

**SP 800-90B Non-Proprietary Public Use
Document
WaveLogic 6 Extreme Encryption Modem
Entropy Source**

Entropy Source Version: 1.0

**Document Version: 1.1
Document Date: 2026-10-14**

Ciena Corporation
7035 Ridge Road
Hanover, MD 21076, USA

Prepared by:
atsec information security corporation
4516 Seton Center Parkway, Suite 250
Austin, TX 78759, USA
www.atsec.com

Table of Contents

1 DESCRIPTION 3

2 SECURITY BOUNDARY 3

3 OPERATING CONDITIONS 4

4 CONFIGURATION SETTINGS 4

5 PHYSICAL SECURITY MECHANISMS 5

6 CONCEPTUAL INTERFACES.....5

7 MIN-ENTROPY RATE 5

8 HEALTH TESTS 5

8.1 CONTINUOUS HEALTH TESTS..... 5

8.1.1 Repetition Count Test (RCT) 5

8.1.2 Adaptive Proportion Test (APT) 5

8.2 STARTUP HEALTH TESTS 6

8.3 ON-DEMAND HEALTH TESTS 6

8.4 ERRORS..... 6

9 MAINTENANCE 6

10 USER VERIFICATION 6

11 VENDOR PERMISSIONS AND RELATIONSHIP 7

1 Description

The information about the entropy source described in this document is contained in Table 1.

Table 1: Entropy source and operational environment information.

Characteristic	Description
Vendor	Ciena Corporation
Entropy source name	WaveLogic 6 Extreme Encryption Modem Entropy Source
Standard, IGs	SP800-90B (2018) IG D.J (2021-11-05) IG D.K (2026-04-16) IG D.O (2021-05-04): N/A
Entropy category	Physical (P)
Entropy source version	1.0
Operational environment	Hardware version: 077-0240-p21 CPU: RISC-V
Embodiment and type	Single-chip hardware

The WaveLogic 6 Extreme Encryption Modem Entropy Source is a physical entropy source in the WaveLogic 6 Extreme Encryption Modem SoC. The noise generation of this entropy source is based upon the principle of free-running ring oscillators (FROs). The noise source was tested under the assumption that its output is non-IID.

2 Security Boundary

The Security Boundary of the entropy source is depicted in Figure 1.

The noise source is composed of 24 Free-Running Oscillators (FROs), the digital sample-and-combine logic, and the associated control logic.

Each FRO is a chain of an odd number of delay (inverter) elements arranged in a ring, producing a free-running square wave. The 24 FROs are deliberately built with different numbers of delay elements so that they oscillate at distinct frequencies, which mitigates frequency injection locking between rings.

The outputs of the 24 FROs are combined by an XOR into a single toggle flip-flop, producing one combined bit per sample instant. Eight of these XOR-combined bits are concatenated to form an 8-bit symbol, which is the unit referred to as a single sample from the noise source for continuous health testing and entropy estimation. The 8-bit samples are the output of the entropy source. There is no conditioning component.

Continuous health tests, implemented in hardware, are composed of the SP 800-90B Repetition Count Test (RCT) and the Adaptive Proportion Test (APT).

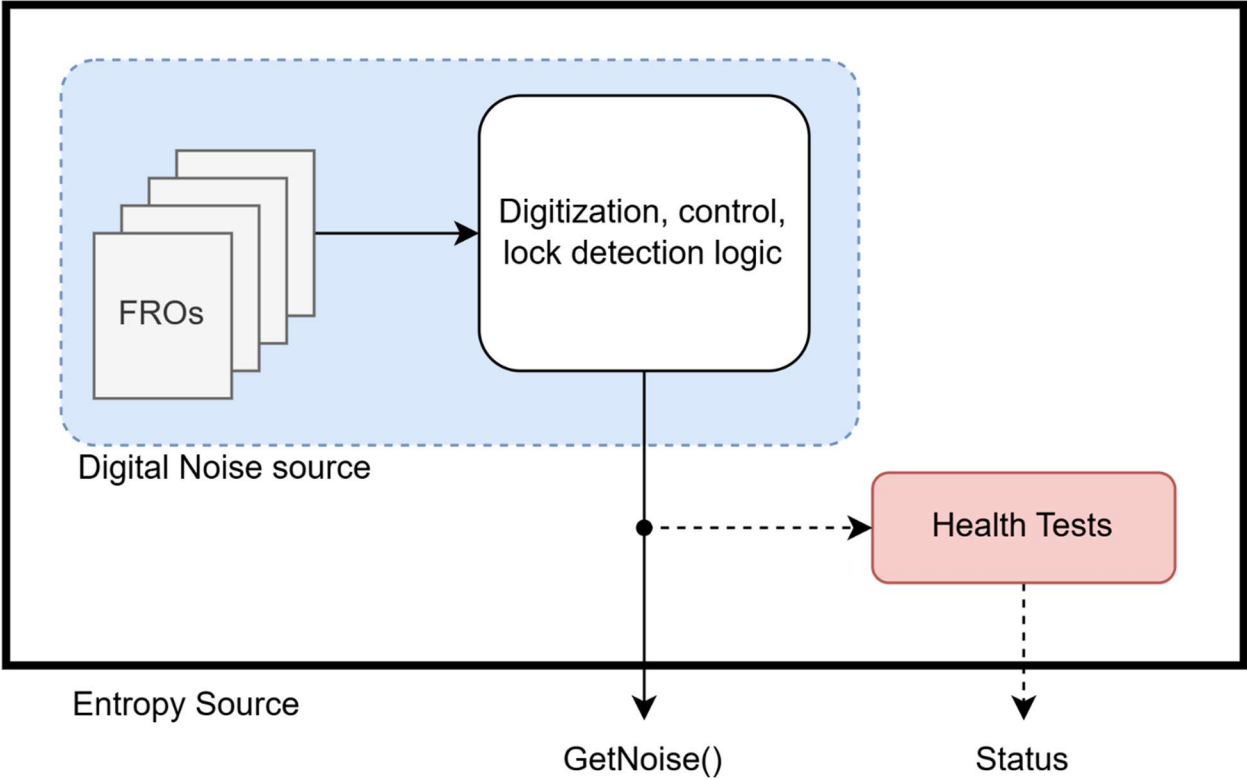


Figure 1: Security boundary.

3 Operating Conditions

The entropy source operating conditions are reflected from the chassis into which the Encryption Modem is installed. Those operating conditions are provided in Table 2:

Table 2: Operating conditions.

Parameter	Value
Operating Temperature Range	5°C to 40°C
Operating relative humidity (Network Equipment Building System (NEBS) standard GR-63-CORE)	5% to 85%
Power supply operating voltage	-40 to -72 Vdc 100 to 240 Vac

4 Configuration Settings

The operator of the entropy source does not have the ability to modify any of the entropy source configuration settings.

5 Physical Security Mechanisms

The entropy source resides within the operational environments identified in Table 1, characterized as single-chip enclosed in an opaque package. The packaging of the chip is production grade and cannot be removed or penetrated without causing serious damage to the chip.

6 Conceptual Interfaces

There are two conceptual interfaces as shown in Figure 1:

- a) GetNoise(): outputs raw noise data.
- b) Status: reports status of health tests (pass or fail).

7 Min-Entropy Rate

The entropy source provides a min-entropy rate of 0.5 bits/bit at its output. The output length is 8 bits.

8 Health Tests

The health tests are performed on the raw noise samples in word-wise (8 bits). The entropy source implements three types of health tests:

- Continuous health tests.
- Startup health tests.
- On-demand health tests.

8.1 Continuous Health Tests

8.1.1 Repetition Count Test (RCT)

The entropy source implements the RCT as specified in SP 800-90B.

The parameters for the health tests are given in Table 3.

Table 3: Parameters for RCT.

Parameter	Value
Cut-off	6

8.1.2 Adaptive Proportion Test (APT)

The entropy source implements the APT as specified in SP 800-90B with two window sizes in parallel: $W = 512$ (the SP 800-90B default for a non-binary source) and $W = 64$ (a shorter window for faster detection of gross failures).

The parameters for the health tests are given in Table 4.

Table 4: Parameters for APT.

Parameter	Value	
	APT-64	APT-512
Window size	64	512
Cut-off	17	62

8.2 Startup Health Tests

The startup health tests are executed automatically after a reset or power-up. During startup, the health test unit collects 1024 samples of raw data and performs the continuous health tests on this data. The collected data samples are available for use if the health tests pass.

8.3 On-Demand Health Tests

The on-demand health tests may be invoked by resetting the entropy source, which will automatically invoke the startup health tests.

8.4 Errors

Errors during health tests are raised from the hardware via an interrupt and then signaled to the consumer via the status interface of the entropy source. In case of error, the entropy source discards any sample that was generated and not yet consumed, and halts production of any new data. The entropy source can be recovered by restarting or rebooting via the operator.

Table 5 lists error codes in the status interface.

Table 5: Error codes from the status interface/register.

Name	Value	Function
Repcnt_fail	1	RCT health test error
Aprop_fail	1	APT health test error

9 Maintenance

There are no maintenance requirements applicable to this entropy source, except that if there is a health test failure event, the entropy source needs to be rebooted.

10 User Verification

To test the entropy source, raw noise data samples consisting of at least 1,000,000 64-bit samples must be collected from GetNoise() interface at normal operating conditions, mapped down to 8-bit samples and processed by the SP 800-90B entropy tool that is provided by NIST.

Restart data must be collected at normal operating conditions through the GetNoise() interface, following the restart procedure specified in SP 800-90B (i.e., 1,000 samples from 1,000 restarts each) and processed by the NIST SP 800-90B entropy tool. The minimum of

the row-wise and column-wise entropy rate must be more than half that of the raw noise entropy rate.

The user of the entropy source can verify the version of this entropy source by visually inspecting the hardware version of the Encryption Modem as indicated in Table 1.

Figure 2 illustrates the hardware and the location of the hardware version.



Figure 2: SoC in which the entropy source is implemented.

11 Vendor Permissions and Relationship

Reuse restricted to vendor.