration file is obtained by Auto-Config, the new configuration settings can be appended to the existing running configuration using the **auto-config apply-config append** command, or can replace the existing startup configuration file using the **auto-config apply-config replace** command. Replacing the startup configuration will automatically reboot the device so that the new startup configuration will be used. The default setting is to append the running configuration file.

To append the configuration settings to the current running configuration, enter the command as follows:

```
(config)#auto-config apply-config append
```

To replace the startup configuration with the new configuration information, enter the command as follows:

```
(config)#auto-config apply-config replace
```

NOTE

Using the **append** keyword only appends the parameters to the currently running configuration. It does not affect the startup configuration file. The appended parameters will not be retained if the device is rebooted. To store the running configuration as the startup configuration after Auto-Config is done, make certain the last line of the configuration is the **do write** command.

5.8 Step 8: Specify the Firmware Download Settings (Optional)

The Auto-Config feature can optionally be used to download new firmware to the AOS device. Use the **auto-config firmware** command to specify the name and location of the firmware definition file to be downloaded. The firmware definition file specifies the path and file name of the firmware image to download. It also optionally specifies the local file name used to store the file. Additional parameters can be configured using other variations of this command.

To specify the path and static file name of the firmware definition file, enter the **auto-config firmware definition-file** *<path and file name>* command from the Global Configuration mode. The definition file consists of two lines, where the first line is the path and file name of the firmware file on the server, and the second line is an optional local file name. Blank lines are ignored when entering the path and file name, and any text entered after the first two lines is ignored. The following is an example of a firmware definition file that instructs

the device to download **Firmware/T900E3A-R11-10-2-E.biz** from the server and store it locally as **primary.biz: Firmware/T900E3A-R11-10-2-E.biz primary.biz**

```
(config)#auto-config firmware definition-file Firmware/T900E3A-R11-10-2-
 E.biz primary.biz
```

To specify whether to store the firmware image on the device's internal flash memory or CompactFlash memory, enter the **auto-config firmware destination [cflash | flash]** command from the Global Configuration mode prompt. The cflash keyword indicates that CompactFlash is used, and the flash keyword indicates that internal flash memory is used. To specify the firmware image is stored on CompactFlash, enter the command as follows:

```
(config)#auto-config firmware destination cflash
```

To enable the firmware image download, enter the **auto-config firmware download** command from the Global Configuration mode prompt as follows:

```
(config)#auto-config firmware download
```

To specify the delay, in seconds, after downloading the new firmware image before the device reboots, enter the **auto-config firmware reload-after** *<seconds>* command from the Global Configuration mode prompt. Valid delay range is **60** to **604800** seconds. A value of **0** seconds can be specified to disable the reboot. To specify the reboot delay as 100 seconds, enter the command as follows:

```
(config)#auto-config firmware reload-after 100
```

To specify whether the new firmware replaces the existing primary firmware on the AOS device, enter the **auto-config firmware replace primary [maintain | replace] secondary** command from the Global Configuration mode prompt. The **maintain** keyword specifies that the current primary firmware image is replaced with the new firmware, but the existing secondary firmware image is retained (if one exists). The **replace** keyword specifies that the current primary firmware image is replaced with the new firmware, and the existing primary firmware becomes the new secondary image (deleting the current secondary image if it exists). To specify that the primary image is replaced, while the secondary image is maintained, enter the command as follows:

```
(config)#auto-config firmware replace primary maintain secondary
```

To specify that the existing secondary firmware image is replaced with the new firmware image, while retaining the current primary image, enter the **auto-config firmware replace secondary** command from the Global Configuration mode prompt as follows:

```
(config)#auto-config firmware replace secondary
```

5.9 Step 9: Initiate Auto-Config

Once all of the Auto-Config settings are configured, Auto-Config must be initiated. You can choose to initiate Auto-Config manually, or it can be initiated when the AOS device receives a SIP NOTIFY message.

To restart the Auto-Config process, issue the **auto-config restart** command from the Enable mode prompt. Enter the commands as follows:

```
(config)#exit
#auto-config restart
```

Auto-Config can also be initiated by halting an ongoing Auto-Config process, and then restarting it, using commands from the Global Configuration mode. To stop (halt) Auto-Config processes once they have begun, enter the Global Configuration mode and enter the **no**

auto-config command, followed by the **auto-config** command to restart the Auto-Config process. Enter the commands as follows:

```
#configure terminal
(config)#no auto-config
(config)#auto-config
```

Auto-Config can also be initiated when the AOS device receives a SIP NOTIFY message. The SIP NOTIFY (check-sync event) can be configured to trigger the restart of Auto-Config using the **auto-config sip-notify user** *<user>* command. This command specifies a SIP user to receive the SIP NOTIFY (check-sync event) which triggers the Auto-Config process. Enter the command from the Global Configuration mode prompt as follows:

```
(config)#auto-config sip-notify user 2001
```

NOTE

Only certain AOS devices support SIP NOTIFY check-sync events. In order for the SIP NOTIFY message to be received, the AOS device must support SIP messaging (this excludes switches and routers without SIP proxy), and have SIP enabled in the configuration. The AOS device's firewall must also be provisioned to allow the device to receive SIP messages from the server.

6 Implementing Auto-Config with Zero-Touch Provisioning

Another method for implementing Auto-Config is by allowing the AOS device to self-configure upon start up, receiving the necessary configuration settings from a DHCP client on the host. This method is referred to as Zero-Touch Provisioning. Zero-Touch Provisioning can be used to replace a device that has already been in service, with a new device.

NOTE

Zero-Touch Provisioning is not available on all AOS products. Refer to the AOS Feature Matrix, available online at ADTRAN's Support Forum, https://supportforums.adtran.com for a complete list of the platforms capable of using this method.

Zero-Touch Provisioning does not require changing any of the default settings for Auto-Config. Instead, the AOS device is rebooted after removing the startup configuration file. The device goes through the Auto-Config process and finds the network device from which to download its configuration file. The steps to initiate Zero-Touch Provisioning and the process which occurs are outlined in the following sections.

6.1 Initiating Zero-Touch Provisioning

To initiate Zero-Touch Provisioning, follow these steps:

1. Remove the startup configuration from the AOS device by entering the **erase startup-configuration** command from the Enable mode prompt as follows:

   ```
   (config)#erase startup-configuration
   ```

2. Once the startup configuration is removed, reboot the AOS device by entering the **reload** command from the Enable mode prompt as follows:

   ```
   (config)#reload
   ```

After the startup configuration has been removed, and the device has been rebooted, it will no longer show a startup configuration file while booting. For example, the output of a NetVanta 1534 booting up without a startup configuration file is shown below:

```
ADTRAN, Inc., NetVanta 1534 (1702590G1)
AOS Version: R10.04.00, Checksum 5F091215, Wed Jul 27 13:26:46 2012
Cause of reset: External Hard Reset
vfs: NONVOL: 240 tracks, 64 sectors/track, 1024 bytes/sector.
SNMP Agent: Starting: Success!
FTP server: Starting service on first mounted drive.
cli: starting user interface
Gigabit switch chip initializing
No startup-config found.
Starting Auto-Config, press enter to begin or...
You have 60 seconds to press escape to halt Auto-Config.
```

Once the device discovers that it does not have a startup configuration file (highlighted in line 9 of the previous output), AOS triggers Auto-Config, but allows the user 60 seconds to respond to the prompt. There are two valid key responses. Each have different outcomes as explained below.

- **Escape** key - Cancels Auto-Config and AOS boots without any loaded startup configuration file.
- **Enter** key - Aborts the remaining portion of the 60-second waiting period and the device immediately proceeds to booting with Auto-Config active.

If neither key is pressed at the prompt, the timer expires within 60 seconds and the device continues with the Auto-Config process.

Once Auto-Config is initiated, the following message displays:

```
2005.10.12 12:59:52 AUTOCONFIG Started. To halt enter config-mode and
 type "no auto-config".
```

6.2 Auto-Config Process in Zero-Touch Provisioning

Once Auto-Config is triggered, a series of events occurs. The following information is provided to assist with understanding the process and what occurs on the device.

NOTE

Auto-Config alters a device's configuration ONLY if the device is booted without a startup configuration file. If Auto-Config is triggered by other means, it assumes the device's running configuration allows network connectivity to download the file and does not change the settings.

NOTE

When Auto-Config terminates, it does not automatically undo any of the settings. If it is desired that the device's final running configuration not retain any of the settings added in this step, the user must either disable them manually or add commands that disable them to the file downloaded and applied by Auto-Config.

1. First, Auto-Config enables basic IP connectivity to ensure the steps that follow will complete successfully. For example, on a switch this means that Auto-Config enables VLAN 1 with all switchports in VLAN 1, and enables the DHCP client for the interface. The equivalent CLI input is as follows:

```
int vlan 1
  ip address dhcp
  no shutdown
```

2. Second, Auto-Config enables all non-switch Ethernet ports and activates a DHCP client on these ports. For example, on a NetVanta 3305 (a router with two Ethernet ports), the equivalent CLI input is as follows:

```
interface ethernet 0/1
  ip address dhcp
  no shutdown
  exit

interface ethernet 0/2
  ip address dhcp
  no shutdown
```

3. Next, once DHCP is enabled, one of the DHCP clients obtains a lease from a DHCP server on the network. The lease includes a file name (DHCP OPTION 67) and a TFTP server address (DHCP OPTION 66) as well as the lessee's IPv4 address. Auto-Config then uses this information to download the configuration file.

   There can be multiple DHCP clients operating on a single Auto-Config host. AOS keeps DHCP clients ordered internally, and Auto-Config uses data from the first DHCP client that provides both options 66 and 67.

   Auto-Config uses TFTP to attempt to download the configuration file. If all the necessary data is present, the file is downloaded from the host. The current Auto-Config status displays **Downloading** as shown in the following output from the **show auto-config** command:

```
#show auto-config
Auto-Config is enabled, current status: Downloading.
 File transfer method is TFTP
 Config Server is 10.10.10.1
 Config filename is TESTFILE
 Maximum retry count is 0 (repeat indefinitely), total retries is 0
 Last failure: HTTP: Could not send initial message to HTTP server
```

NOTE

The **show auto-config** command (entered from the Enable mode prompt) displays the current state of the Auto-Config feature. For a complete explanation of the output displayed, see "Troubleshooting" on page 34.

If TFTP fails to download the file, Auto-Config waits for 60 seconds and re-attempts the download. The current status displays **Download Pending** as shown in the following output from the **show auto-config** command:

```
#show auto-config
Auto-Config is enabled, current status: Download Pending.
File transfer method is TFTP
Config Server is 172.20.15.174
Config filename is not set
Default Fallback filename [00A0C8AE103A.cfg | adtran_4700254F2.cfg |
  adtran_000000000000.cfg], Current: (adtran_000000000000.cfg)
Maximum retry count is 10, total retries is 0
Polling timer: not active
Last failure: waiting
```

The maximum number of retries is set to **0** by default, which means downloads will repeat indefinitely until a successful download occurs. If Auto-Config is unable to download the configuration file within the maximum number of retries, a failure is declared and Auto-Config is halted. The current status displays as **Download failed** as shown in the following output from the **show auto-config** command:

```
#show auto-config
Auto-Config is enabled, current status: Download failed.
File transfer method is TFTP
Config Server is myServer
Config filename is abc.cfg
Default filename is [00A0C8AE103A.cfg | adtran_4700254F2.cfg |
  adtran_000000000000.cfg], Current: (Disabled)
Maximum retry count is 0 (repeat indefinitely), total retries is 0
Last failure: DNS could not resolve host name
```

NOTE

The download process may not resolve on the first attempt and could require subsequent attempts to resolve successfully.

4. If the configuration file is successfully received, Auto-Config proceeds to apply the configuration file to the device's running configuration. Applying the configuration file affects the running configuration only, not the startup configuration file. To store the running configuration as the startup configuration after Auto-Config is complete, make certain the last command of the downloaded file is **do write**. The equivalent CLI input is as follows:

```
auto-config server SERV1
auto-config filename TESTFILE
!
!
vlan 100
  name "VLAN0100"
vlan 101
  name "VLAN0101"
!
end
```

7 Configuration Examples

The examples contained in this section are designed to enhance the understanding of Auto-Config configurations on AOS products, and to provide real-world CLI configuration for typical network usage.

NOTE

The configuration parameters entered in these examples are sample configurations only. These applications should be configured in a manner consistent with the needs of your particular network. CLI prompts have been removed from the configuration examples to provide a method of copying and pasting configurations directly from this configuration guide into the CLI. These configurations should not be copied without first making the necessary adjustments to ensure they will function properly in your network.

7.1 Standard Auto-Config with TFTP Method

In this example, a Total Access 916 automatically configures itself from a NetVanta 3305 following a standard Auto-Config approach using TFTP to transfer the configuration file and a DHCP server to assign an IPv4 address. The connectivity between these two units is shown in Figure 1, as well as the communication that occurs between the devices during the automatic configuration process.

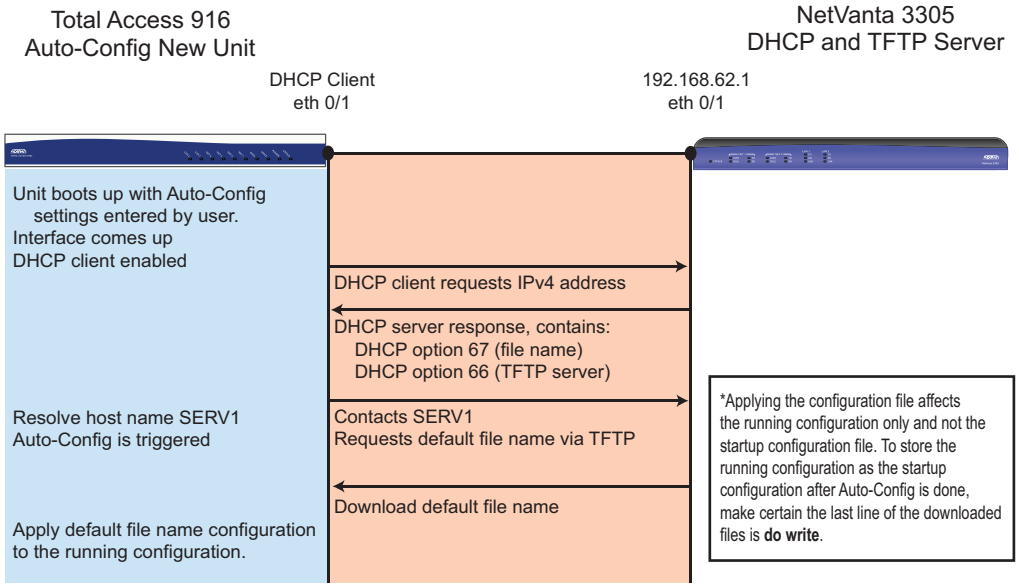

Figure 1. Example of Auto-Config Using a TFTP and DHCP Server

In this example, the Total Access 916 is a new device on the network and uses a startup configuration file (**CONFIG-TA916.cfg**) to prepare itself through automatic configuration. The NetVanta 3305 acts as the DHCP and TFTP servers in this scenario. The following are the CLI configurations for the Total Access 916 and the NetVanta 3305

Total Access 916 Configuration

The following commands are entered into the Total Access 916:

```
config terminal
!
interface eth 0/1
```

```
  ip address dhcp
  media-gateway ip primary
  no shutdown
  exit
!
auto-config
!
end
```

NetVanta 3305 Running Configuration

The following output shows the pertinent information from the running configuration of the NetVanta 3305:

```
show running-config
Building configuration...
!
hostname "Router3305"
!
interface eth 0/1
  ip address 192.168.62.1 255.255.255.0
  no shutdown
!
ip route 0.0.0.0 0.0.0.0 10.20.20.2
!
ip dhcp-server pool "POOL1"
  network 192.168.62.0 255.255.255.0
  option 66 ascii 192.168.62.1
  option 67 ascii CONFIG-TA916.cfg
!
end
```

Contents of the CONFIG-TA916.cfg Configuration File

Since the NetVanta 3305 is also acting as the TFTP server, its file system must contain the configuration file (**CONFIG-TA916.cfg**) for the new device to download. The configuration file will configure the device. The Total Access 916 obtains the TFTP server address and TFTP file name via DHCP.

The following are the contents of the file **CONFIG-TA916.cfg**:

```
show file CONFIG-TA916.cfg
voice feature-mode network
!
voice dial-plan 1 local NXX-XXXX
voice dial-plan 2 long-distance 1-NXX-NXX-XXXX
!
voice class-of-service GLOBAL
  call-privilege all
!
voice codec-list GLOBAL
  default
  codec g729
  codec g711ulaw
```

```
!
voice trunk T01 type sip
  sip-server primary 10.0.0.1
  registrar primary 10.0.0.1
!
voice grouped-trunk MAIN
  trunk T01
  accept $ cost 0
voice user 1001
  connect fxs 0/1
  cos day "GLOBAL"
  sip-identity 1001 T01 register auth-name USER1 password PASSWORD1
  codec-group GLOBAL
!
voice user 1002
  connect fxs 0/2
  cos day "GLOBAL"
  sip-identity 1002 T01 register auth-name USER2 password PASSWORD2
  codec-group GLOBAL
!
ip sip
!
line telnet 0 4
  login
  password adtran
!
auto-config
!
do write
!
```

7.2 Enhanced Auto-Config for Broadsoft Device Management

In this example, a Total Access 916 is a new device to be installed and the host device is a NetVanta 3305 configured as both the DHCP and HTTPS servers. The Total Access 916 is manually configured with the Ethernet interface (**`eth 0/1`**) set to **`dhcp`**, the **`auto-config apply-config`** is set to **`replace`**, the **`auto-config transfer method`** is set to **`https`** with authentication credentials provided, and SIP NOTIFY messages are accepted to trigger a restart of Auto-Config. When the Total Access 916 requests a DHCP address, it receives OPTION 66 and 67 from the host device.

The connectivity between these two units, as well as the communication between the devices that occurs during the automatic configuration process, are shown in Figure 2 on page 26.

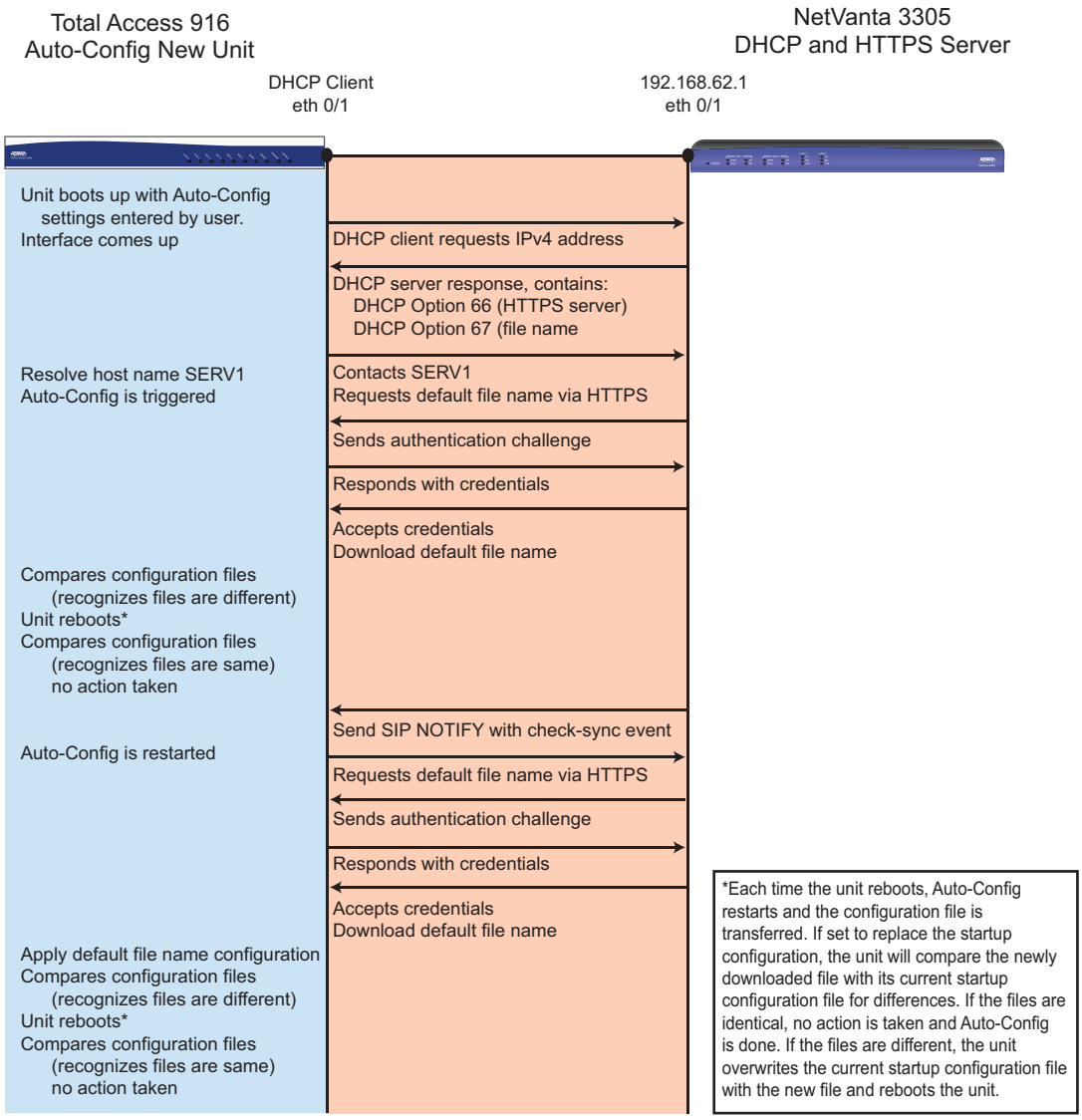

Figure 2. Application Example for Broadsoft Device Management

The configuration of both units in this scenario are provided below, as well as the configuration file that is downloaded from the host device to the Total Access 916.

Total Access 916 Configuration

The following commands are entered into the Total Access 916:

```
config terminal
!
interface eth 0/1
  ip address dhcp
  media-gateway ip primary
  no shutdown
  exit
!
```

```
auto-config
auto-config apply replace
auto-config authname $SYSTEM_SERIAL_NUMBER password fRiax&crOus9I#p
auto-config method https
!
!
end
```

NetVanta 3305 Running Configuration

The following output shows the pertinent information from the running configuration of the NetVanta 3305:

```
show running-config
Building configuration...
!
hostname "Router3305"
!
interface eth 0/1
  ip address 192.168.62.1 255.255.255.0
  no shutdown
!
ip route 0.0.0.0 0.0.0.0 10.20.20.2
!
ip dhcp-server pool "POOL1"
  network 192.168.62.0 255.255.255.0
  option 66 ascii 192.168.62.1
  option 67 ascii CONFIG-TA916.cfg
!
end
```

Contents of CONFIG-TA916.cfg Configuration File

The following output shows the pertinent information from the **CONFIG-TA916.cfg** configuration file:

```
voice trunk T01 type sip
  sip-server CORPORATE

voice grouped-trunk TOBROADSOFT
  trunk T01
  accept $

voice user 2001
  connect fxs 0/1
  sip-identity 2001 T01 register auth-name JSMITH password
 fRiax&crOus9I#p
!
auto-config
auto-config apply replace
auto-config authname $SYSTEM_SERIAL_NUMBER password fRiax&crOus9I#p
auto-config http-auth basic
auto-config http-auth digest
auto-config method https
```

```
auto-config sip-notify user 2001
!
```

7.3 Zero-Touch Provisioning on a Device Without a Startup Configuration File

In the following example, a NetVanta 3305 is configured as both the DHCP and TFTP server. The NetVanta 1534 is the new device on the network and uses Auto-Config to automatically configure itself with the information provided from the host device (NetVanta 3305). Initially, the NetVanta 1534 must have the startup configuration manually removed. The device is then rebooted and allowed to automatically self-configure.

The connectivity between the two units and the events that occur during the automatic configuration process are shown in Figure 3.

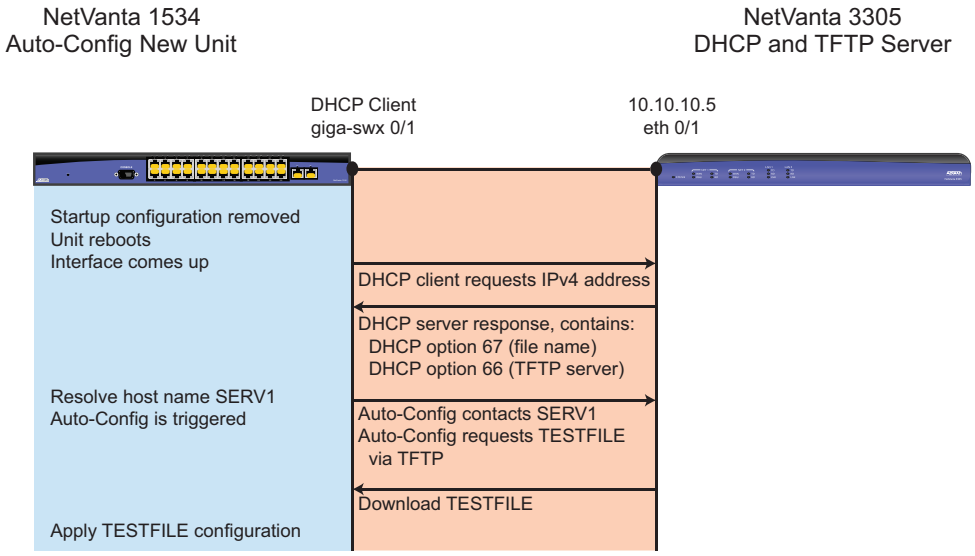

Figure 3. Application Example for Zero-Touch Provisioning

WARNING!
Erasing a startup configuration file will permanently destroy all the data in that file!

The configuration information and the Zero-Touch Provisioning processes for both devices in this scenario are provided below.

NetVanta 1534

The following initial commands are entered on the NetVanta 1534, from the Global Configuration mode prompt, to remove the startup configuration and reboot the device:

```
erase startup-config
Erase startup-configuration? [y or n]y
Startup configuration erased.
(config)#reload
```

NetVanta 3305 Running Configuration

The following output shows the pertinent sections from the running configuration of the NetVanta 3305:

```
show running-config
Building configuration...
!
hostname "Router"
no enable password
!
ip subnet-zero
ip classless
ip domain-proxy
ip host SERV1 10.10.10.5
ip routing
!
ip dhcp-server excluded-address 10.10.10.5
!
ip dhcp-server pool "POOL1"
  network 10.10.10.0 255.255.255.0
  dns-server 10.10.10.5
  netbios-node-type h-node
  default-router 10.10.10.5
  tftp-server SERV1
  bootfile TESTFILE
!
interface eth 0/1
  ip address  10.10.10.5  255.255.255.0
  no shutdown
!
ip tftp server
```

Zero-Touch Provisioning Function on the NetVanta 3305

On the NetVanta 3305, the DHCP pool **POOL1** lists a bootfile option (OPTION 67) called **TESTFILE**. For this example, **TESTFILE** must also reside on the NetVanta 3305 which is shown by the following output from the **show flash** command:

```
show flash
4690344 NV3305A-11-01-00.biz
   1280 startup-config
    119 TESTFILE
4842824 bytes used, 1737400 available, 6580224 total
```

TESTFILE Contents

In our example, the **TESTFILE** consists of commands to create two VLANs, disable Auto-Config, and save the configuration using the **do write** command at the end of the file. When **TESTFILE** is applied to the NetVanta 1534, all of these commands will be executed. The contents of **TESTFILE** are shown in the following example:

```
show file TESTFILE
Using 120 bytes
vlan 100
vlan 101
```

```
exit
no auto-config
do write
```

Zero Touch Provisioning Function on the NetVanta 1534

Once the NetVanta 1534 boots up and discovers that it does not have a startup configuration file, AOS triggers Auto-Config but allows the user 60 seconds to respond to the prompt to cancel the process or continue. There are two valid key responses, press the **Escape** or **Enter** key. (This behavior is described in further detail in “Implementing Auto-Config with Zero-Touch Provisioning” on page 19.) The NetVanta 1534 obtains a DHCP lease with data pertinent to Auto-Config. It resolves the host name **SERV1** into IP address **10.10.10.5**. It then proceeds to download **TESTFILE** from **10.10.10.5**. Once the download is complete, Auto-Config applies the configuration to the device.

After the application of the TESTFILE contents on the NetVanta 1534, the running configuration shows the new settings as follows:

```
show running-config
Building configuration...
!
!
no auto-config
  auto-config server SERV1
  auto-config filename TESTFILE
!
!
vlan 100
  name "VLAN0100"
vlan 101
  name "VLAN0101"
!
end
```

8 Auto-Config Command Summary

The CLI commands used to configure Auto-Config are summarized in Table 3.

Table 3. Auto-Config Configuration Commands

Prompt	Command	Description
(config)#	**auto-config method tftp**	Specifies using TFTP to transfer the configuration file. This is the default file transfer method for Auto-Config.
(config)#	**auto-config method [http | https]** **[port** *<number>***]**	Specifies using HTTP(S) to transfer the configuration file. It is optional to specify a port number. Valid port range is **1** to **65535**.
(config)#	**auto-config server dhcp** **auto-config server dhcp option [66 | 160]**	Specifies using DHCP to automatically learn the configuration server settings. Optionally, if OPTION 66 or 160 are specified, one of these methods is used to define the DHCP server location.
(config)#	**auto-config server** **[***<hostname>* **|** *<ipv4 address>***]**	Specifies the IPv4 address or host name of TFTP server from which to retrieve the Auto-Config parameters.
(config)#	**auto-config authname** *<authname>* **password** *<password>*	Specifies the authentication user name and password to access the host server for the HTTP(S) file transfer. The user name can also be defined using a system variable as detailed in "Step 3: Configure Authentication for HTTP(S) File Transfer (Optional)" on page 14.
(config)#	**auto-config mac-auth mode [http-user-agent | none]**	Specifies the MAC authentication mode for HTTP(S) file transfer. The **http-user-agent** parameter specifies that the MAC address is included in the HTTP User header. The parameter **none** indicates no MAC authentication is used.
(config)#	**auto-config mac-auth address** *<mac address>*	Enables using the MAC address mode for HTTP(S) file transfer authentication and specifies the MAC address. MAC addresses should be expressed in the following format **xx:xx:xx:xx:xx:xx** (for example, **00:A0:C8:00:00:01**). For this command, colons are optional.
(config)#	**auto-config mac-auth interface** *<interface>*	Specifies an interface from which to use the MAC address for HTTP(S) file transfer authentication.
(config)#	**[no] auto-config http-auth [basic | digest]**	Enables the HTTP(S) authentication modes **basic** and/or **digest**, which provide clear text or encrypted text authentication respectively. By default, both are enabled. Use the **no** form of this command to disable the authentication mode.

Table 3. Auto-Config Configuration Commands (Continued)

Prompt	Command	Description
(config)#	**auto-config filename [dhcp| *<name>*]**	Specifies the configuration file name to download. The *<name>* parameter is the file name, which can be defined using system parameters (as explained in "Step 5: Specify the Configuration File Name" on page 16). The **dhcp** parameter specifies using DHCP OPTION 67 to learn the configuration file name. The default setting is **dhcp** which requires DHCP OPTION 67 to be defined on the DHCP server or auto-config will not download a configuration file.
(config)#	**auto-config retry-count** *<number>*	Specifies the maximum number of retries allowed to automatically configure the device. Range is **0** to **1000**. The default is set to **0**, allowing the feature to continuously retry until Auto-Config is disabled.
(config)#	**auto-config apply-config [append | replace]**	Specifies whether to append the existing running configuration or replace the startup configuration with the new configuration settings. The default setting is to **append** to the running configuration.
#	**auto-config restart**	Restarts the Auto-Config process if it has been previously halted. This command is executed from the Enable mode prompt.
(config)#	**[no] auto-config**	Enables the automatic self-configuration feature. Use the **no** form of this command to halt the automatic configuration process once started.
(config)#	**auto-config sip-notify user** *<user>*	Specifies the SIP user to whom SIP NOTIFY (check-sync events) are sent. This is one of the methods that can be used to initiate the Auto-Config process.
(config)#	**auto-config firmware definition-file** *<path and file name>*	Specifies the path and static file name for the firmware definition file to be downloaded.
(config)#	**auto-config firmware destination [flash | cflash]**	Specifies to store the downloaded firmware image on the device's internal flash memory or on the CompactFlash memory.
(config)#	**auto-config firmware download**	Enables the firmware download.
(config)#	**auto-config firmware reload-after** *<seconds>*	Specifies the delay, in seconds, after downloading the new firmware image before the device reboots. The valid range is **60** to **604800**. Use the value **0** to disable the reboot.

Table 3. Auto-Config Configuration Commands (Continued)

Prompt	Command	Description
(config)#	**auto-config firmware replace primary maintain secondary**	Specifies to replace the current primary firmware image with the new image while retaining the existing secondary firmware image, if one exists, and deleting the current primary image.
(config)#	**auto-config firmware replace primary update secondary**	Specifies to replace the current primary firmware image with the new image, while the existing primary firmware image becomes the new secondary image, deleting the existing secondary image.
(config)#	**auto-config firmware replace secondary**	Specifies to replace the existing secondary firmware image with the new image, deleting the existing secondary image, while retaining the current primary image.
(config)#	**auto-config sip-notify reboot always**	Specifies that the device reboot regardless of the configuration, when receiving a SIP NOTIFY message.
(config)#	**auto-config sip-notify reboot on-change**	Specifies that the device reboot only if the configuration on the server has changed, when receiving a SIP NOTIFY message.
(config)#	**auto-config timer polling** *<seconds>*	Specifies the Auto-Config periodic restart interval in seconds. The valid range is **30** to **2592000**.

9 Troubleshooting

There are several **show** and **debug** commands that can be entered from the Enable mode prompt to assist with troubleshooting the Auto-Config feature.

9.1 Show Commands

The following **show** commands can be used to display specific portions of the configuration.

The **show auto-config** command displays the current state of the Auto-Config feature. It displays the current method, current server, file name, last attempt status, number of retries attempted, and reason for the last failure. This output changes depending on the status of the function while it is running.

For example, the command is entered while the Auto-Config function is actively downloading a configuration file:

```
>enable
#show auto-config
Auto-Config is enabled, current status: Downloading.
File transfer method is TFTP
Config Server is 10.10.10.1
Config filename is ADTRAN_CONFIG.cfg
Default filename is [00A0C8AE103A.cfg | adtran_4700254F2.cfg |
 adtran_000000000000.cfg], Current: (Disabled)
Maximum retry count is 0 (repeat indefinitely), total retries is 0
Last failure: HTTP: Could not send initial message to HTTP server
```

The available states displayed by Auto-Config are described in Table 4.

Table 4. Auto-Config Current Status

Current Status	Description
Applying configuration	Auto-Config is in the process of applying new configuration settings from the downloaded configuration file.
Downloading	Auto-Config is in the process of downloading the configuration file.
Download error	An error was experienced during the previous download attempt. Auto-Config is waiting to retry the download attempt.
Download failed	An error was encountered during the previous download attempt and the maximum number of retries has been reached.
Download pending	A download is pending, waiting on a timer.
Idle	When comparing the configuration file with the startup configuration, the files were the same. No further action will be taken.
Success	Auto-Config was successful in downloading the configuration file.

The **show flash** command can be useful to confirm the configuration files that exist on the device prior to creating any new configuration files:

```
>enable
#show flash
5970 startup-config
5710 startup-config.bak
13439188 T9162A-R10-4-M-5-E.biz
13795810 T9162A-R10-5-0-2-E.biz
27611341 bytes used, 4157714 available, 31769055 total
```

CAUTION!
If a file name already exists on a device and an attempt is made to save a new one with the same name, it will overwrite the file with the new contents. This will destroy the old contents. Always confirm the file system prior to saving new configuration files.

The **show running-config auto-config** command shows the Auto-Config settings of the current running configuration:

```
>enable
#show running-config auto-config
Building configuration...
!
!
auto-config
auto-config filename ADTRAN_CONFIG.cfg
auto-config http-auth basic
no auto-config http-auth digest
auto-config server 10.17.220.1
!
End
```

9.2 Debug Commands

The **debug auto-config** command activates debug messages associated with Auto-Config events. Debug messages are displayed in real time. Use the **no** form of this command to disable the debug messages.

WARNING!
Turning on a large amount of debug information can adversely affect the performance of your device.

The **debug auto-config** command displays the Auto-Config processes as they occur and is an excellent tool for assisting with troubleshooting this feature. The following sample output displays that the Auto-Config feature is started:

```
>enable
#debug auto-config
1970.01.01 12:12:05 AUTOCONFIG.STATUS Beginning
1970.01.01 12:12:05 AUTOCONFIG.TIMER Loading timer with 500 milliseconds
#
1970.01.01 12:12:05 AUTOCONFIG Started. To halt enter config-mode and
 type "no auto-config".
1970.01.01 12:12:05 AUTOCONFIG.STATUS Pending
1970.01.01 12:12:05 AUTOCONFIG.TIMER Loading timer with 40 seconds
```

The following additional sample output from the **debug auto-config** command displays that the initial settings have been applied and the first configuration file (**TA916_BOOTSTRAP.cfg**) is downloaded. Once the **TA916_BOOTSTRAP.cfg** file is applied, Auto-Config is restarted (due to the bootstrap configuration file configuration).

```
>enable
#debug auto-config
1970.01.01 12:12:45 AUTOCONFIG.STATUS Download: TA916_BOOTSTRAP.CFG from
 10.17.220.1
1970.01.01 12:12:45 AUTOCONFIG.TIMER Loading timer with 1 seconds
1970.01.01 12:12:46 AUTOCONFIG.STATUS Applying Configuration
1970.01.01 12:12:47 AUTOCONFIG.TIMER Loading timer with 500 milliseconds
1970.01.01 12:12:47 AUTOCONFIG.STATUS Done
1970.01.01 12:12:47 AUTOCONFIG.TIMER Loading timer with 500 milliseconds
1970.01.01 12:12:47 AUTOCONFIG Done. File: TA916_BOOTSTRAP.CFG applied
 to running-config.
1970.01.01 12:12:47 AUTOCONFIG.STATUS Beginning
1970.01.01 12:12:47 AUTOCONFIG.TIMER Loading timer with 500 milliseconds
1970.01.01 12:12:47 AUTOCONFIG Delayed Restart from event config entry
1970.01.01 12:12:48 AUTOCONFIG Started. To halt enter config-mode and
 type "no auto-config".
```

The following additional sample output from the **debug auto-config** command displays the new Auto-Config settings (applied from the **TA916_BOOTSTRAP.CFG** file) are executed:

```
>enable
#debug auto-config
1970.01.01 12:12:48 AUTOCONFIG.STATUS Pending
1970.01.01 12:12:48 AUTOCONFIG.TIMER Loading timer with 20 seconds
1970.01.01 12:13:08 AUTOCONFIG.STATUS Download: AUTO_CONFIG_FINAL.CFG
 from 10.17.220.1
1970.01.01 12:13:08 AUTOCONFIG.TIMER Loading timer with 1 seconds
1970.01.01 12:13:09 AUTOCONFIG.STATUS Applying Configuration
1970.01.01 12:13:09 AUTOCONFIG.STATUS Done
1970.01.01 12:13:09 AUTOCONFIG.TIMER Loading timer with 500 milliseconds
1970.01.01 12:13:10 AUTOCONFIG Done. File: AUTO_CONFIG_FINAL.CFG applied
 to running-config.
```

The **debug http client** command activates debug messages associated with HTTP client operation in AOS. This **debug** command is useful only when using HTTP(S) to transfer the configuration files. The output displays the commands being sent to the server. In the following example, the server could not be reached:

```
>enable
#debug http client
13:07:04 HTTP_CLIENT GET string:
GET /ADTRAN_CONFIG.cfg HTTP/1.1
Authorization: Basic YWR0cmFuOmFkdHJhbg==
Connection: close
Host: 10.10.10.1
User-Agent: TA916/Total Access 916 (2nd Gen)

13:07:04 HTTP_CLIENT Resolved hostname 10.10.10.1 to 10.10.10.1
13:07:04 HTTP_CLIENT Connecting to service at 10.10.10.1:80
```

```
1970.01.01 13:07:24 HTTP_CLIENT Timeout connecting to service at
 10.10.10.1
```

The **debug ip tftp client packets** command activates debug messages associated with TFTP client packets. This debug command is useful only when using a TFTP server to retrieve configuration files. The output displays the commands being sent to the server. In the following example, the file was successfully transferred:

```
>enable
#debug ip tftp client packets
1970.01.01 13:17:37 TFTP.CLIENT TX Read Request (retry 0) to
 ::FFFF:10.17.220.1 for file "ADTRAN_CONFIG.cfg"
1970.01.01 13:17:37 TFTP.CLIENT RX block 1 from ::FFFF:10.17.220.1:62775
1970.01.01 13:17:37 TFTP.CLIENT TX ACK for block 1 (retry 0) to
 ::FFFF:10.17.220.1:62775
1970.01.01 13:17:37 TFTP.CLIENT Received "ADTRAN_CONFIG.cfg" from
 ::FFFF:10.17.220.1:62775 successfully. Saved as local file "auto-
 config-download".

1970.01.01 13:17:39 AUTOCONFIG Done. File: ADTRAN_CONFIG.cfg applied to
 running-config.
```

10 Creating Configuration Files in AOS

A configuration file is an ASCII text file that contains valid AOS commands. For the Auto-Config feature, these files are usually short and can be created using any text editor program. Alternatively, you can create a configuration file on an AOS device directly, especially if the device is a TFTP server used by Auto-Config hosts. This is the method used for this example.

This following steps outline how to create a configuration file named **TESTFILE** on an AOS device.

1. Verify that there is not a file named **TESTFILE** already on the device's file system using the **show flash** command from the Enable mode prompt.

```
#show flash
5970 startup-config
5710 startup-config.bak
13439188 T9162A-R10-4-M-5-E.biz
13795810 T9162A-R10-5-0-2-E.biz
27611341 bytes used, 4157714 available, 31769055 total
```

2. Since a file with this name does not exist on the file system, it is safe to create one. Using the **copy console** *<file name>* command at the Enable mode prompt, create the file and use AOS to compose the contents. After each command is composed, press the **Enter** key. While in this mode, the **Backspace** key deletes a character and moves the cursor back one space. However, editing is done line by line so AOS does not allow the user to edit to a previous line once **Enter** is pressed. When finished entering the contents of the configuration file, enter **Ctrl-D**.

```
#copy console TESTFILE
Enter text to be saved to "TESTFILE".
 Type CTRL+D to finish.
! This is a comment. Comments are not processed
!
interface ethernet 0/2
  no shutdown
```

```
  exit
!
ip tftp server
  enable password qwerty
  banner motd !

This is the message of the day

!
do write
<Ctrl-D>
```

3. Verify that the file was created on the file system using the **show flash** command from the Enable mode prompt.

```
#show flash
186 TESTFILE
5970 startup-config
5710 startup-config.bak
13439188 T9162A-R10-4-M-5-E.biz
13795810 T9162A-R10-5-0-2-E.biz
27611527 bytes used, 4157528 available, 31769055 total
```

4. To display the contents of the file, use the **show file** *<file name>* command.

```
#show file TESTFILE
Using 187 bytes

! This is a comment. Comments are not processed
!
interface ethernet 0/2
  no shutdown
  exit
!
ip tftp server
  enable password qwerty
  banner motd !

This is the message of the day

!
do write
```

11 Warranty and Contact Information

11.1 Warranty

Warranty information can be found at:

www.adtran.com/warranty.

11.2 Contact Information

For all customer support inquiries, please contact ADTRAN Customer Care:

Contact	Support	Contact Information
Customer Care	From within the U.S. From outside the U.S. **Technical Support:** ■ Web: **Training:** ■ Email: ■ Web:	1.888.4ADTRAN (1.888.423.8726) + 1.256.963.8716 www.adtran.com/support training@adtran.com www.adtran.com/training www.adtranuniversity.com
Sales	Pricing and Availability	1.800.827.0807