

(BootROM) طقف ءءارقلا ءركاذ نم ءاذحلل ءحص نم ققحتلال موقى

(uBoot) ىملاعال دىهمتلال ءحص نم ققحتلالاب Booton موقى

OS ءروص ءحص نم ققحتلالاب Uboot موقى

لصتاف ،اذه ثدح اذل .دىهمتلال نم زاهجال عنمىس ف ،لطف ءودح "نمآلا دىهمتلال" فشتك اذل
بجى ىتلا ءىلاتلا تاوطخلل دىدحتل (TAC) ءىنقتلا ءءاسملا زكرمب وأ Cisco كىرشب
إنه رقناف ،Cisco كىرش ىلع روثلل ىل ءءاب تنك اذل .ءلاجل هذه ىف ءءابتا

نمآلا دىهمتلل Syslog لوكوتورب

ءنمآلا دىهمتلال تامولعم ءءابطب ماظنلل موقىس ،لىغشلال ءدب ءانثأ

(eFuse) ىئابرهك مامص ءب دجوى ال ىتلا ءزهجال ىف - نمآلا دىهمتلال لىطعت/نكىمت
ل SYStem ل اىنللا (CPU) ءىزكرملا ءءلاعملل ءدو لثم ،(System-on-Chip) ءءمرربلل لباق
لىطعت" ىه ءءوبطملا ءخسنلل نوكت ،eFuse ل نمآت ب نىىعت مدع ءلاجل ىف وأ (MSYS)
ىه ءءوبطملا ءخسنلل نوكتس ،"نمآلا دىهمتلال" نىكىمت ءلاجل ىف . "نمآلا دىهمتلال
"نمآلا دىهمتلال نىكىمت"

(ءءصللا نم ققحتلال ءلاجل ءءابطب موقى ،ءمزجل ءحص نم ققحتلالاب BootROM ماىق دعب
(ءلش ف/ءهرىرمت م

(ءءصللا نم ققحتلال ءلاجل ءبطبى هنإف ،Uboot ءحص نم ققحتلالاب Booton موقى نأ دعب
(ءلش ف/ررم

(ءءصللا نم ققحتلال ءلاجل ءبطبى هنإف ،OS ءروص ءحص نم ققحتلالاب Uboot موقى نأ دعب
(ءلش ف/ءهرىرمت م

دىهمتلال ءىلمع فاىل مئىس ،لشلال ءلاجل ىف :ءطءالم

2.4.0.91 رادصلل ،تباثلل ءم انربلل لاثم Secure Boot Output

```
BootROM - 1.73
Booting from NAND flash, Secure modeBootROM: RSA Public key verification PASSED
BootROM: CSK block signature verification PASSED
BootROM: Boot header signature verification PASSED
BootROM: Flash ID verification PASSED
BootROM: Box ID verification PASSED
BootROM: JTAG is enabled
General initialization - Version: 1.0.0
AVS selection from EFUSE disabled (Skip reading EFUSE values)
Overriding default AVS value to: 0x23
Detected Device ID 6811
High speed PHY - Version: 2.0
:** Link is Gen1, check the EP capability
PCIe, Idx 0: Link upgraded to Gen2 based on client capabilities
High speed PHY - Ended Successfully
DDR3 Training Sequence - Ver TIP-1.55.0
DDR3 Training Sequence - Switching XBAR Window to FastPath Window
DDR3 Training Sequence - Ended Successfully
BootROM: Image checksum verification PASSED
BootROM: Boot image signature verification PASSED
efuse secure mode: ON

Aldrin ROS Booton: Oct 29 2017 13:42:52 ver. 2.0

Press x to choose XMODEM...
Booting from NAND flash
verify secure U-Boot pass
Running UBOOT...

U-Boot 2013.01 (Oct 29 2017 - 13:42:35) Marvell version: 2016_T1.0.eng_drop_v10 2.4.24
```

Secure Boot Output ماث ال، تباط ال، جمان ربال لاثم 2.5.0.83:

```
BootROM - 1.73
Booting from NAND flash, Secure modeBootROM: RSA Public key verification PASSED
BootROM: CSK block signature verification PASSED
BootROM: Boot header signature verification PASSED
BootROM: Flash ID verification PASSED

General initialization - Version: 1.0.0
AVS selection from EFUSE disabled (Skip reading EFUSE values)
Overriding default AVS value to: 0x23
Detected Device ID 6811
High speed PHY - Version: 2.0

Init Customer board mvHwsPexConfig: Link is Gen1, check the EP capability
PCIe, Idx 0: Link upgraded to Gen2 based on client capabilities
High speed PHY - Ended Successfully
DDR3 Training Sequence - Ver TIP-1.55.0
DDR3 Training Sequence - Switching XBAR Window to FastPath Window
DDR3 Training Sequence - Ended Successfully
BootROM: Image checksum verification PASSED
BootROM: Boot image signature verification PASSED

Armada38x Booton: Apr 17 2018 21:23:48 ver. 2.1.3
efuse secure mode: ON

Press x to choose XMODEM...
Booting from NAND flash
Verify secure U-Boot pass
Running UBOOT...

U-Boot 2013.01 (Jun 18 2019 - 16:47:25) Marvell version: 2016_T1.0.eng_drop_v10 2.5.18

Loading system/images/active-image ...
Verify ROS secure Image pass, efuse is programmed
Uncompressing Linux... done, booting the kernel.
I2C frequency 100 kHz (Tclk 200 MHz, freq_m 12, freq_n 3)
```

رارقلا

ك.ت.ك.ب.ش ةي امح ي ف دعاسي نأ نكمي فيكون نم آلا ديهم تلاب ةيارد يلع نآلا تحبصأ

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا