

Access-Points

- Flashing Cisco AP to autonomous mode
- Access-Point Configuration

Flashing Cisco AP to autonomous mode

Prerequisites

- USB to serial converter
- Installation of Tera Term
- Cisco IOS firmware file (Requires log-in) (More firmwares here (public. dead link :(you're on your own))

Flashing

Boot the AP to recovery mode and get root access

1. Plug in the USB to serial converter to the PC and the AP.
2. Run Tera Term and open the appropriate COM port
3. Hold reset/mode for 20 seconds or until the LED turns red. Release.
4. You should now see a prompt which looks like `ap:` .
5. Run the following commands:

```
del flash:private-multiple-fs
```

```
del flash:env_vars
```

This will reset the AP to factory defaults

6. Type `reset` and answer yes to reboot the AP to regular system

Remove previous firmware

When the AP has booted to its current firmware you can type the default username `Cisco` and password `Cisco`. After logging in type `enable` to get a proper shell. Once again the password is `Cisco`.

To set up the shell to allow debug commands run the following:

```
debug capwap console cli
debug capwap client no-reload
```

To erase the filesystem and completely reset the firmware, type the following command

```
erase flash:
```

This will take around 5 minutes to complete, and the AP might spit out log messages sporadically.

Afterwards restart the AP. It will boot to recovery mode, because there is no firmware.

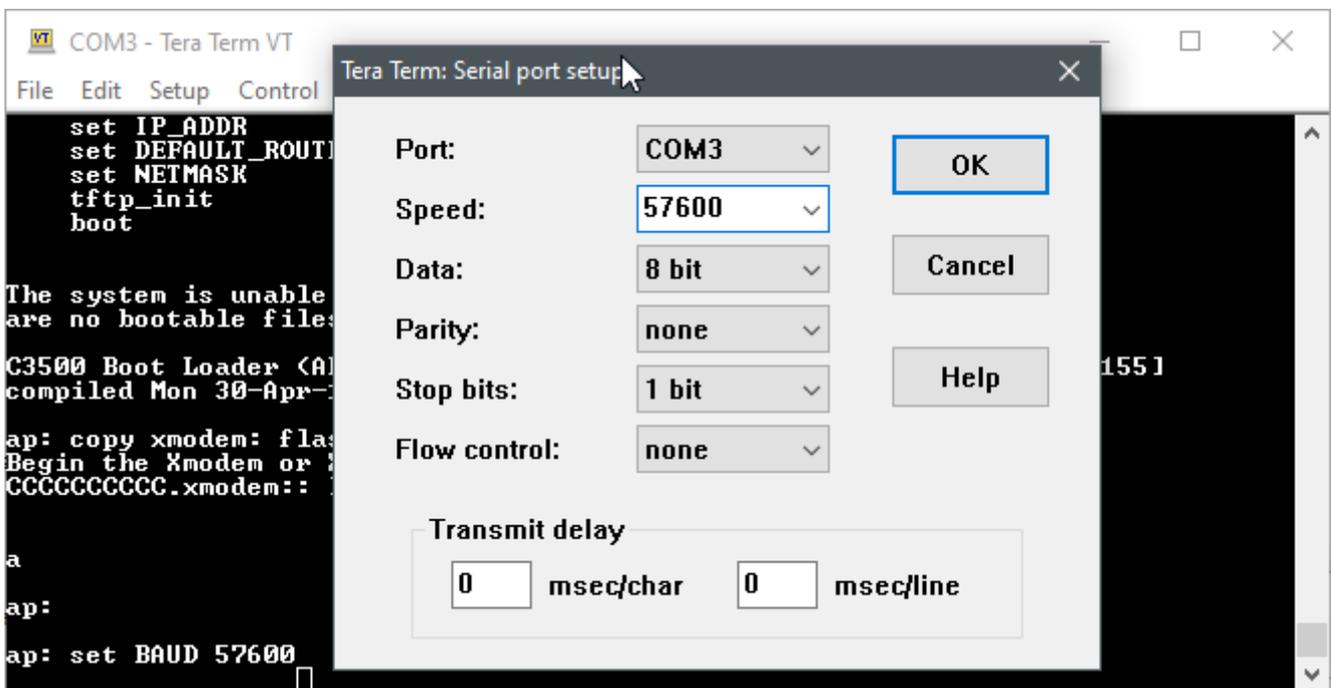
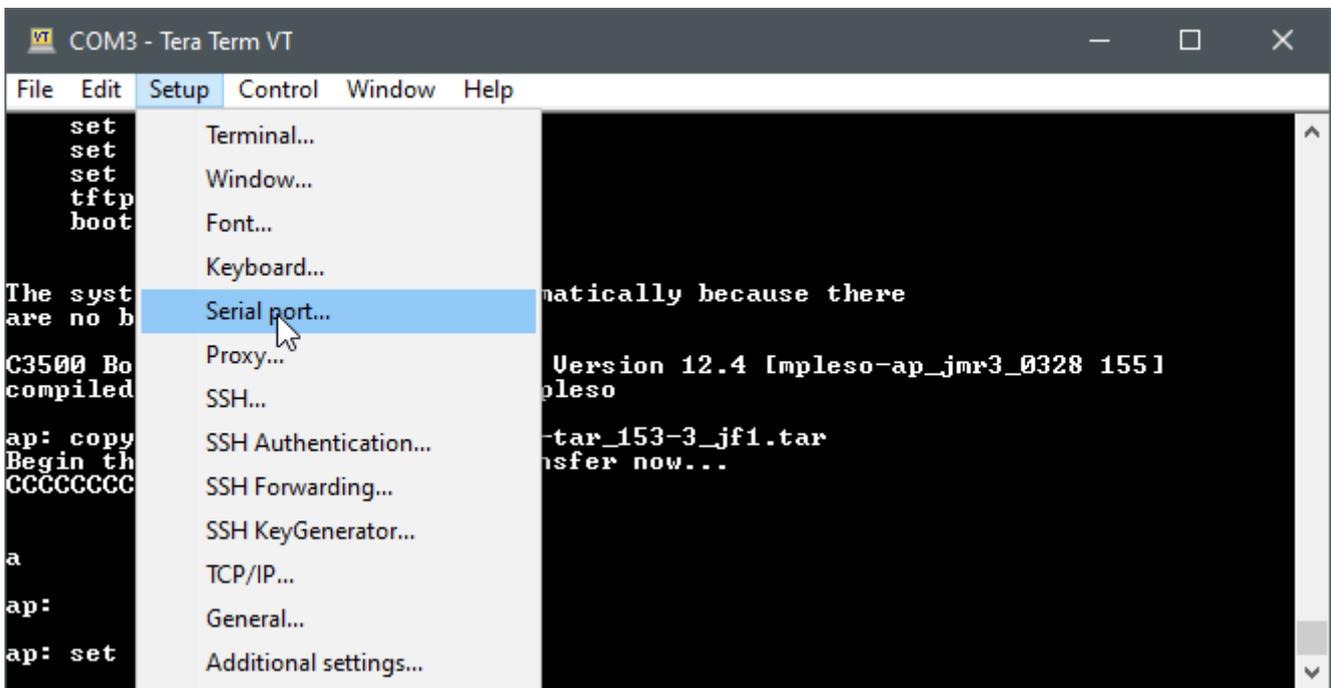
Flash the new firmware

Transfer file from PC to AP

First, to speed up the transfer you need to set a higher speed on the COM port.

```
set BAUD 57600
```

In Tera-Term set the speed on the COM port.

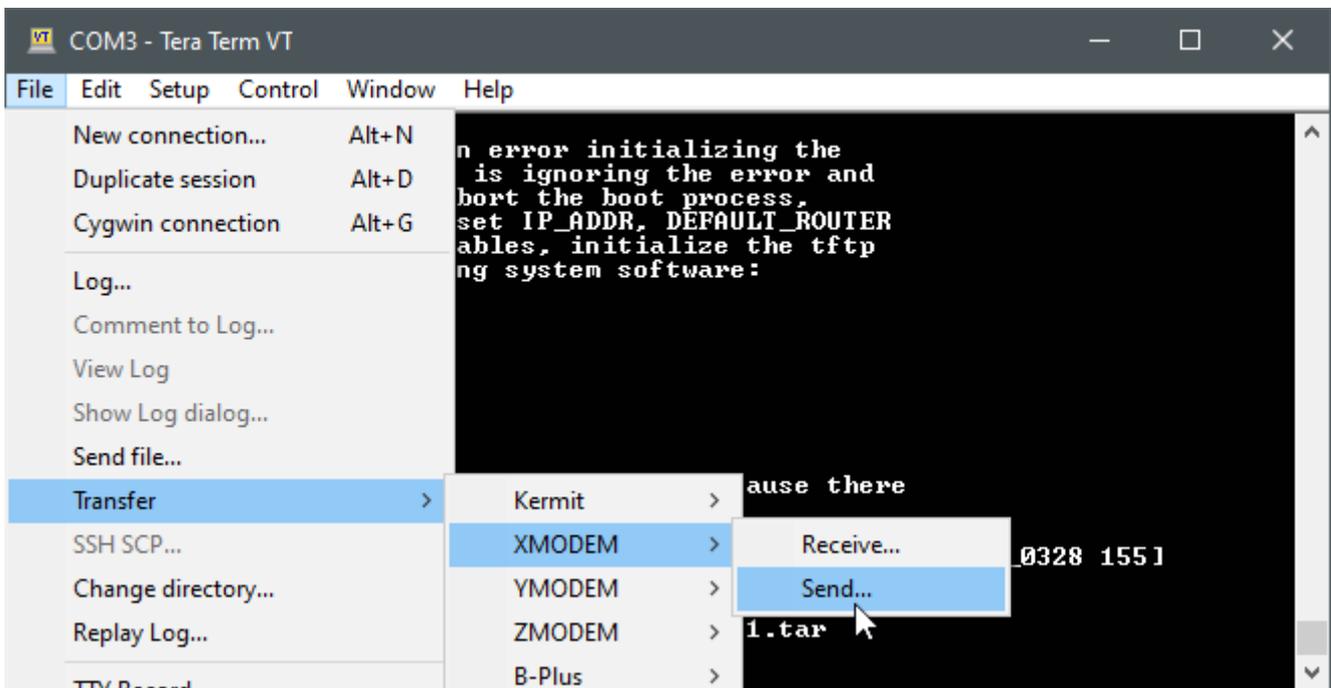


Type the following command:

```
copy xmodem: flash: ap3g1-k9w7- tar_153-3_jf1. tar
```

If you use a different firmware file, change the filename.

In Tera Term open the following menu:



and select your firmware file. You can check the 1K transfer option for a slight additional speedup. This will take a long time.

When the transfer is complete, set the speed back to 9600 using the instructions above with 9600 instead of 57600.

Extracting(/installing) the firmware file

Type the following command to extract the firmware file.

```
tar -xtract flash: ap3g1-k9w7- tar_153-3_jf1. tar flash:
```

If you use a different firmware file, change the filename.

After extraction has finished you can reboot the AP with command `reset`.

After reboot has completed you will see a message like:

```
*Mar 1 00: 00: 32. 976: %DHCP-6- ADDRESS_ASSIGN: Interface BVI1 assigned DHCP address  
128. 39. 204. 157, mask 255. 255. 252. 0, hostname ap
```

You can enter the assigned IP address in your web browser to access the web interface. The default username is `Cisco` with password `Cisco`.

Access-Point Configuration

To access the web interface go to the IP address that was assigned to the access point in your web browser.

Creating an SSID

Go to Security > SSID Manager

The screenshot displays the 'Security: Global SSID Manager' web interface. The main section is titled 'SSID Properties' and contains the following configuration fields:

- Current SSID List:** A dropdown menu with '< NEW >' and 'test' (selected).
- SSID:** A text input field containing 'test'.
- VLAN:** A dropdown menu set to '< NONE >' with a 'Define VLANs' link.
- Backup 1, 2, 3:** Three empty text input fields.
- Band-Select:** A checkbox labeled 'Band Select' which is unchecked.
- Universal Admin Mode:** A checkbox which is checked.
- Interface:** Two checked radio buttons: 'Radio0-802.11N 2.4GHz' and 'Radio1-802.11N 5GHz'.
- Network ID:** A text input field with '(0-4096)' next to it.
- Delete:** A button located at the bottom left of the SSID Properties section.

The lower section is titled 'Client Authentication Settings' and includes:

- Methods Accepted:** Four checkboxes: 'Open Authentication' (checked), 'Web Authentication', 'Shared Authentication', and 'Network EAP'. Each has a corresponding dropdown menu set to '< NO ADDITION >'.
- Server Priorities:** Two columns of settings for 'EAP Authentication Servers' and 'MAC Authentication Servers'. Each column has a radio button for 'Use Defaults' (unchecked) and 'Customize' (checked). Below each are three priority dropdown menus, all set to '< NONE >'.

These settings will create an SSID with no password called "test".

To broadcast the SSID, you must enable Guest Mode further below.

You must also enable the appropriate radios over at network interfaces configuration and set the role in network as Root bridge for mesh (guest nodes should be set to non-root bridge) or access

point for basic access point.

CLI

IP configuration

Enter privileged mode by typing `enable`.

```
AP#conf t //Configure from terminal
AP(config)#int bvl 1 //Configure bridge-virtual-interface number 1
AP(config-if)# ip address <IP> <subnetmask>
AP(config-if)# exit
AP(config)#ip route 0.0.0.0 0.0.0.0 <IP GW>
```

You can also type `ip address dhcp` for DHCP based IP.

Show IP address

Enter privileged mode by typing `enable`.

```
show ip interface
```

Check signal strength

Enter privileged mode by typing `enable`.

```
dot11 Dot11Radio 0/1 linktest
```

0 = 2.4ghz

1 = 5ghz