

EFFICIENCY IMPROVEMENTS IN FIRMWARE UPDATES FOR LARGE DEPLOYMENTSTechnical Field

5 The present disclosure relates to a system and method for updating firmware on devices and in particular to a system and method for updating firmware on groups of those devices using a plurality of servers.

Background

10 A number of endpoint devices accessible over a network may be provided with firmware for performing their required operations. For example, in the context of monitoring the usage of electricity or gas, the endpoint devices may take the form of smart meters, which collect readings of electricity and gas usage and dispatch those readings in packets sent over the network to a headend system. To perform these operations, the
15 smart meters comprise firmware held in the memory of the smart meter that provides low-level control of the smart meter, enabling it to perform its operations of collecting measurement data and reporting the measurement data to the headend system.

20 There may be a need at certain times to provide updates to the firmware running on the endpoint devices. This may be achieved by a server dispatching packets comprising firmware updates to a number of endpoint devices, with each of these devices being configured to apply the updates to the firmware held in its memory. However, challenges may arise when there are large numbers of endpoint devices to which the updates must be applied.

25

Summary

When firmware updates are to be provisioned to large number of endpoint devices, a large number of gateways may be used to supply the necessary updates to the endpoint
30 devices. In this case, different firmware operations may be performed for different groups of endpoints associated with different gateways. However, problems may arise due to network topology changes, wherein an endpoint may become associated with a different part of the network (e.g. a different gateway) and hence receive packets associated with a different firmware update operation and containing a different transfer identifier
35 associated with the firmware update. Such network topology changes may result in an

inefficient update operation, due to the number of losses on the network, since the endpoint devices may drop received packets associated with different firmware update operations.

5 According to a first aspect, there is provided a data processing system comprising: a control system for initiating a firmware update process to provide a firmware update to a plurality of endpoint devices; a plurality of servers, each of the servers hosting a firmware update service and comprising memory storing the firmware update to be supplied to the plurality of endpoint devices; a plurality of gateways, each of which is configured to
10 interface one of the servers with ones of the endpoint devices in order to supply the firmware update to the ones of the endpoint devices; and the plurality of endpoint devices, wherein the control system is configured to provide a different one of a plurality of firmware update requests to each of the servers, wherein each of the firmware update requests comprises an identifier of a different group of one or more of the gateways,
15 wherein each of the servers is configured to, in response to receipt of the respective one of the firmware update requests, dispatch packets comprising the firmware update to the respective one or more of the gateways identified by the identifier in the respective one of a plurality of firmware update requests, each of the packets comprising a same identifier for the firmware update process, wherein each of the endpoint devices is
20 configured to: receive a plurality of further packets from at least one of the gateway devices, the plurality of further packets comprising the firmware update and the same identifier for the firmware update process; and accept the respective plurality of further packets in response to determining that the same identifier for the firmware update process is present in the received further packets.

25 A central control system initiates a single operation, to cause the firmware update to be applied across the network by providing multiple requests to different servers, where the network is divided by each request specifying a unique set of gateways. Each of the servers supplies packets comprising the firmware update to the set of gateways identified
30 by the request received from the control system, where those packets comprise the same transfer identifier (i.e. the same identifier for the firmware update process). Each endpoint receives packets from a gateway. Since those packets comprise the same transfer identifier, if an endpoint migrates between gateways, the endpoint will still receive packets having the same transfer identifier, which will, therefore not be dropped.

35

According to a second aspect, there is provided a control system for initiating a firmware update process to provide a firmware update to a plurality of endpoint devices, wherein the control system comprise processing circuitry configured to: generate a plurality of firmware update requests by: dividing a plurality of gateway devices into a plurality of groups of gateway devices, each of the groups of gateway devices comprising one or more gateway devices; and providing each of the firmware update requests with: an identifier of a different one of the groups of gateway devices; a same identifier of the firmware update process; and a same identifier of the firmware update to be provisioned to each of the endpoint devices; and providing each of the plurality of firmware update requests to a different one of a plurality of servers.

According to a third aspect, there is provided a method comprising: providing from a control system, a different one of a plurality of firmware update requests to each of a plurality of servers, wherein each of the firmware update requests comprises an identifier of a different group of one or more of the gateways; at each of a plurality of servers: hosting a firmware update service for a firmware update process for providing the firmware update to each of a plurality of endpoint devices; and in response to receipt of the respective one of the firmware update requests, dispatch packets comprising the firmware update to the one or more of the gateways identified by the identifier in the respective one of the firmware update requests; and at each of the endpoint devices: receiving a plurality of further packets from at least one of the gateways, the plurality of further packets comprising the firmware update and the same identifier for the firmware update process; and accepting each of the plurality of further packets in response to determining that the same identifier for the firmware update process is present in each of the received further packets.

In some embodiments, a method comprises: at a first of the endpoints: receiving part of the firmware update from a first of the gateways in a first subset of the respective further packets; and subsequently, receiving a further part of the firmware update from a second of the gateways in a second subset of the respective further packets.

In some embodiments, the method comprises: at a first of the endpoints, following reception of the part of the firmware update, providing an indication to the second of the gateways of progress of provision of the firmware update to the first of the endpoints; and at the second of the gateway devices continuing provision of the firmware update from a point identified based on the indication of progress.

In some embodiments, the method comprises, at a first of the endpoints: receiving the part of the firmware update during a first time period during which the first of the endpoints is connected to the first of the gateways; and receiving the further part of the
5 firmware update during a second time period during which the first of the endpoints is connected to the second of the gateways.

In some embodiments, each of the endpoint devices is a smart meter comprising: processing circuitry; and memory storing firmware for controlling the processing circuitry,
10 wherein the method comprises, at each smart meter: updating the firmware stored in the memory based on the received firmware update.

In some embodiments, the method comprises, at each smart meter to: under the control of the firmware, causing measurements of energy usage to be reported to the control
15 system.

In some embodiments, the control system is a headend system associated with the smart meters.

In some embodiments, the method comprises: each of the endpoint devices, in response to receipt of one or more initial packets comprising the same transfer identifier: causing the same transfer identifier to be stored in storage of the endpoint; and subsequently, determining to accept the respective plurality of further packets in response to determining a match between the same transfer identifier held in the storage and the
20 same transfer identifier in each of the respective plurality of further packets.
25

In some embodiments, the method comprises: at a first endpoint of the plurality of the endpoints, in response to determining that one or more parts of the firmware are missing from memory of the respective endpoint, sending a request for the missing firmware to
30 a first of the servers; and the first of the servers retrieving from its memory the one or more parts of the firmware and returning the one or more parts of the firmware to the first endpoint in response to receipt of the request.

According to a fourth aspect, there is provided a method for initiating a firmware update process to provide a firmware update to a plurality of endpoint devices, wherein the
35 method comprises: generating a plurality of firmware update requests by: dividing a

plurality of gateway devices into a plurality of groups of gateway devices, each of the groups of gateway devices comprising one or more gateway devices; and providing each of the firmware update requests with: an identifier of a different one of the groups of gateway devices; a same identifier of the firmware update process; and a same identifier of the firmware update to be provisioned to each of the endpoint devices; and dispatching each of the plurality of firmware update requests to a different one of a plurality of servers.

In some embodiments, the method comprises storing each of the plurality of firmware update requests in storage of the control system; and for each of the plurality of firmware update requests, send each of the firmware update requests to a respective one of the servers in response to receipt of a request from the respective one of the servers.

In some embodiments, the method comprises: for each of the plurality of firmware update requests: store an associated lock in storage of the control system; and when the respective firmware update request is sent to one of the servers, update the associated lock to indicate that the firmware update request is unavailable; and in response to receipt of each of the requests from the servers: select one of the plurality of firmware update requests in response to determining that the lock associated with that firmware update request indicates that that firmware update request is available; and send the selected one of the plurality of firmware update requests to the server from which the respective request was received.

According to a fifth aspect, there is provided a computer program comprising computer readable instructions, which when executed by at least one processor, causes a method according to the fourth aspect or any embodiment thereof to be performed.

According to a sixth aspect, there is provided a non-transitory computer readable medium storing the computer program according to the fifth aspect.

Brief Description of Drawings

Arrangements of the present invention will be understood and appreciated more fully from the following detailed description, made by way of example only and taken in conjunction with drawings in which:

Figure 1 shows an example network in which a control system interfaces with a plurality of endpoint devices via a plurality of network gateway devices and a plurality of servers;

Figure 2A illustrates an example of how an initial firmware update request may be divided into a plurality of firmware update requests by a control system;

Figure 2B illustrates how the firmware and plurality of firmware requests may be stored in storage of the control system;

5 Figure 3A shows how the work represented by multiple requests is divided between a plurality of servers;

Figure 3B shows an example of how a firmware update request may be provided to a server, which is configured to distribute the firmware update to a plurality of gateways identified in the firmware update request;

10 Figure 4 shows an example of how firmware received from a server is distributed by a gateway device to a plurality of endpoint devices connected to that gateway device;

Figure 5 illustrates various processing circuitry and storages within an endpoint device;

Figure 6A illustrates how an endpoint may request missing firmware blocks from the server;

15 Figure 6B illustrates how an endpoint may change the gateway with which it is associated;

Figure 7 illustrates an example computer system comprising memory and processing circuitry;

20 Figure 8 illustrates an example device comprising a user interface, memory, and processing circuitry;

Figure 9 illustrates an example method implemented in the data processing system; and

Figure 10 illustrates an example method implemented in the control system of the data processing system.

25 Detailed Description

Embodiments are implemented in a data processing system that interfaces with a plurality of endpoints for collecting measurement data from those endpoints.

30 Reference is made to Figure 1, which illustrates a data processing system 1, in which a control system 2 interfaces with a plurality of servers 4 and with a plurality of network devices 6 and endpoints 8 reachable by the network devices 6. The data processing system 1 comprises the control system 2, servers 4, network devices 6, and endpoints 8. The network devices 6 are referred to herein as gateways 6. The gateways 6 may also
35 be referred to as gateway devices. The gateways 6 are part of a network in which the

control system 2 sends commands to the endpoints 8 and receives data (e.g. measurement data) from the endpoints 8 in return.

5 In the context in which the endpoints 8 take the form of smart meters, the control system 2 may be a headend system, and the gateway devices 6 may take the form of collectors, which are responsible for collecting measurement data from the smart meters and returning this measurement data to the headend system.

10 The gateways 6 additionally interface the servers 4 with the endpoints 8 for the purpose of enabling the servers 4 to transmit firmware updates to the endpoints 8 to update the firmware stored in the endpoints 8. Each of the servers 4 comprises computer readable instructions, which when executed by at least one processor of the server 4 provides a firmware download service 3, which causes firmware to be provided to the endpoints 8 of the system 1. The control system 2 may provide a same set of firmware to each of the
15 servers 4 to enable the firmware download service 3 to distribute this firmware to each of the endpoints 8. Each of the servers 4 is operable to provide firmware updates to more than one of the gateways 6, and each of the gateways 6 is operable to provide firmware updates to more than one of the endpoints 8. However, the relationship between a server 4 and a gateway device 6 to which it provides firmware is not fixed, such that it is possible
20 for a gateway device 6 to communicate with more than one of the servers 4. Additionally, the relationship between the gateways 6 and the endpoints 8 is not fixed, such that it is possible for one of the endpoints 8 to switch between gateways 6 with which it is communicating as a result of network topology changes.

25 Once the control system 2 has distributed firmware to the servers 4, the control system 2 is configured to issue commands to cause the servers 4 to dispatch the firmware to the gateways 6 and endpoints 8. To do so, the control system 2 divides the network with reference to the gateways 6.

30 Reference is made to Figure 2A, which illustrates processing that may be performed in the control system 2 in order to generate a plurality of firmware update requests. An initial request 210 is generated by the system 2.

35 The initial request 210 comprise an identifier of the firmware update operation, which is referred to herein as the transfer ID. The transfer ID is used by endpoints 8 to distinguish packets associated with one firmware update process from those associated with

another firmware update process, and to drop packets associated with a firmware update process different from the process used to update firmware on the endpoints 8. The initial request 210 also comprises the firmware update itself (shown as 'Firmware Binary' in Figure 2A). This is the firmware to be provided to each of the endpoints 8 as part of the
5 firmware update process.

The initial request 210 further comprises a set of identifiers of a number of gateway devices 6 in the system 1. The number of gateways is N, and the identifiers are identifiers of gateways that may be referenced by numbers 1 to N.

10 The request 210 is provided to a staging stage 220 which based on the request 210, produces a plurality of firmware update requests 230a-c. Three example requests 230a-c are shown in Figure 2A, but it would be appreciated that there may be a different number of requests. In producing the requests 230a-c, the control system 2 divides the
15 set of gateways (i.e. 1 to N in the example shown) into a plurality of subsets of gateways (e.g. 1 to m, m to 2m, N-m to N), and provides each request with an indication of a different one of the subsets.

The staging stage 220 extracts the firmware update 240 from the initial request 210, and
20 includes in each of the requests 230a-c, an identifier of the firmware 240. Each of the requests 230a-c also comprises a transfer ID and an identifier of the firmware to be applied to the endpoints 8. The transfer ID and the firmware identifier are the same for each of the requests 230a-c. Each of the requests 230a-c may also comprise a request token, which is used by the control system 230 to identify the firmware update process
25 associated with the multiple requests 230a-c.

Although not shown in Figure 2A, each of the requests 230a-c may also comprise an indication of the time at which the request was generated. Each of the requests 230a-c may also comprise an indication of the settings for downloading the firmware. Such
30 settings could relate for example to the network protocol used.

Reference is made to Figure 2B, which shows how the control system 2 stores the firmware 240 and each of the requests 230a-c in a storage 250 of the control system 2. The firmware 240 is stored as part of the storage 250. In addition to the storage of the
35 firmware image 240, the control system 2 stores in the storage 250, a table 260, which may be referred to as the firmware blocks table 260. The firmware image 240 is logically

divided into a plurality of blocks, since the entire image 240 may be too large to transmit in a single packet. In some embodiments, the firmware image 240 may be between 800KB to 900KB, with each firmware block of the image being 1000 bytes in size. The firmware blocks table 260 comprises, for each of the plurality of blocks, a pointer
5 associated with that respective block and a length field associated with the respective block. The term 'firmware blocks' herein refers to parts of the firmware image 240.

The storage 250 stores a plurality of firmware update requests 230a-c and state information 280 associated with each of the firmware update requests 230a-c. The state
10 information 280 indicates for each request, whether or not that request is being handled by one of the servers 4. The state information 280 may, for this purpose, comprise a lock associated with each of the requests 230a-c.

Reference is made to Figure 3A, which illustrates how the servers 4 retrieve the requests
15 from the control system 2. After storing the firmware 240 and the update requests 230a-c in the storage 250, the control system 2 issues a notification (shown as "1. Notification" in Figure 3A) to each of the servers 4. In response to receipt of such a notification, each server 4 issues a request (shown as "2. Poll" in Figure 3A) to the control system 2 to retrieve one of the firmware update requests 230a-c. The requests sent by the server 4
20 do not identify a particular one of the firmware update requests 230a-c. In response to receipt of each of the requests from the servers 4, the control system 2 checks the state information 280 to determine whether or not any of the requests 230a-c are available (i.e. are not currently being serviced by any of the other servers 4). If any of the requests 230a-c are available, the control system 2 sends one of the available requests (shown
25 as "3. Request" in Figure 3A) to the respective server 4. The control system 2 then updates the state information 280 to indicate that the request that was available is no longer available. The control system 2 follows the same process for responding to each of the requests ("2. Poll") from the other servers 4. By implementing locks in the state information 280 in this way, the control system 2 ensures that each of the requests 230a-c is allocated to a different server 4. However, the allocation of requests 230a-c to servers
30 4 is not predetermined and is dependent upon the order in which the requests ("2. Poll") are received at the control system 2.

Reference is made to Figure 3B, which illustrates the provision of a firmware update
35 request 230a and part of the firmware update 240 to one of the servers 4. The request 230a (which corresponds to one of "3. Request" shown in Figure 3A) is transmitted to

the server 4 in a plurality of packets. In response to receipt of the request 230a, the server 4 issues one or more requests 300 to retrieve blocks of the firmware 240 from the storage 250 of the control system 2. The requests 300 comprise an identifier of the firmware 240 identified by the firmware identifier contained in the request 230a. The control system 2, in response to receipt of these requests 300, returns packets 310 comprising the requested firmware to the server 4.

The firmware update 240 is dispatched to the server 4 in a plurality of packets sent over the network. The server 4 stores in memory, the firmware provided in this plurality of packets.

The first request 230a is dispatched to the server 4 in one or more packets sent over the network. Based on the identification of the first subset of gateways 1 to m in the first request 230a, the server 4 dispatches sets of packets 300a-c to the gateways 1 to m. In response to receipt of the packets 310, the server 4 dispatches the firmware contained in those packets to each of the gateways 6. The server 4 dispatches the firmware in packets 320a-c to each of the gateways 6. Specifically, the server 4 dispatches one of the sets of packets 300a-c to each of the gateways 1 to m. Each of the sets of packets 300a-c comprise the same set of firmware that was received by the server 4 from the control system 2. The server 4 continues to request and receive blocks of the firmware 240 from the control system 2 and transfer the received blocks to each of the gateways 6.

In addition to including the updated firmware to be applied to the endpoints 6, each packet belonging to the sets of packets 320a-c also includes the transfer ID that is contained in the request 230a.

Although not illustrated in Figure 3B, each of the other servers 4 that receives one of the requests 230a-c from the control system 2 dispatches the firmware 240 to each of the gateways 6 identified in the respective one of the requests 230a-c received from the control system 2.

Reference is made to Figure 4, which illustrates the provision of firmware to endpoints 8 that are in communication with one of the gateway devices 6. In this example, there are two endpoints 8 that are each associated with the gateway GW1 for the purposes of sending measurement data to the control system 2 and receiving firmware updates. The

association between the endpoints 8 and the gateway GW1 may be a temporary one, which may change as the network topology changes.

5 In response to the set of packets 300a, the gateway 6 provides a set of packets 400a-b to each of the endpoints 8 that it is currently associated with. A first one or more of the set of packets 400a-b sent to each of the endpoints 8 provides an indication that a firmware update is to be provided to the endpoints 8 in the following packets. The first one of the packets also comprise the transfer ID received by the gateway 6 from the server 4. The transfer ID is stored by each endpoint 8 and used to check that further
10 incoming packets received and associated with a firmware update process are associated with the same firmware update process.

Although not illustrated in Figure 4, each of the other gateways 6 in the system 1 that is identified in one of the requests 230a-c dispatched from the control system 2, also
15 dispatches a set of packets to endpoints 8 with which it is associated, where those packets contain the firmware and the transfer ID.

Reference is made to Figure 5, which illustrates components of an endpoint 8. The endpoint 8 shown may be the endpoint EP1 shown in Figure 4. The endpoint 8 comprises
20 an interface 500 at which the set of packets 400a are received. The interface 500 may comprise protocol processing circuitry to remove one or more lower layer headers of each of the packets 400a. When the first of the packets 400a is received, the circuitry 510 receives the transfer ID contained in this packet and stores that transfer ID in the transfer ID storage 520. Subsequent ones of the packets 400a are received at the
25 interface 500, where those packets comprise firmware to be applied to update the firmware currently stored in the memory 540 of the endpoints. Each of those subsequent ones of the packets 400a also comprises a transfer ID. In response to receipt of each packet, the circuitry 510 checks the transfer ID received in those packets 400a against the transfer ID held in the storage 520 to determine whether there is a match. In response
30 to determining a match, the respective packet and the associated piece of firmware contained in the respective packet is accepted. In response to determining a mismatch, the packet is dropped and the contents of the packet are erased.

When a match between the transfer ID in one of the packets 400a and the stored transfer
35 ID is detected, the memory controller 530 writes the firmware contained within that

packet to the firmware memory 540. In doing so, part of an earlier version of the firmware stored in the memory 540 may be overwritten.

5 The endpoint 8 also comprise processing circuitry 550, which is configured to operate in accordance with the firmware stored in the memory 540. For example, the processing circuitry 550 may, under the control of the firmware held in the memory 540, cause measurements of electricity or gas usage to be recorded, and cause reports of these measurements to be dispatched to the control system 2.

10 Although not illustrated in Figure 5, each of the other endpoint 8 in the system 1 that is associated with one of the gateways 6 identified in one of the requests 230a-c also performs equivalent processing with respect to packets received from its associated gateway and containing the same transfer ID.

15 In some embodiments, each of the endpoints 8 may determine whether or not it has received all of the blocks of the firmware update 240. If the endpoint 8 determines it has not received all of the blocks of the firmware update 240, the endpoint 8 issues a request to the server 4 with which it is associated to retrieve those missing blocks.

20 Reference is made to Figure 6A, which illustrates an example in which an endpoint 8 has received a part 600 of the firmware update 240. The part 600 comprises a number of blocks of the firmware 240 but, as indicated, is missing two blocks (i.e. blocks #2 and #9). In response to determining that two of the blocks of firmware 240 are missing, the endpoint 8 issues a request 610 to retrieve the missing blocks. The request 610 is sent
25 by the endpoint 8 to the gateway 6, and is sent from the gateway 6 to the server 4. The server 4 stores a copy of the firmware 240. In response to receipt of the request 610, the server 4 retrieves the identified missing firmware blocks and sends the blocks 620a, 620b to the gateway 6 from which the request 610 was received. The gateway 6 sends the blocks 620a, 620b to the endpoint 8.

30 In the example of Figure 6A, the firmware 240 is shown as comprising only 10 blocks. However, in practice the number of blocks may be different and would likely be more than 10. Furthermore, in the example given, the number of missing blocks is two, but could be a different number. The example is given for one of the endpoints 8, but each
35 of the other endpoints 8 in the system 1 could also perform the same process to retrieve blocks from its associated server 4.

An advantage of providing a firmware download service 3 at each of the servers 4 is that if any endpoint 8 is missing blocks of the firmware 240, that endpoint may retrieve those missing blocks from its associated server 4, rather than having to request them from the control system 2. In this way, a bottleneck at the control system 2 is avoided.

Network topology changes during the firmware update process, may cause an endpoint 8 to switch from being associated with one gateway 6 to being associated with another gateway 6. According to embodiments, when the endpoint 8 switches gateway 6 in this way, the provision of the firmware to that endpoint 8 may continue. The endpoint 8 may provide a status indication indicating its position in the firmware update process, which is used by the gateway 6 to continue providing remaining firmware to the endpoint 8.

Reference is made to Figure 6B, which shows a server 4, a gateway 6, and an endpoint EP3. Initially, the endpoint EP3 is associated with the gateway GW1 and receives packets 600a comprising firmware from gateway GW1, which have been received at gateway GW1 from server 4. The packets 600a comprise part of the firmware update to be applied to the endpoint EP3. Following the receipt of the packets 600a, the endpoint 8 connects to gateway GW2 instead of gateway GW1, and so no longer receives packets from gateway GW1. In this way, the firmware updates from the GW1 are interrupted. When EP3 connects instead to GW2, EP3 may send an indication of its progress in downloading the firmware to the gateway GW2. Such an indication may indicate how much of the total firmware update has been received so far at EP3. In response, the gateway GW2 commences sending the remaining part of the firmware update in a further set of packets 600b. Each of the further set of packets 600b contains the same transfer ID as the set of packets 600a, and so the further set of packets 600b are accepted and the firmware therein applied to update the firmware held in memory 540.

Reference is made to Figure 7, which illustrates an example computer system 700 that may provide any of the control system 2, server 4, gateway devices or endpoint devices 8. The system 700 may comprise a server, back-end system, or the like.

The system 700 comprises at least one memory 710, 720, at least one data processing unit 730, 740 and an input/output interface 750. The at least one memory 710, 720 comprises a random access memory 710 and at least one hard drive 720. The memories 710, 720 store computer executable code which, when executed by at least one data

processing unit 730, 740, perform the steps described as being performed by the system 700. The memories 710, 720 may be used for storing data associated the control application. In particular, the memories 710, 720 may be used for storing a log file comprising data logged by the control application.

5

The at least one processor 730, 740 communicates with the memories 710, 720 to load instructions for execution, load data for processing, and store the results of processing that data. At the interface 750, the system 700 sends and receives messages. The messages received at the interface 750 comprise data for processing by the at least one processor 730, 740. The messages sent from the interface 750 are created by the at least one processor 730, 740.

10

The operations described above as being performed by any of the control system 2, the server 4, the gateway device 6, and endpoint devices 8 may be performed by the data processor 730 executing computer readable instructions to cause the respective system 700 to perform those operations or by additional processing components 740 implementing the operations in hardware (e.g. in an FPGA or ASIC).

15

As an alternative to the server type system 700, one or more of the control system 2, servers 4, gateway devices 6 or endpoint devices 8 may be provided as a different type of device having a user interface. Reference is made to Figure 8, which illustrates an example of such a computing device 800. The device 800 may be a mobile user equipment (UE), a personal computer (PC), a terminal or workstation, or some other form of device.

20

25

The device 800 comprises an interface 840 over which it sends and receive signals. The interface 840 may be a wired or wireless interface. For instance, the interface 840 may comprise a wired interface for connection to a wired network (e.g. a local area network and/or the internet). Alternatively or in addition, the interface 840 may comprise transceiver apparatus configured to send and receive communications over a radio interface. The transceiver apparatus may be provided, for example, by means of a radio part and associated antenna arrangement. The antenna arrangement may be arranged internally or externally to the system 800.

30

35

The system 800 is provided with at least one data processing entity 815, at least one random access memory 820, at least one read only memory 825, and other possible

components 830 for use in software and hardware aided execution of tasks it is designed to perform, including control of, access to, and communications with access systems and other communication devices. The at least one random access memory 820 and the hard drive 825 are in communication with the data processing entity 815, which may be a data processor. The data processing, storage and other relevant control apparatus can be provided on an appropriate circuit board and/or in chipsets. A user controls the operation of the system 800 by means of a suitable user interface such as key pad 810, or by voice commands. A display 805 is included on the system 800 for displaying visual content to a user. The system 800 may also comprise a speaker for providing audio content.

The operations described above as being performed by any of the control system 2, the server 4, the gateway device 6, and endpoint devices 8 may be performed by the data processor 815 executing computer readable instructions to cause the respective device 800 to perform those operations or by additional processing components 830 implementing the operations in hardware (e.g. in an FPGA or ASIC).

Reference is made to Figure 9, which illustrates an example method 900 for performing a firmware update process according to embodiments of the application. The method 900 is implemented in the system 1.

At S910, the control system 2 provides, a different one of the plurality of firmware update requests (e.g. requests 230a-c) to each of a plurality of servers 4. Each of the plurality of firmware update requests comprises a same identifier (i.e. a transfer identifier) of the firmware update process. Each of the firmware update requests also comprises an identifier of a different group of the gateways 6 in the system 1. Each of the plurality of firmware update requests comprises an identifier of the same firmware. Each of the plurality of firmware update requests is made available in the storage 250 of the control system 2 and is fetched by a different one of the servers 4.

At S920, at each of the plurality of servers 4, in response to the firmware update request received at the respective server 4 at S910, a firmware update service 3 is hosted on the server 4. As part of hosting the firmware update service 3, firmware 240 to be distributed to the endpoint devices 8 is stored in memory of the respective server 4.

At S930, each of the plurality of servers 4, in response to receipt of one of the firmware update requests, causes packets (e.g. packets 300a-c) comprising the firmware update to be provided to the group of gateways 6 identified by that request. The firmware update service 3 performs S930.

5

The transfer at S930 from the servers 4 to the different gateways 6 may be concurrent, such that different servers 4 send the firmware update to their respective gateways 6 at the same time.

10 Each of the gateways 6 in response to receiving packets comprising the firmware update from one of the servers 4 provides further packets comprising the firmware update (e.g. one of packets 400a,b) to a number of the endpoint devices 8. As a consequence, at S940, each of the endpoint devices 8 receives packets comprising part of the firmware update from one of the gateways 6.

15

The transfer at S940 from the gateways 6 to the devices 8 may be concurrent, such that different gateways 6 sent the firmware update to their respective devices 8 at the same time.

20 Although, S930 and S940 are shown as being performed sequentially, in practice they may overlap in time. For instance, each server 4 may transfer part of the firmware update to a number of gateways 6, with each gateway 6 transferring that part of the firmware update to a number of endpoint devices 8, before the entire firmware update has been sent from the servers 4 to the gateways 6.

25

S950, S960, and S970 are performed for each of the further packets received at S940.

30 At S950, each endpoint device 8 compares the transfer ID received in each further packet that is received at S940 to the transfer ID received at the endpoint device 8 in an earlier packet sent from the gateway 6. If there is match, the method 900 proceeds to S960, where the further packet is accepted, and the firmware contained therein is stored to memory 540 of the respective endpoint device 8. If there is no match, the method 900 proceeds to S970, where the further packet is rejected, and the firmware contained therein is deleted.

35

Reference is made to Figure 10, which illustrates an example method 1000 for initiating a firmware update process according to embodiments of the application. The method 1000 is implemented in the control system 2.

- 5 At S1010, the control system 2 divides the plurality of gateway devices 6 into a plurality of groups of gateway devices 6. The division of the gateways 6 may be performed evenly such that each of the groups contains a number of gateways that is substantially the same between the different groups.
- 10 At S1020, the control system 2 generates a plurality of firmware update requests, including providing each of the firmware update requests with: an identifier of a different one of the groups of gateway devices 6; a same identifier of the firmware update process; and an identifier of the firmware update to be provisioned to each of the endpoint devices 8.
- 15 At S1030, S1040, and S1050 the control system 2 provides each of the plurality of firmware update requests to a different one of a plurality of servers 4.
- 20 At S1030, the plurality of firmware update requests are stored in storage 250.
- 20 At S1040, a notification is provided to each of the servers 4.
- 25 At S1050, each of the firmware update requests is provided to a different one of the servers 4 in response to a request from each of a different one of the servers 4.
- 25 Steps described above as belonging to the method 900 and method 1000 may be combined.
- 30 Implementations of the subject matter and the operations described in this specification can be realized in digital electronic circuitry, or in computer software, firmware, or hardware, including the structures disclosed in this specification and their structural equivalents, or in combinations of one or more of them. For instance, hardware may include processors, microprocessors, electronic circuitry, electronic components, integrated circuits, etc. Implementations of the subject matter described in this
- 35 specification can be realized using one or more computer programs, i.e., one or more modules of computer program instructions, encoded on computer storage medium for

execution by, or to control the operation of, data processing apparatus. Alternatively or in addition, the program instructions can be encoded on an artificially-generated propagated signal, e.g., a machine-generated electrical, optical, or electromagnetic signal that is generated to encode information for transmission to suitable receiver apparatus for execution by a data processing apparatus. A computer storage medium can be, or be included in, a computer-readable storage device, a computer-readable storage substrate, a random or serial access memory array or device, or a combination of one or more of them. Moreover, while a computer storage medium is not a propagated signal, a computer storage medium can be a source or destination of computer program instructions encoded in an artificially-generated propagated signal. The computer storage medium can also be, or be included in, one or more separate physical components or media (e.g., multiple CDs, disks, or other storage devices).

While certain arrangements have been described, the arrangements have been presented by way of example only, and are not intended to limit the scope of protection. The inventive concepts described herein may be implemented in a variety of other forms. In addition, various omissions, substitutions and changes to the specific implementations described herein may be made without departing from the scope of protection defined in the following claims.

ANNEX A

The present invention can also be defined by reference to the following clauses:

Clause 1. A data processing system comprising:

- 5 a control system for initiating a firmware update process to provide a firmware update to a plurality of endpoint devices;
- a plurality of servers, each of the servers hosting a firmware update service and comprising memory storing the firmware update to be supplied to the plurality of endpoint devices;
- 10 a plurality of gateways, each of which is configured to interface one of the servers with ones of the endpoint devices in order to supply the firmware update to the ones of the endpoint devices; and
- the plurality of endpoint devices,
- wherein the control system is configured to provide a different one of a plurality
- 15 of firmware update requests to each of the servers, wherein each of the firmware update requests comprises an identifier of a different group of one or more of the gateways,
- wherein each of the servers is configured to, in response to receipt of the respective one of the firmware update requests, dispatch packets comprising the firmware update to the respective one or more of the gateways identified by the identifier
- 20 in the respective one of a plurality of firmware update requests, each of the packets comprising a same identifier for the firmware update process,
- wherein each of the endpoint devices is configured to:
- receive a plurality of further packets from at least one of the gateway devices, the plurality of further packets comprising the firmware update and the
- 25 same identifier for the firmware update process; and
- accept the respective plurality of further packets in response to determining that the same identifier for the firmware update process is present in the received further packets.

- 30 Clause 2. A data processing system as in clause 1, wherein a first of the endpoints is configured to:

receive part of the firmware update from a first of the gateways in a first subset of the respective further packets; and

- 35 subsequently, receive a further part of the firmware update from a second of the gateways in a second subset of the respective further packets.

Clause 3. A data processing system as in clause 2, wherein the first of the endpoints is configured to, following reception of the part of the firmware update, provide an indication to the second of the gateways of progress of provision of the firmware update to the first of the endpoints,

wherein the second of the gateway devices is configured to continue provision of the firmware update from a point identified based on the indication of progress.

Clause 4. A data processing system as in clause 2 or clause 3, wherein the first of the endpoints is configured to:

receive the part of the firmware update during a first time period during which the first of the endpoints is connected to the first of the gateways; and

receive the further part of the firmware update during a second time period during which the first of the endpoints is connected to the second of the gateways.

Clause 5. A data processing system as in any preceding clause, wherein each of the endpoint devices is a smart meter comprising:

processing circuitry; and

memory storing firmware for controlling the processing circuitry,

wherein the processing circuitry of each smart meter is configured to:

update the firmware stored in the memory based on the received firmware update.

Clause 6. A data processing system as in clause 5, wherein the processing circuitry of each smart meter is configured to:

under the control of the firmware, cause measurements of energy usage to be reported to the control system.

Clause 7. A data processing system as in clause 5 or clause 6, wherein the control system is a headend system associated with the smart meters.

Clause 8. A data processing system as in any preceding clause, wherein for each of the endpoint devices, processing circuitry of the respective endpoint device is configured to:

in response to receipt of one or more initial packets comprising the same transfer identifier, cause the same transfer identifier to be stored in storage of the endpoint; and

subsequently, determine to accept the respective plurality of further packets in response to determining a match between the same transfer identifier held in the storage and the same transfer identifier in each of the respective plurality of further packets.

- 5 Clause 9. A data processing system as in any preceding clause, wherein a first endpoint of the plurality of the endpoints is configured to, in response to determining that one or more parts of the firmware are missing from memory of the respective endpoint, send a request for the missing firmware to a first of the servers, wherein the first of the servers is configured to retrieve from its memory the one or more parts of the firmware
10 and return the one or more parts of the firmware to the first endpoint in response to receipt of the request.

- Clause 10. A control system for initiating a firmware update process to provide a firmware update to a plurality of endpoint devices, wherein the control system comprise
15 processing circuitry configured to:
 generate a plurality of firmware update requests by:
 dividing a plurality of gateway devices into a plurality of groups of gateway devices, each of the groups of gateway devices comprising one or more gateway devices; and
20 providing each of the firmware update requests with:
 an identifier of a different one of the groups of gateway devices;
 a same identifier of the firmware update process; and
 a same identifier of the firmware update to be provisioned to each of the endpoint devices; and
25 providing each of the plurality of firmware update requests to a different one of a plurality of servers.

- Clause 11. A control system as in clause 10, wherein the control system comprises a storage, wherein the processing circuitry is configured to:
30 store each of the plurality of firmware update requests in the storage; and
 for each of the plurality of firmware update requests, send each of the firmware update requests to a respective one of the servers in response to receipt of a request from the respective one of the servers.

- 35 Clause 12. A control system as in clause 11, wherein the control system comprises a storage, wherein the processing circuitry is configured to:

for each of the plurality of firmware update requests:

store an associated lock in the storage; and

when the respective firmware update request is sent to one of the servers,
update the associated lock to indicate that the firmware update request is
5 unavailable; and

in response to receipt of each of the requests from the servers:

select one of the plurality of firmware update requests in response to
determining that the lock associated with that firmware update request indicates that that
firmware update request is available; and

10 send the selected one of the plurality of firmware update requests to the
server from which the respective request was received.

Clause 13. A method comprising:

15 providing from a control system, a different one of a plurality of firmware update
requests to each of a plurality of servers, wherein each of the firmware update requests
comprises an identifier of a different group of one or more of the gateways;

at each of a plurality of servers:

hosting a firmware update service for a firmware update process for
providing the firmware update to each of a plurality of endpoint devices; and

20 in response to receipt of the respective one of the firmware update
requests, dispatch packets comprising the firmware update to the one or more of
the gateways identified by the identifier in the respective one of the firmware
update requests; and

at each of the endpoint devices:

25 receiving a plurality of further packets from at least one of the
gateways, the plurality of further packets comprising the firmware update
and the same identifier for the firmware update process; and

accepting each of the plurality of further packets in response to
determining that the same identifier for the firmware update process is
30 present in each of the received further packets.

Clause 14. A method for initiating a firmware update process to provide a firmware
update to a plurality of endpoint devices, wherein the method comprises:

generating a plurality of firmware update requests by:

dividing a plurality of gateway devices into a plurality of groups of gateway devices, each of the groups of gateway devices comprising one or more gateway devices; and

providing each of the firmware update requests with:

5 an identifier of a different one of the groups of gateway devices;
 a same identifier of the firmware update process; and
 a same identifier of the firmware update to be provisioned to each
 of the endpoint devices; and

10 dispatching each of the plurality of firmware update requests to a different one of
a plurality of servers.

Clause 15. A computer program comprising computer readable instructions, which when executed by at least one processor, cause a method to be carried out, the method comprising:

15 generating a plurality of firmware update requests by:

 dividing a plurality of gateway devices into a plurality of groups of gateway devices, each of the groups of gateway devices comprising one or more gateway devices; and

 providing each of the firmware update requests with:

20 an identifier of a different one of the groups of gateway devices;
 a same identifier of the firmware update process; and
 a same identifier of the firmware update to be provisioned to each
 of the endpoint devices; and

25 dispatching each of the plurality of firmware update requests to a different one of
a plurality of servers.

CLAIMS:

1. A data processing system comprising:
 - a control system for initiating a firmware update process to provide a firmware update to a plurality of endpoint devices;
 - a plurality of servers, each of the servers hosting a firmware update service and comprising memory storing the firmware update to be supplied to the plurality of endpoint devices;
 - a plurality of gateways, each of which is configured to interface one of the servers with ones of the endpoint devices in order to supply the firmware update to the ones of the endpoint devices; and
 - the plurality of endpoint devices,
 - wherein the control system is configured to provide a different one of a plurality of firmware update requests to each of the servers, wherein each of the firmware update requests comprises an identifier of a different group of one or more of the gateways,
 - wherein each of the servers is configured to, in response to receipt of the respective one of the firmware update requests, dispatch packets comprising the firmware update to the respective one or more of the gateways identified by the identifier in the respective one of a plurality of firmware update requests, each of the packets comprising a same identifier for the firmware update process,
 - wherein each of the endpoint devices is configured to:
 - receive a plurality of further packets from at least one of the gateway devices, the plurality of further packets comprising the firmware update and the same identifier for the firmware update process; and
 - accept the respective plurality of further packets in response to determining that the same identifier for the firmware update process is present in the received further packets.
2. A data processing system as claimed in claim 1, wherein a first of the endpoints is configured to:
 - receive part of the firmware update from a first of the gateways in a first subset of the respective further packets; and
 - subsequently, receive a further part of the firmware update from a second of the gateways in a second subset of the respective further packets.

3. A data processing system as claimed in claim 2, wherein the first of the endpoints is configured to, following reception of the part of the firmware update, provide an indication to the second of the gateways of progress of provision of the firmware update to the first of the endpoints,

wherein the second of the gateway devices is configured to continue provision of the firmware update from a point identified based on the indication of progress.

4. A data processing system as claimed in claim 2, wherein the first of the endpoints is configured to:

receive the part of the firmware update during a first time period during which the first of the endpoints is connected to the first of the gateways; and

receive the further part of the firmware update during a second time period during which the first of the endpoints is connected to the second of the gateways.

5. A data processing system as claimed in claim 1, wherein each of the endpoint devices is a smart meter comprising:

processing circuitry; and

memory storing firmware for controlling the processing circuitry,

wherein the processing circuitry of each smart meter is configured to:

update the firmware stored in the memory based on the received firmware update.

6. A data processing system as claimed in claim 5, wherein the processing circuitry of each smart meter is configured to:

under the control of the firmware, cause measurements of energy usage to be reported to the control system.

7. A data processing system as claimed in claim 5, wherein the control system is a headend system associated with the smart meters.

8. A data processing system as claimed in claim 1, wherein for each of the endpoint devices, processing circuitry of the respective endpoint device is configured to:

in response to receipt of one or more initial packets comprising the same transfer identifier, cause the same transfer identifier to be stored in storage of the endpoint; and

subsequently, determine to accept the respective plurality of further packets in response to determining a match between the same transfer identifier held in the storage and the same transfer identifier in each of the respective plurality of further packets.

9. A data processing system as claimed in claim 1, wherein a first endpoint of the plurality of the endpoints is configured to, in response to determining that one or more parts of the firmware are missing from memory of the respective endpoint, send a request for the missing firmware to a first of the servers, wherein the first of the servers is configured to retrieve from its memory the one or more parts of the firmware and return the one or more parts of the firmware to the first endpoint in response to receipt of the request.

10. A control system for initiating a firmware update process to provide a firmware update to a plurality of endpoint devices, wherein the control system comprise processing circuitry configured to:

generate a plurality of firmware update requests by:

dividing a plurality of gateway devices into a plurality of groups of gateway devices, each of the groups of gateway devices comprising one or more gateway devices; and

providing each of the firmware update requests with:

an identifier of a different one of the groups of gateway devices;

a same identifier of the firmware update process; and

a same identifier of the firmware update to be provisioned to each of the endpoint devices; and

providing each of the plurality of firmware update requests to a different one of a plurality of servers.

11. A control system as claimed in claim 10, wherein the control system comprises a storage, wherein the processing circuitry is configured to:

store each of the plurality of firmware update requests in the storage; and

for each of the plurality of firmware update requests, send each of the firmware update requests to a respective one of the servers in response to receipt of a request from the respective one of the servers.

12. A control system as claimed in claim 11, wherein the control system comprises a storage, wherein the processing circuitry is configured to:

for each of the plurality of firmware update requests:

store an associated lock in the storage; and

when the respective firmware update request is sent to one of the servers, update the associated lock to indicate that the firmware update request is unavailable; and

in response to receipt of each of the requests from the servers:

select one of the plurality of firmware update requests in response to determining that the lock associated with that firmware update request indicates that that firmware update request is available; and

send the selected one of the plurality of firmware update requests to the server from which the respective request was received.

13. A method comprising:

providing from a control system, a different one of a plurality of firmware update requests to each of a plurality of servers, wherein each of the firmware update requests comprises an identifier of a different group of one or more of the gateways;

at each of a plurality of servers:

hosting a firmware update service for a firmware update process for providing the firmware update to each of a plurality of endpoint devices; and

in response to receipt of the respective one of the firmware update requests, dispatch packets comprising the firmware update to the one or more of the gateways identified by the identifier in the respective one of the firmware update requests; and

at each of the endpoint devices:

receiving a plurality of further packets from at least one of the gateways, the plurality of further packets comprising the firmware update and the same identifier for the firmware update process; and

accepting each of the plurality of further packets in response to determining that the same identifier for the firmware update process is present in each of the received further packets.

14. A method for initiating a firmware update process to provide a firmware update to a plurality of endpoint devices, wherein the method comprises:

generating a plurality of firmware update requests by:

dividing a plurality of gateway devices into a plurality of groups of gateway devices, each of the groups of gateway devices comprising one or more gateway devices; and

providing each of the firmware update requests with:

an identifier of a different one of the groups of gateway devices;
a same identifier of the firmware update process; and
a same identifier of the firmware update to be provisioned to each

of the endpoint devices; and

dispatching each of the plurality of firmware update requests to a different one of a plurality of servers.

15. A non-transitory computer readable storage medium storing a computer program comprising computer readable instructions, which when executed by at least one processor, cause a method to be carried out, the method comprising:

generating a plurality of firmware update requests by:

dividing a plurality of gateway devices into a plurality of groups of gateway devices, each of the groups of gateway devices comprising one or more gateway devices; and

providing each of the firmware update requests with:

an identifier of a different one of the groups of gateway devices;
a same identifier of the firmware update process; and
a same identifier of the firmware update to be provisioned to each

of the endpoint devices; and

dispatching each of the plurality of firmware update requests to a different one of a plurality of servers.