

(51) International Patent Classification:
H04B 10/00 (2006.01)(21) International Application Number:
PCT/US2010/050908(22) International Filing Date:
30 September 2010 (30.09.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12/578,814 14 October 2009 (14.10.2009) US(71) Applicant (for all designated States except US):
SCHWEITZER ENGINEERING LABORATORIES, INC. [US/US]; 2350 NE Hopkins Court, Pullman, WA 99163 (US).

(72) Inventor; and

(75) Inventor/Applicant (for US only): **HILTON, Andrew** [CA/CA]; #1 1550 Larkhall Crescent, North Vancouver, BC (CA).(74) Agent: **EDGE, Richard, M.**; 2350 NE Hopkins Court, Pullman, WA 99163 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: SYSTEMS AND METHODS FOR A CONFIGURABLE COMMUNICATION DEVICE

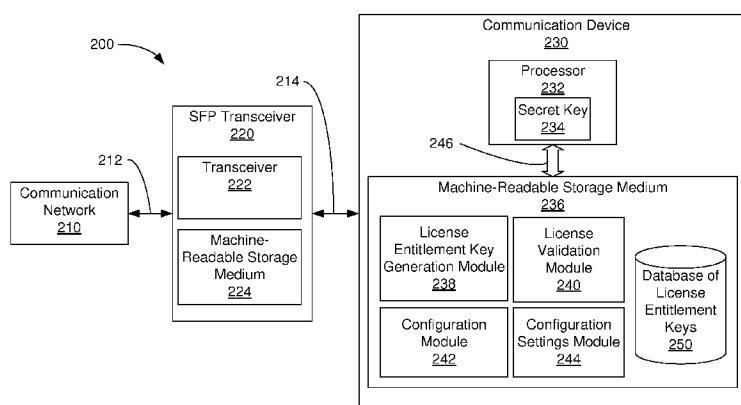


FIG. 2

(57) **Abstract:** The present disclosure relates to systems and methods for configuring a communication device based, at least in part, on a small form-factor pluggable (SFP) transceiver. An SFP transceiver may be utilized in connection with a communication device that transmits data according to a variety of communication protocols. In various embodiments, the configuration may be based upon an SFP configuration value stored in a machine-readable storage medium in the SFP transceiver. In certain embodiments, the SFP configuration value may be an input, together with other values associated with the SFP transceiver and a secret key, to an algorithm for generating a license entitlement key. Certain embodiments may allow for the configuration of a communication device and/or distribution of license entitlement keys in the field.

SYSTEMS AND METHODS FOR A CONFIGURABLE COMMUNICATION DEVICE

Technical Field

- 5 **[0001]** The present disclosure relates to systems and methods for a configurable communication device. More particularly, the present disclosure relates to a communication device that is configurable based, at least in part, upon a small form-factor pluggable transceiver.

Brief Description of the Drawings

- 10 **[0002]** FIG. 1 illustrates a flow chart of one embodiment of a method for configuring a communication device.
- [0003]** FIG. 2 illustrates a functional block diagram of a system including a configurable communication device.
- 15 **[0004]** FIG. 3 illustrates a block diagram of one embodiment of a machine-readable storage medium, which may be comprised within an SFP transceiver.

Detailed Description of Preferred Embodiments

- [0005]** Disclosed herein are systems and methods for configuring a communication device based, at least in part, upon a small form-factor pluggable (SFP) transceiver. An SFP transceiver may be utilized in connection with a communication device that transmits data according to a variety of communication protocols. In various embodiments, the configuration may be based upon an SFP configuration value stored in a machine-readable storage medium in the SFP transceiver. In certain
- 20 embodiments, the SFP configuration value may be an input, together with one or more values associated with the SFP transceiver and a secret key, to an algorithm for generating a license entitlement key. The secret key may be stored in the communication device, and may be stored in such a manner so to not be externally readable. Certain embodiments may allow for the configuration of a communication
- 25 device and/or distribution of license entitlement keys in the field and without the use of a license server, Internet connection, dial-up connection and/or a USB dongle. Such embodiments may advantageously allow for devices to be upgraded and reconfigured in place and may thus reduce downtime and expense associated with the upgrade.
- 30

[0006] In certain embodiments, configuration settings may be tied to a generated license entitlement key. In one embodiment, based on a first value of the generated license entitlement key, a communication device may be configured to operate as an Ethernet switch, while based on a second value of the generated license entitlement key, the communication device may be configured to operate as a multiplexer in a synchronized optical network (SONET). Such embodiments may provide a convenient and transparent system for an end user to upgrade the communication device that combines the task of license management and device configuration. Further, such embodiments may facilitate the process of upgrading from one communication standard to another. In other embodiments, configuration settings may be independent of a license entitlement key. For example, a configuration setting may be stored in a machine-readable storage medium, or may be based upon a detected hardware parameter of an SFP transceiver.

[0007] An SFP transceiver is a hot-pluggable transceiver, which may be used for both telecommunication and data communications applications. SFP transceivers may be configured to interface a communication device (e.g., a switch or a router) to a fiber optic or copper networking cable. SFP transceivers may be designed to support communications according to a variety of communication protocols and standards, including SONET, Ethernet, Fibre Channel, synchronous digital hierarchy (SDH), and the like. An SFP transceiver may also be configured to comply with various standards, including the SFP+ standard and the XFP standard. It will be understood that in any instance where an SFP transceiver is received herein, an SFP+ transceiver or an XFP transceiver may also be utilized.

[0008] An SFP transceiver may comply with a multi-source agreement (MSA), which ensures the interchangeability of SFP transceivers from different vendors. An SFP transceiver may comply with one or more MSAs, including SFP-8472 digital diagnostic monitor interface (DMI). This allows the SFP transceiver to monitor its various signal levels. It also provides information about the configuration of the SFP transceiver. The DMI interface provides access to two databases, namely an A0 database and an A2 database, which can be read via an I2C interface. The A0 database may contain vendor specific information, while the A2 database contains SFP transceiver parameters and user configuration data.

[0009] SFP transceivers are available with a variety of different transmitter and receiver types, allowing users to select the appropriate transceiver for each link to

provide the required optical reach over the available optical fiber type (e.g., multi-mode fiber or single-mode fiber). SFP transceivers are also available with a copper cable interface, allowing a communication device designed primarily for optical fiber communications to also communicate over an unshielded twisted pair networking cable.

5 **[0010]** Several aspects of the embodiments described below will be illustrated as software modules or components. As used herein, a software module or component may include any type of computer instruction or computer executable code located within a memory storage device. A software module or component may, for instance, comprise one or more physical or logical blocks of computer instructions, which may be
10 organized as a routine, program, object, component, data structure, etc., that performs one or more tasks or implements particular abstract data types.

[0011] In certain embodiments, a particular software module or component may comprise disparate instructions stored in different locations of a memory storage device, which together implement the described functionality of the module. Indeed, a
15 module or component may comprise a single instruction or many instructions, and may be distributed over several different code segments, among different programs, and across several memory storage devices. Some embodiments may be practiced in a distributed computing environment where tasks are performed by a remote processing device linked through a communications network. In a distributed computing
20 environment, software modules or components may be located in local and/or remote memory storage devices. In addition, data being tied or rendered together in a database record may be resident in the same memory storage device, or across several memory storage devices, and may be linked together in fields of a record in a database across a network.

25 **[0012]** Embodiments may be provided as a computer program product including a machine-readable storage medium having stored thereon instructions that may be used to program a computer (or other electronic device) to perform processes described herein. The machine-readable storage medium may include, but is not limited to, hard drives, floppy diskettes, optical disks, CD-ROMs, DVD-ROMs, ROMs, RAMs, EPROMs,
30 EEPROMs, magnetic or optical cards, solid-state memory storage devices, or other types of media/machine-readable storage medium suitable for storing electronic instructions.

[0013] Reference in the specification to “one embodiment” or “an embodiment” means that a particular feature, structure, or characteristic described in connection with

the embodiment is included in at least one embodiment. The appearance of the phrase “in one embodiment” in various places in the specification are not necessarily all referring to the same embodiment.

[0014] FIG. 1 illustrates a flow chart of one embodiment of a method 100 for

5 configuring a communication device. At step 110, an SFP transceiver is communicatively coupled with a communication device. The communication device may be of any type of device that is configured to receive an SFP transceiver. For example, the communication device may be configurable as either an Ethernet switch, or a SONET multiplexer. The communication device may also communicate according
10 to different communication protocols. Similarly, the SFP transceiver may be configured to communicate according to a variety of different communication protocols, line rates, link lengths, and transmission media.

[0015] The SFP transceiver may be communicatively coupled to the communication device by way of a communication link. The communication link may comply with the
15 SFP Transceiver Multi-Source Agreement (MSA). An SFP transceiver may also comply with other multi-source agreements, such as XFP, SFP+, and the like.

[0016] In certain embodiments, once the SFP transceiver is in communication with the communication device, the communication device may determine whether the SFP transceiver has a stored license entitlement key (LEK) 120. If a stored LEK exists,
20 method 100 may proceed to step 160. If a stored license entitlement key does not exist, method 100 proceeds to step 130. In other embodiments not relying on a license entitlement key, various steps of method 100, including step 120, may be omitted. In addition, in embodiments not relying on license entitlement keys, steps 140, 150, and 160 may also be omitted. In such embodiments, method 100 for configuring a
25 communication device comprises communicatively coupling an SFP transceiver with the communication device 110, accessing an SFP configuration value 130, and configuring the communication device 170.

[0017] At step 130, an SFP configuration value may be accessed 130. In certain embodiments, an SFP transceiver may include a machine-readable storage medium,
30 which may contain the SFP configuration value. In other embodiments, the SFP configuration value may be tied to a particular hardware value or other value associated with the SFP. In certain embodiments, a unique SFP configuration value may be assigned to each SFP transceiver.

[0018] According to some embodiments, a secret key may be accessed 140 for use in generating the LEK. In certain embodiments, the secret key is included within a processor or a field-programmable gate array (FPGA) in the communication device. Certain processors or FPGAs may include internal values that are not readable external
5 to the processor or FPGA. In certain embodiments, the secret key is stored such that it is not readable external to the processor or FPGA. In this way, the secrecy of the secret key may be enhanced. In other embodiments, the secret key may be stored in other locations and in a variety of forms of machine-readable media. In one embodiment, the secret key may be stored in an encrypted external flash memory, such
10 as the Numonyx Krypto security technologies available from Numonyx B.V., of Rolle, Switzerland.

[0019] Using the secret key and the SFP configuration value, an LEK may be generated and stored 150. In one embodiment, the generated LEK may be the output of a hash algorithm, which utilizes as inputs the SFP configuration value and the secret
15 key. The hash algorithm may include secure hash algorithms (SHA), including SHA-0, SHA-1, SHA-2. In alternative embodiments, other hash functions or data algorithms may be utilized. The output of the hash algorithm may be utilized as a license entitlement key. In various embodiments, further manipulation may be performed on the output of the hash algorithm in order to generate the license entitlement key. Once
20 the license entitlement key has been generated, it may be stored. In certain embodiments, the license entitlement key may be stored in a machine-readable storage medium within the SFP transceiver. In one embodiment, the secret key and the SFP configuration value are used as inputs to an SHA-1 algorithm. The output of the SHA-1 is a 20 byte long value, and constitutes the LEK. The LEK may then be stored into a
25 machine-readable storage medium in the SFP transceiver.

[0020] After generating the LEK, method 100 may then determine whether the generated LEK is valid 160. A variety of techniques may be utilized to validate the LEK. In various embodiments, a database of valid license entitlement keys may be stored in a machine-readable storage medium in the SFP transceiver or stored in a machine-
30 readable storage medium in the communication device. The generated LEK may be compared to the database of valid license entitlement keys. In still other embodiments, a license server, a USB authentication fob, a smart card, or other authentication technique may be employed. If the generated LEK is not found by one of the above-listed techniques, the LEK may be determined to be invalid. Upon determining that the

LEK is not valid, method 100 may disable the communication device 180. In this manner, a measure of security may be introduced to ensure proper licensing.

[0021] At step 170 the communication device may be configured, either based on the SFP configuration value and/or based on a license associated with the generated
5 LEK. For example, a configuration setting may be associated with a particular license, and based on the configuration setting, the communication device may be reconfigured. In one embodiment, the configuration setting may comprise a setting of an FPGA. The configuration setting may cause the FPGA to select from a plurality of configuration files. For example, one configuration file may configure the FPGA to process Ethernet
10 communications, while another configuration file may configure the FPGA to process communications according to a different protocol, such as SONET or SDH. A configuration file may be provided for each of the various communications protocols compatible with an SFP transceiver.

[0022] FIG. 2 illustrates one embodiment of a functional block diagram of a system
15 200 for configuring a communication device. As illustrated in FIG. 2, a communication network 210 is in communication with an SFP transceiver 220 via a communication link 212. A transceiver 222 may be configured to send and receive data via communication link 212 to communication network 210. Communication link 212 may include a variety of transmission media, including fiber optic or electrical cable. SFP transceiver 220
20 may be configured to communicate with communication network 210 in a variety of protocols and line speeds, including SONET (e.g., OC-1, OC-3, OC-12, OC-24, OC-48, OC 192), SDH (e.g., STM-1, STM-4, STM-16 and STM-64), and Ethernet (e.g., 100BASE-T, 100BASE-FX, 100BASE-SX, 100BASE-BX, 1000BASE-X, 1000BASE-T, and 1000BASE-CX).

[0023] SFP transceiver 220 includes a machine-readable storage medium 224. As illustrated in greater detail in FIG. 3 and discussed in greater detail below, machine-readable storage medium 224 may include a variety of types of information, including an SFP configuration value, and other types of information, such as a serial number, an identifier of a manufacturer, information regarding the type of the SFP transceiver, and
30 the like. SFP transceiver 220 may be communicatively coupled via an SFP transceiver communication link 214 to a communication device 230. Link 214 may comprise an I2C interface. Each of communication device 230 and SFP transceiver 220 may comprise a port or an interface to create link 214.

[0024] SFP transceiver 220 is in communication with communication device 230 by way of an SFP communication link 214. Communication device 230 may include a processor 232. Processor 232 may operate using any number of processing rates, architectures, and may be embodied as a general purpose processor, an application specific processor, a field-programmable gate array, or other programmable device. Processor 232 may be configured to perform various algorithms and calculations described herein. In certain embodiments, including the illustrated embodiment of FIG. 2, a secret key 234 is stored within processor 232. In certain embodiments, secret key 234 may not be readable outside of processor 232, and accordingly, the secrecy of secret key 234 may be enhanced. Certain FPGA devices may allow for such secret values to be maintained within the FPGA. In other embodiments, secret key 234 may be stored in other locations.

[0025] A data bus 246 may provide a communication link between processor 232 and a machine-readable storage medium 236. Machine-readable storage medium 236 may be implemented using a variety of technologies, including hard drives, floppy diskettes, RAM, solid-state memory storage devices, and other storage media suitable for storing electronic instructions and other data. Certain embodiments may be provided as a computer program product including a machine-readable storage medium having stored instructions thereon that may be used to program a computer (or other electronic device) to perform processes described herein.

[0026] Machine-readable storage medium 236 may be the repository of software modules or other machine-readable instructions that are executable by processor 232. In particular, machine-readable storage medium 236 may store a license entitlement key generation module 238, a license validation module 240, a configuration module 242, configuration settings module 244, and a database of license entitlement keys 250.

[0027] License entitlement key generation module 238 may perform a method for generating a license entitlement key. In one embodiment, license entitlement key generation module 238 comprises a secure hash algorithm, which may utilize values stored in machine-readable storage medium 224 and secret key 234 to generate an output digest.

[0028] License validation module 240 may be operable to validate the license entitlement key generated by license entitlement key generation module 238. In one embodiment, a valid license entitlement key (not shown) is maintained in machine-

readable storage medium 224. In certain embodiments, machine-readable storage medium 224 comprises only a single valid license entitlement key, which is specific to SFP transceiver 220. The license entitlement key generated by license entitlement key generation module 238 may be compared to the valid license entitlement key stored in machine-readable medium 224 in order to assess the validity of the generated license entitlement key.

[0029] In other embodiments, license validation module 240 may be configured to operate in conjunction with a database of license entitlement keys 250 stored on machine-readable storage medium 236. In some embodiments, database of license entitlement keys 250 may be encrypted so as to protect against unauthorized access to the database of license entitlement keys 250. In alternative embodiments, database of license entitlement keys 250 may be remote to communication device 230, and various techniques may be utilized to validate a license entitlement key (e.g., a license server, a USB authentication fob, a smart card, and the like).

[0030] Configuration module 242 may configure communication device 230 based upon the SFP configuration value and/or the license corresponding to a valid license entitlement key. Various configuration settings may be stored in configuration settings module 244. In one embodiment, the configuration setting may comprise one or more settings of an FPGA, in embodiments where processor 232 comprises an FPGA. For example, the configuration setting may cause the FPGA to select from a plurality of configuration files, which may be stored in configuration settings module 244. One configuration file may configure the FPGA in a mode to process Ethernet communications, while another configuration file may configure the FPGA in another mode to process communications according to a different protocol, such as SONET.

[0031] FIG. 3 illustrates one embodiment of machine-readable storage medium 224, which may be comprised within an SFP transceiver. Machine-readable storage medium 224 comprises two databases, an A0 database 310, and an A2 database 330. Various data may be stored in A0 database 310, including a vendor name 312, a serial number 314, a transceiver wavelength 316, a manufacturer identification 318, and a line rate 320. In certain embodiments, A0 database 310 may comprise read-only memory. A2 database 330 may comprise both read and write accessible memory and read-only memory. In a memory location for calibration data 332, various data may be recorded relating to the calibration of the SFP transceiver.

[0032] An SFP configuration value 336, a generated license entitlement key value 338, and a valid license entitlement key value 340 may be stored in a memory location for user configuration information 334. In certain embodiments, the SFP configuration value 336 and/or the valid license entitlement key value 340 may be stored in read-only memory.

[0033] As discussed in connection with FIGS. 1 and 2, above, SFP configuration value 336 may be utilized to select a configuration setting or may be a value that is utilized as an input to an algorithm for generating a license entitlement key. Similarly, various values from A0 database 310 may also be used as inputs to the configuration setting or to the algorithm for generating a license entitlement key. The generated license entitlement key value may be compared to the valid license entitlement key value 340 in order to validate the generated license entitlement key. Once generated, a license entitlement key may be stored in the memory location for a generated license entitlement key value 338. By storing a generated license entitlement key, a system can validate the license entitlement key when the system is activated without requiring that the license entitlement key be generated again.

[0034] It will be obvious to those having skill in the art that many changes may be made to the details of the above-described embodiments without departing from the underlying principles of the present disclosure. The scope of the present invention should, therefore, be determined only by the following claims.

Claims

1. A configurable communication system comprising:
a small form-factor pluggable (SFP) transceiver comprising,
an SFP configuration value,
5 a device communication port, and
a network communication port configured to communicatively couple the
SFP transceiver to a network; and
a communication device configurable in at least one of a first mode and a
second mode, the communication device comprising,
10 a processor,
an SFP transceiver interface configured to communicatively couple
the SFP transceiver to the communication device,
a first machine-readable storage medium comprising,
a configuration module executable by the processor, the
15 configuration module configured to select a configuration setting
based at least in part on the SFP configuration value;
wherein upon communicatively coupling the SFP transceiver to the
communication device, the configuration module configures the communication device
in one of the first mode and the second mode, and
20 wherein the communication device is configured in the first mode to process
communications received via the network communication port according to a first
communications protocol and is configured in the second mode to process
communications received via the network communication port according to a second
communications protocol.
25
2. The system of claim 1, wherein the first communications protocol
comprises Ethernet, and the second communications protocol comprises at least one of
synchronized optical networking (SONET) and synchronous digital hierarchy (SDH).
- 30 3. The system of claim 1, wherein the network communications port is
configured to communicate using at least one of 100BASE-T, 100BASE-FX, 100BASE-
SX, 100BASE-BX, 1000BASE-X, 1000BASE-T, and 1000BASE-CX.

4. The system of claim 1, wherein the network communications port is configured to communicate using at least one of OC-1, OC-3, OC-12, OC-24, OC-48, OC 192, STM-1, STM-4, STM-16 and STM-64.

5 5. The system of claim 1, wherein the processor comprises a field-programmable gate array (FPGA), and wherein the configuration setting comprises a setting of the FPGA.

10 6. The system of claim 5, wherein the configuration setting in the first mode configures the FPGA to process Ethernet communications, and the configuration setting in a second mode configures the FPGA to process synchronized optical network communications.

15 7. The system of claim 5, wherein the FPGA further comprises a secret key; and
wherein the first machine-readable medium further comprises:
a license entitlement key generation module executable on the processor
and configured to generate a license entitlement key based on the SFP
configuration value and the secret key, and
20 wherein the configuration setting is further based upon the generated license entitlement key.

25 8. The system of claim 1, wherein the SFP transceiver comprises a second machine-readable storage medium, and wherein the SFP configuration value comprises a value stored on the second machine-readable storage medium.

9. The system of claim 8, wherein the value stored on the second machine-readable storage medium comprises at least one of an identifier of a manufacturer of the SFP transceiver and a serial number of the SFP transceiver.

30 10. The system of claim 1, wherein the configuration value comprises a hardware value of the SFP transceiver.

11. The system of claim 1, wherein the SFP transceiver communication interface comprises an I2C interface.

12. The system of claim 1, wherein the communication device is configured to operate as an Ethernet switch in the first mode and is configured to operate as a SONET multiplexor in the second mode.

13. A method for configuring a communication device, the method comprising:

10 communicatively coupling a small form-factor pluggable (SFP) transceiver with a communication device, the SFP transceiver comprising a network communication port configured to communicatively couple the SFP transceiver to a network;
accessing an SFP configuration value stored on the SFP transceiver;
selecting a configuration setting based at least in part on the SFP configuration
15 value;
configuring the communication device based on the configuration setting in one of the first mode and the second mode; and
processing communications received via the network communication port according to a first communications protocol in the first mode and according to a
20 second communications protocol in the second mode.

14. The method of claim 13, wherein the first communications protocol comprises Ethernet, and the second communications protocol comprises at least one of synchronized optical networking (SONET) and synchronous digital hierarchy (SDH).
25

15. The method of claim 13, wherein the configuration setting comprises a setting of a field-programmable gate array (FPGA).

16. The method of claim 15, wherein configuring the communication device
30 comprises selecting code executable on the FPGA based at least in part on the SFP configuration value.

17. The method of claim 13, further comprising generating a license entitlement key using the SFP configuration value; and
configuring the communication device based upon the generated license entitlement key.

5

18. The method of claim 13, further comprising configuring the communication device to operate as a synchronized optical network multiplexer in the first mode.

10

19. The method of claim 13, further comprising configuring the communication device to operate as an Ethernet switch in the second mode.

15

20. A communication device configured to receive a small form-factor pluggable (SFP) transceiver, the SFP transceiver comprising an SFP configuration value, the communication device comprising:

a processor;

an SFP transceiver interface configured to communicatively couple the SFP transceiver to the communication device; and

a first machine-readable storage medium comprising,

20

a configuration module executable by the processor, the configuration module configured to select a configuration setting based at least in part on the SFP configuration value,

25

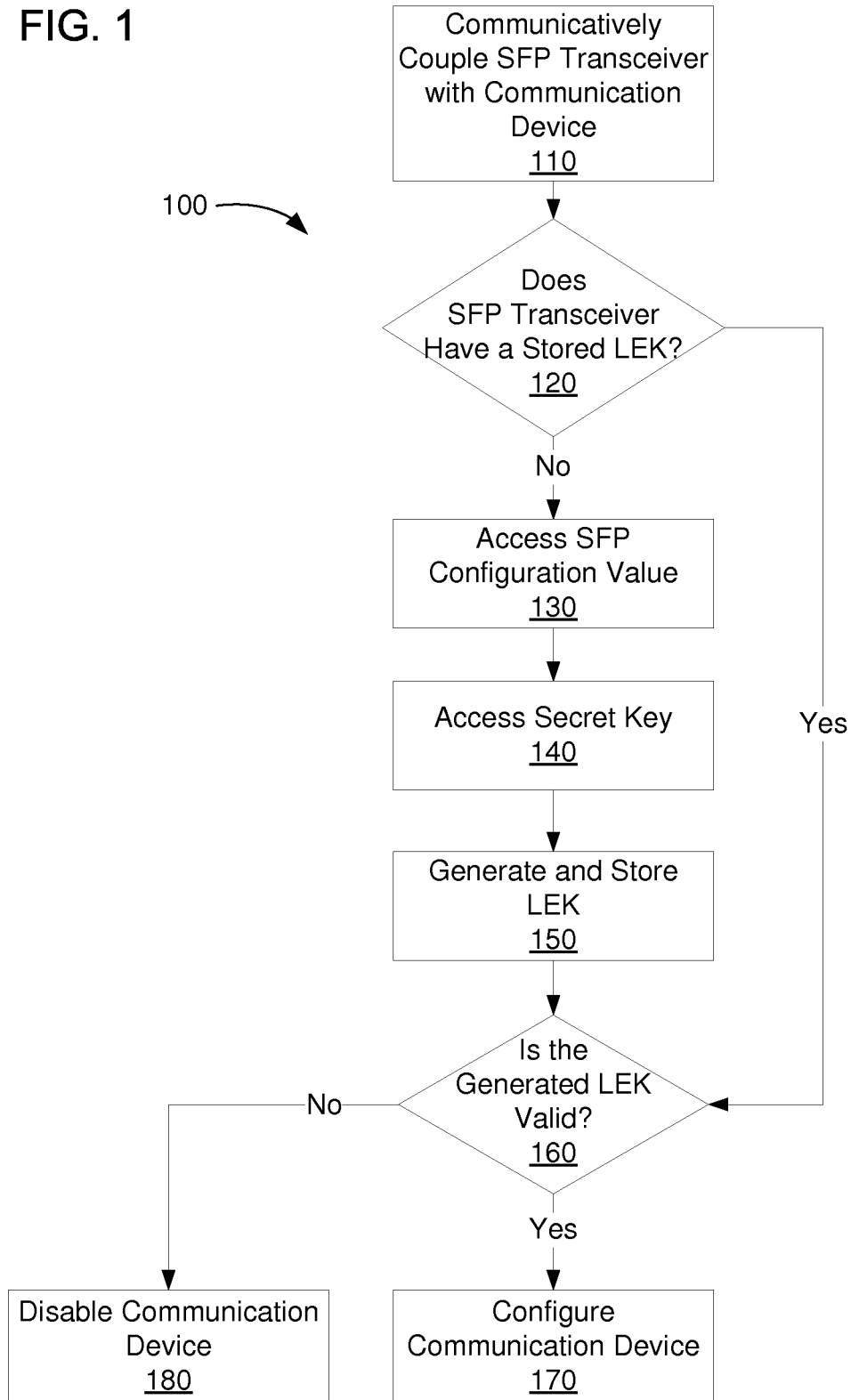
wherein upon communicatively coupling the SFP transceiver to the communication device, the configuration module configures the communication device in one of the first mode and the second mode, and

30

wherein the communication device is configured in the first mode to process communications received via the network communication port according to a first communications protocol and is configured in the second mode to process communications received via the network communication port according to a second communications protocol.

1/3

FIG. 1



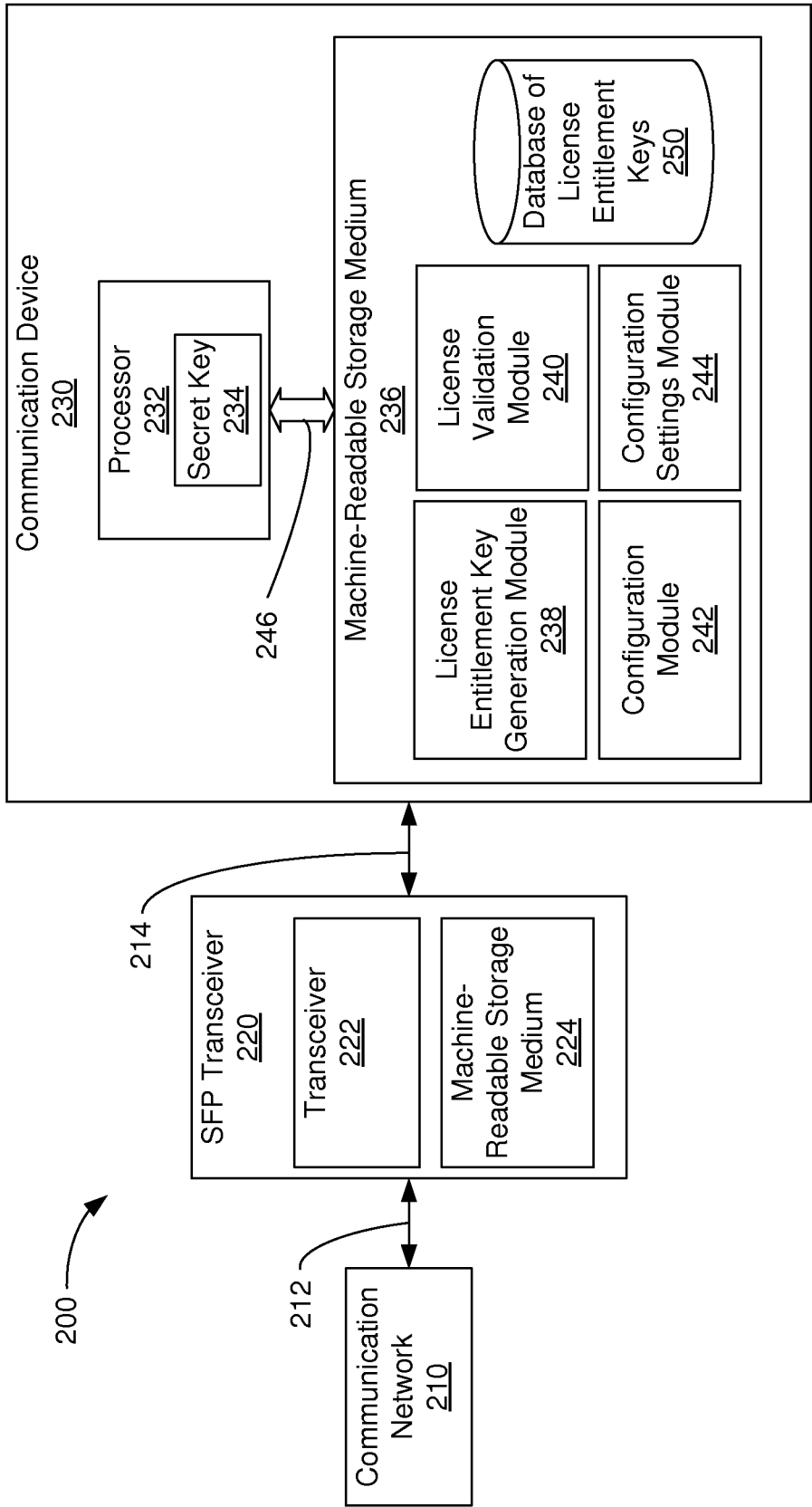


FIG. 2

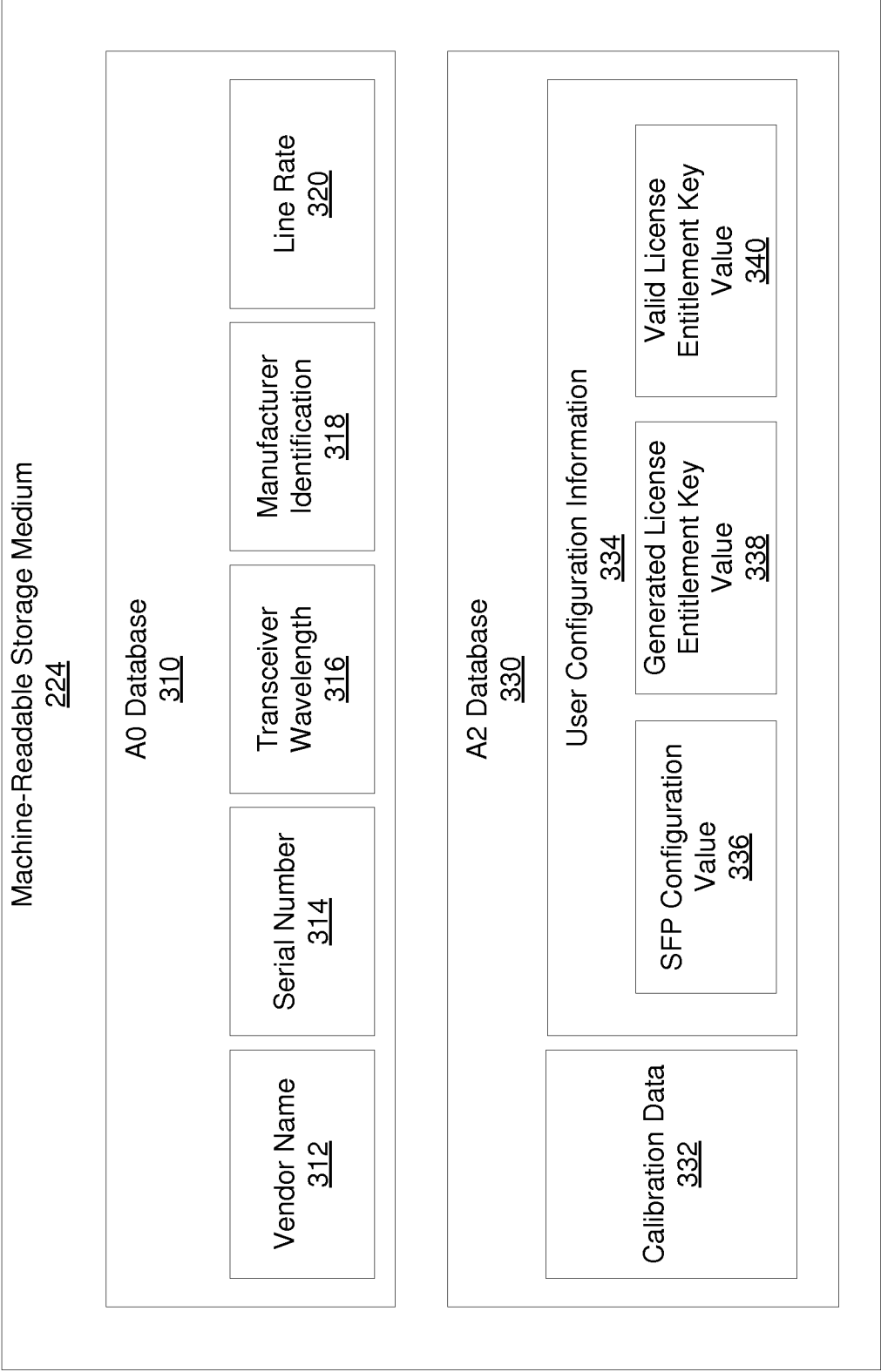


FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US2010/050908

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - H04B 10/00 (2010.01)

USPC - 398/135

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC(8) - H04B 10/00 (2010.01)

USPC - 398/135, 9, 136; 380/44; 370/907

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

USPTO WEST System (US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT), Google Patents, PatBase

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2004/0071389 A1 (HOFMEISTER et al) 15 April 2004 (14.04.2004) entire document	1-20
Y	US 2005/0265717 A1 (ZHOU) 01 December 2005 (01.12.2005) entire document	1-20
Y	US 2005/0049976 A1 (YANG) 03 March 2005 (03.03.2005) entire document	5-7, 15-17
A	US 7,187,709 B1 (MENON et al) 06 March 2007 (06.03.2007) entire document	1-20
A	US 2006/0025018 A1 (DUBE et al) 02 February 2006 (02.02.2006) entire document	1-20
A	US 7,360,954 B1 (SEEVER et al) 22 April 2008 (22.04.2008) entire document	1-20
A	US 2006/0277346 A1 (DOAK et al) 07 December 2006 (07.12.2006) entire document	1-120
A	US 2007/0258715 A1 (ANDRONI et al) 09 November 2007 (09.11.2007) entire document	1-20

☐ Further documents are listed in the continuation of Box C.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

15 November 2010

Date of mailing of the international search report

24 NOV 2010

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents
P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-3201

Authorized officer:

Blaine R. Copenheaver

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774