(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 September 2013 (26.09.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/139980 A1

(51) International Patent Classification:
H04W 8/08 (2009.01) *H04W 8/04* (2009.01)
H04W 8/12 (2009.01) *H04W 8/06* (2009.01)
H04L 29/12 (2006.01) *H04W 80/04* (2009.01)

(21) International Application Number:
PCT/EP2013/056142

(22) International Filing Date:
22 March 2013 (22.03.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12161075.2 23 March 2012 (23.03.2012) EP

(71) Applicant: **NEC EUROPE LTD.** [DE/DE]; Kurfürsten-Anlage 36, 69115 Heidelberg (DE).

(72) Inventors: **BIFULCO, Roberto**; Bergheimerstraße 38, 69115 Heidelberg (DE). **HASSELMEYER, Peer**; Mittlerer Hasenpfad 26, 60598 Frankfurt (DE). **BRUNNER, Marcus**; Hermann-Oberth-Weg 2, 69181 Leimen (DE).

(74) Agent: **MAISCH, T.**; Ullrich & Naumann, Schneidmühlstr. 21, 69115 Heidelberg (DE).

(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, BN, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, 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, RS, 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: METHOD FOR SUPPORTING MOBILITY OF END-POINTS IN A NETWORK, CONTROLLER ENTITY AND NETWORK

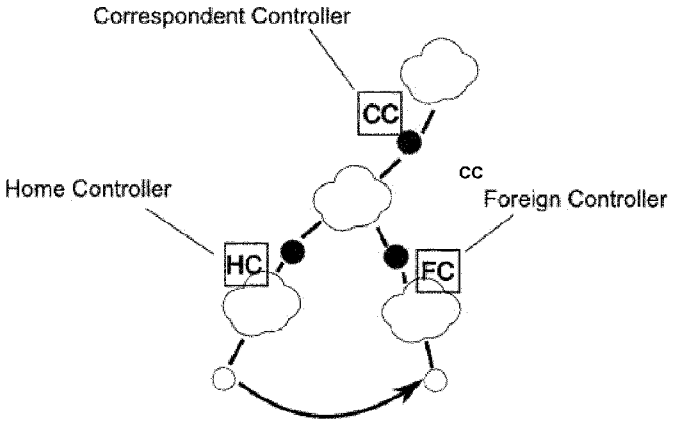

Fig. 2

(57) Abstract: A method for supporting mobility of end-points in a network, in particular a TCP/IP network, wherein said network includes access networks and a core network, wherein said access networks are connected to said core network via a switch, preferably being configured to use the Open Flow protocol, wherein said core network provides connectivity among said access networks, wherein an end-point – migrating node – connected to one of said access networks – home network – migrates to another one of said access networks – foreign network –, wherein one or more controller entities, in particular Open Flow Controllers, are employed for controlling the switches of said access networks, wherein said one or more controller entities are able to play the roles of - a home controller that controls a home switch of said home network, - a foreign controller that controls a foreign switch of said foreign network and/or - a correspondent controller that controls a correspondent switch of a correspondent network, wherein, after migration of said migrating node from said home network to said foreign network, a new IP address – locator – belonging to said foreign network is assigned to said migrating node, wherein said locator is employed to find the current location of said migrating node in the network, wherein said migrating node's original IP address – identifier – belonging to said home network is employed to identify said migrating node, and wherein an identifier/locator mapping is employed and reactively updated at the controllers. Furthermore, a corresponding controller entity and a network are disclosed.

WO 2013/139980 A1

METHOD FOR SUPPORTING MOBILITY OF END-POINTS IN A NETWORK, CONTROLLER ENTITY AND NETWORK

The present invention relates to a method for supporting mobility of end-points in a network, in particular a TCP/IP network. Furthermore, the present invention relates to a controller entity for executing a method for supporting mobility of end-points in a network. Still further, the present invention relates to a network, in particular a TCP/IP network, for supporting mobility of end-points.

TCP/IP (Transmission Control Protocol / Internet Protocol) network architecture uses a single address to both identify and locate a device on the network. However, modern networks require more flexibility in the handling of the network connections, since new IT technologies are bringing new requirements such as mobility. According to this, a network is required to be able to take care of a device location change. Examples of these technologies are related to cellular phones, Wi-Fi or WLAN (Wireless Local Area Network) enabled devices or virtual devices being able to migrate among different networks, e.g., virtual machines (VM).

Mobility support relates to the problems of identifying and locating a network node's network interface, or more precisely network interface controller (NIC), in a TCP/IP network. In the current TCP/IP architecture a NIC gets an IP (Internet Protocol) address following some configuration procedures, e.g. manually configured or assigned by a network service such as DHCP (Dynamic Host Configuration Protocol). The assigned IP address works both as identifier, i.e. it is used to send packets to that particular addressed network interface, and as locator, i.e. it is used to locate the node on the network. If a network node is moving, a NIC, belonging to such a node, could change its attachment point to the network, hence, the node/NIC should also change the locator address. However, since the assigned IP address is being employed also as identifier, this would have the effect of breaking all the ongoing communications in which the moving node is involved.

Current proposed solutions, such as Mobile IP and Mobile IPv6, require direct involvement of the moving entities, i.e. the end-points, in order to add mobility

support in the network. On the other end, a proposal like Proxy Mobile IP provides mobility without involving end-points by placing mobility aware proxy devices in the network. In any case, in Mobile IP the forwarding of the data packets follows suboptimal routing, since tunnels and/or triangular routing is usually in place.

The limitation of using suboptimal forwarding paths is problematic also in closed environment like data-center infrastructures, where mobility is becoming an important feature as well, because of server virtualization technologies. The usually highly hierarchical architecture of a data-center network makes triangular routing and tunneling solutions really inefficient from the perspective of the traffic flowing in the data-center's network.

To overcome the difficulty of bringing innovation in the network, such as adding mobility support, some initiatives are taking place; one of them, usually identified with the name of Software Defined Network (SDN) led to the definition of a new architecture for the network management. This new architecture adds flexibility to the network by providing programmability of network switches. It is noted that in this context there is no difference among routers and switches, since the behavior of the device depends on how the control-plane operates it. The programmability is provided by separating the control-plane, which is the part of the device that elaborates the forwarding decision logic, from the data-plane, which is the part of the device that is in charge of actually performing the forwarding of packets. While the data-plane is realized on the device itself, e.g. the switch, the control plane is provided by a separated network entity, which is referred to as controller. The controller is in charge of controlling several network devices by running programs written to define the network behavior from a global perspective. This new architecture is supported and realized by the OpenFlow standard, which defines the device programming and configuration model, and the communication protocol between controller and network devices functioning as switches/routers. Thus, OpenFlow is the first standard protocol for controlling flow-based programmable network devices, in particular SDN devices, by providing an interface that allows communication between the control plane and the data plane. The OpenFlow paradigm is described for example in McKeown et al. *"OpenFlow: Enabling*

Innovation in Campus Networks", ACM Computer Communication Review, Vol. 38, Issue 2, pp. 69-74, 2008.

Since the OpenFlow architecture provides just a new management architecture, data packets are still in the form of being defined by protocols of the current TCP/IP network stack. Thus, it is allowed to mix OpenFlow-enabled switches with traditional/legacy switches and routers.

A first example of the application of OpenFlow to solve network mobility issues is described in David Erickson et al., *"A demonstration of virtual machine mobility in an OpenFlow network", Proceedings of ACM SIGCOMM Demo, Seattle, WA, Aug 2008,* where OpenFlow is used to migrate a virtual machine (VM) among different IP subnets by using a network fully composed by OpenFlow switches and rerouting network packets according to the VM location. However, this approach does not provide any solutions to the scalability problems of the control-plane when the involved networks are large, e.g. in large scale networks.

Another approach is described in Farinacci, D., Fuller, V., Meyer, D., and Lewis, D., *"Locator/ID separation protocol (LISP)", Internet-Draft draft-ietf-lisp-13.txt, IETF Secretariat, June 2011*, that is based on the concept of separation among locator and identifier addresses. The LISP architecture uses an "alternate topology" to distribute identifier/locator mapping information among routers in the network. LISP does not provide mobility support natively, while it is added in its "mobility extensions" that need direct involvement of mobile devices in the identifier/locator mapping.

The OpenFlow Controller Platform HyperFlow, described in Amin Tootoonchian and Yashar Ganjali, *"HyperFlow: a distributed control plane for OpenFlow", Proceedings of the 2010 internet network management conference on Research on enterprise networking (INM/WREN'10), USENIX Association, Berkeley, CA, USA, 3-3,* provides scalability at the OpenFlow Controller level by introducing the possibility to scale-up the number of used controllers in a network. Each one of the controllers is linked to some of the switches but still gets a global view of all the managed switches in the network. HyperFlow uses a publish/subscribe system to

propagate network events among controllers, while each controller instance executes the same application. The introduction of a distributed control-plane requires a trade-off on the consistency of the network view that requires some time to converge. Since each controller obtains a complete view of the network, even if more of them are added, each one must be able to handle the complete network state. Thus this approach is also disadvantageous and inefficient.

Furthermore, another controller platform Onix, described in Teemu Koponen et al., *"Onix: A distributed control platform for large-scale production networks", In Operating Systems Design and Implementation (OSDI) October 2010*, provides only a set of features to support the distribution of an application, leaving to the application developer the responsibility to use the provided features appropriately. In particular, Onix defines a network data model NIB that can be accessed and modified in a distributed manner. Applications are in charge of defining the way given information is stored in the NIB, by defining the requirements in terms of durability, consistency, and update rates. According to Onix a completely replicated network view is required which is inefficient and complex.

It is therefore an object of the present invention to improve and further develop a method for supporting mobility of end-points in a network, in particular a TCP/IP network, of the initially described type in such a way that, by employing mechanisms that are readily to implement, an adequate performance for client-server communication is achieved in an efficient way, in particular with regard to scalability issues. Additionally a controller entity and a network for supporting mobility of end-points should be provided.

In accordance with the invention, the aforementioned object is accomplished by a method comprising the features of claim 1. According to this claim a method for supporting mobility of end-points in a network, in particular a TCP/IP network, is claimed, wherein said network includes access networks and a core network, wherein said access networks are connected to said core network via a switch, preferably being configured to use the OpenFlow protocol, wherein said core network provides connectivity among said access networks, wherein an end-point – migrating node – connected to one of said access networks – home network –

migrates to another one of said access networks – foreign network –, wherein one or more controller entities, in particular OpenFlow Controllers, are employed for controlling the switches of said access networks, wherein said one or more controller entities are able to play the roles of

- a home controller that controls a home switch of said home network,
- a foreign controller that controls a foreign switch of said foreign network and/or
- a correspondent controller that controls a correspondent switch of a correspondent network,

wherein, after migration of said migrating node from said home network to said foreign network, a new IP address – locator – belonging to said foreign network is assigned to said migrating node, wherein said locator is employed to find the current location of said migrating node in the network, wherein said migrating node's original IP address – identifier – belonging to said home network is employed to identify said migrating node, and wherein an identifier/locator mapping is employed and reactively updated at the controllers.

Furthermore, the aforementioned object is accomplished by a controller entity comprising the features of claim 15. According to this claim a controller entity, in particular an OpenFlow controller for supporting mobility of end-points in a network is claimed, being configured to play the roles of

- a home controller that controls a home switch of said home network,
- a foreign controller that controls a foreign switch of said foreign network and/or
- a correspondent controller that controls a correspondent switch of a correspondent network.

Still further, the aforementioned object is accomplished by a network comprising the features of claim 16. According to this claim a network, in particular a TCP/IP network, for supporting mobility of end-points, comprising a core network and access networks is claimed, wherein said access networks are connected to said core network via a switch, preferably being configured to use the OpenFlow

protocol, wherein said core network provides connectivity among said access networks, wherein an end-point – migrating node – connected to one of said access networks – home network – migrates to another one of said access networks – foreign network –, wherein one or more controller entities, in particular OpenFlow Controllers, control the switches of said access networks, wherein said one or more controller entities are able to play the roles of

- a home controller that controls a home switch of said home network,
- a foreign controller that controls a foreign switch of said foreign network and/or
- a correspondent controller that controls a correspondent switch of a correspondent network,

wherein, after migration of said migrating node from said home network to said foreign network, a new IP address – locator – belonging to said foreign network is assigned to said migrating node, wherein said locator is employed to find the current location of said migrating node in the network, wherein said migrating node's original IP address – identifier – belonging to said home network is employed to identify said migrating node, and wherein an identifier/locator mapping is employed and reactively updated at the controllers.

According to the invention it has first been recognized that mobility of an end-point and communication quality between end-points in a network can be significantly improved by the end-points being totally unaware of the change of the access network an end-point as migrating node is residing on. Specifically, this is provided by assigning a new IP address belonging to the foreign network to the migrating node in order to work as locator, upon the migrating node is migrated from the home network to the foreign network. This new address is used to find the current location of the migrating node in the network. The original/previous IP address of the migrating node is still used by the migrating node itself and by any node that is communicating with the migrating node, i.e. any correspondent node of a correspondent network. The original IP address of the migrating node is used to identify the migrating node. In accordance with the invention, one or more controlling entities, e.g. OpenFlow Controllers, employ the identifier/locator

mapping information for any migrated node. Thus, appropriate forwarding and/or OpenFlow rules can be installed on involved switches.

Further, it has been recognized that three aspects should be considered from the controller entity perspective: a) the ability to manage a large number of switches, b) the ability to manage a large number of end-point migrations and c) how fast the controller entity is able to react to network events, such as the establishment of a new communication. In accordance with the invention three roles are therefore defined for a controller entity. The roles are defined from the migrating node's perspective, so that any controller can play different roles at the same time, depending on the migrating nodes in the network:

- a home controller that controls a home switch of the home network,
- a foreign controller that controls a foreign switch of the foreign network and/or
- a correspondent controller that controls a correspondent switch of a correspondent network.

Hence, a flexible architecture is provided, wherein the identifier/locator mapping can be efficiently employed and reactively updated at the controllers. Furthermore, in accordance with the invention, the OpenFlow architecture may be used to solve the mobility issue by providing a means to implement the concept of locator address and identifier address, without involvement of end-points.

Thus, the method and the system according to the invention enable an adequate performance for client-server communication in an efficient way, in particular with regard to scalability issues. The present invention does not need a completely replicated network view. Instead, only the minimum required set of needed information, in particular the identifier/locator mapping information, is shared among cooperating controllers, making communication more efficient and the system more scalable.

According to a preferred embodiment the identifier may be used by the migrating node itself and by any correspondent node of the correspondent network that is communicating with the migrating node.

According to a further preferred embodiment the locator may be used in the core network to forward packets to the correct location of the migrating node.

According to a further preferred embodiment it may be provided that for the purposes of the migration set-up, the home controller sends information about the migrating node , e.g. the identifier of the migrating node, to the foreign controller of the foreign network, wherein the foreign controller subsequently generates the locator of the migrating node and sends the locator to the home controller, and wherein the identifier/locator mapping is stored at the home controller and at the foreign controller. Thus, the interactions between the home controller and the foreign controller are performed in an efficient way and, furthermore, the home switch and the foreign switch can be configured with the proper forwarding rules for data packets from a correspondent node of the correspondent network. Both the home controller and the foreign controller have the complete information about the identifier/locator mapping.

Advantageously, OpenFlow rules based on the identifier/locator mapping may be installed on the home switch by the home controller and on the foreign switch by the foreign controller in order to be able to perform the required address resolutions.

With regard to the case that the correspondent node starts a communication to the migrating node, it may be provided that upon reception of a packet that is destined to the identifier of the migrating node that is already migrated to the foreign network, the home controller performs the steps of:

- determining the correspondent controller that is in charge of managing the correspondent network from which the packet comes from,

- informing the correspondent controller about the identifier/locator mapping and designating the correspondent controller in a local list as updated,
- rewriting the destination address of the packet by using the identifier/locator mapping, and
- rerouting the rewritten packet to the migrating node that is already migrated to the foreign network.

When the correspondent node sends a packet to the migrating node, it may always use the identifier address as the packet's destination. Since the corresponding switch does not know yet about the updated identifier/locator mapping, the correspondent switch performs no rewriting on the packet, which is therefore forwarded along the route to migrating node's home network. Once the packet reaches the home switch, it may be intercepted and a message to update the identifier/locator mapping at the correspondent controller is sent. The packet is then forwarded by substituting the identifier with the locator, using triangular routing. Furthermore, it may be necessary to store the information of which correspondent controller has been updated with the identifier/locator mapping information, since subsequent migrations will trigger an update for all the stored correspondent controllers. Otherwise, packets generated by correspondent nodes will continue to be directed to the old migrating node's location.

With regard to the case that the migrating node starts a communication to the correspondent node, it may be provided that upon reception of a packet comprising the identifier as source address, the foreign controller performs the steps of:

- determining the correspondent controller that is in charge of managing the correspondent network to which the packet is destined to,
- checking in a local list indicating updated correspondent controllers if the correspondent controller is designated as updated,
- in case the correspondent controller is not designated as updated, informing the correspondent controller about the identifier/locator

mapping and designating the correspondent controller in the local list as updated,

- rewriting the source address of the packet by using the identifier/locator mapping, and
- rerouting the rewritten packet to the destined correspondent network.

According to a further preferred embodiment the foreign controller may further perform the step of setting up the foreign switch by installing OpenFlow rules for being able to handle directly subsequent packets destined to the same correspondent network.

According to a further preferred embodiment, it may be provided that the home controller informs the foreign controller when the migrating node migrates back from the foreign network to the home network, wherein the foreign controller may send its local list of updated correspondent controllers to the home controller, wherein the home controller informs any updated correspondent controller about the remigration of the migrating node, and wherein the home controller resets the home switch to the default configuration by installing the original OpenFlow rules.

According to a further preferred embodiment, it may be provided that in case the migrating node being already migrated to the foreign network migrates to a new foreign network, the home controller sends information about the migrating node, in particular the identifier of the migrating node, to the new foreign controller of the new foreign network, wherein the foreign controller subsequently generates the new locator of the migrating node and sends the new locator to the home controller, and wherein the identifier/locator mapping is stored at the home controller and at the new foreign controller.

Advantageously, the home controller may inform the foreign controller and any updated correspondent controller about the new migration of the migrating node.

According to a further preferred embodiment, it may be provided that upon the correspondent controller has received updated identifier/locator mapping for the

migrating node, the correspondent controller sets up the correspondent switch by installing OpenFlow rules based on the received identifier/locator mapping.

According to a further preferred embodiment, the proposed architecture is flexible enough to enable a single controller entity of the controller entities to play one, two or all the roles for the same migrating node, for example because the same controller entity is in charge of managing multiple networks.

With regard to guaranteeing also the possibility to adapt the number of used controllers in the network to face the actual network load, it may be provided that a scale-out approach is used, increasing the number of access networks, and consequently reducing the number of nodes per access network. Then, each controller can be assigned at managing a number of access networks, the range is from one to all the access networks, with the aim of sharing the overall load.

There are several ways how to design and further develop the teaching of the present invention in an advantageous way. To this end it is to be referred to the patent claims subordinate to patent claim 1 on the one hand and to the following explanation of preferred embodiments of the invention by way of example, illustrated by the figure on the other hand. In connection with the explanation of the preferred embodiments of the invention by the aid of the figure, generally preferred embodiments and further developments of the teaching will be explained. In the drawing

Fig. 1 is a schematic view illustrating an application scenario according to the present invention,

Fig. 2 is a schematic view illustrating a distributed controller architecture according to an embodiment of the present invention,

Fig. 3 is a sequence diagram illustrating interactions for migration set up between a home controller and a foreign controller according to an embodiment of the present invention,

Fig. 4 is a schematic view illustrating a conceptual overview of a procedure for reactively updating identifier/locator mapping at correspondent controller in case a correspondent node starts the communication,

Fig. 5 is a sequence diagram illustrating interactions of the procedure of Fig. 4,

Fig. 6 is a sequence diagram illustrating the handling of migration of a migrating node from the foreign network back to the home network,

Fig. 7 is a sequence diagram illustrating the handling of migration of a migrating node from the foreign network to a new foreign network,

Fig. 8 is a schematic view illustrating a conceptual overview of a procedure for reactively updating identifier/locator mapping at correspondent controller in case a migrating node starts the communication, and

Fig. 9 is a sequence diagram illustrating interactions of the procedure of Fig. 8.

Embodiments of the invention propose a technology which is designated as Follow-Me Cloud in the following. Follow-Me Cloud (FMC) is a technology that allows transparent migration of services in TCP/IP networks, thanks to the dynamic configuration of a set of coordinated OpenFlow switches located at the edge of the network. FMC overcomes the current TCP/IP architecture mobility limitations by providing both the ability of migrating network end-points and to reactively relocate network services depending on users' locations.

Specifically, FMC enables mobility of network end-points in a TCP/IP network among different IP (Internet Protocol) subnets, both in closed environments, such as data-centers, and on a geographic scale, maintaining active all the ongoing network communications of the moving entity and requiring no modifications to the involved end-points.

FMC is applied to a TCP/IP network in which access networks are connected to a traditional TCP/IP network which can also be designated as core network that provides connectivity among them, through OpenFlow-enabled switches. Each access network corresponds to a single IP subnet. Thus, packets in the access networks are delivered to hosts on the same access network by means of the data-link layer protocol.

Fig. 1 shows an application scenario in the form of an example network with three access networks. FMC is used to maintain ongoing communications and location transparency for a migrating node MN that is changing the access network. Fig. 1 describes also the names used to identify all the network devices involved from the perspective of a migrating node MN. Without loss of generality, the application scenario of Fig. 1 includes a single correspondent node CN, but many of them located at the same or at different access networks can be present; moreover, it is assumed that the migrating node MN has one network interface, even though FMC is applicable also to the case of multiple network interfaces.

According to Fig. 1, by using FMC, the migrating node MN can migrate from an access network A, to an access network B, without changing it's network configuration including, but not limited to IP address and/or Gateway Address. From a network perspective, migrating node MN is totally unaware of the change of the access network it is residing on. All the ongoing communications are kept active, e.g. TCP sessions are not lost.

Any correspondent node, i.e. any node that is on an access network different from network A or network B and that is communicating with migrating node MN is unaware of the migration node MN location change as well.

To provide this result, FMC requires that, after the migration of migrating node MN from network A to network B, a new IP address IP_{b1}, belonging to the network B, is assigned to migrating node MN. This new address IP_{b1} is called “locator” and is used to find the current location of the migrating node MN on the network. The original IP address IP_{a1} of migrating node MN is still used by migrating node MN itself and by any node that is communicating with MN. This last address IP_{a1} is

designated “identifier” and is used to identify migrating node MN. For any migrated node, a FMC OpenFlow controller stores the identifier/locator mapping information. Once the identifier/locator mapping is defined, the FMC OpenFlow Controller configures, with proper rules installation, involved OpenFlow switches, i.e. the home switch HS, the foreign switch FS and any correspondent switch CS.

When the number of managed switches and migrating end-points grows, the OpenFlow Controller (OF-C) can become a bottleneck for the system performance. In particular, three aspects are critical from the controller perspective:

(i) the ability to manage a large number of switches,
(ii) the ability to manage a large number of end-point migrations and
(iii) how fast the controller is able to react to network events, such as the establishment of a new communication.

These issues are influenced by the dimension of the managed network, i.e. higher number of switches and end-points corresponds to a larger network state to maintain at the FMC OpenFlow Controller. When the switches to be managed are distributed on a geographic scale, higher communication delays between them and the controller make the problem even harder, since the control-plane traffic gets delayed accordingly, rendering reactions to events slow and thereby decreasing performance of the system.

An embodiment according to the present invention illustrated by Fig. 2 provides a solution to the scalability problems of the FMC OpenFlow Controller by defining a distributed architecture and a distributed management algorithm.

According to Fig. 2, the defined architecture has multiple controllers and each controller is in charge of managing a subset of all the OpenFlow switches. Assuming the general case in which each one of the switches, i.e. home switch HS, foreign switch FS and correspondent switch CS, is managed by a different controller, the proposed architecture defines three roles for the controllers. The roles are defined from the perspective of the migrating node MN. Thus, any

controller can play different roles at the same time, depending on the migrating nodes in the network:

- Home Controller HC is the controller that controls the OpenFlow switch where the migrating node MN firstly appeared on the network, i.e. the controller that controls the network to which the identifier address IP_{a1} belongs to;
- Foreign Controller FC is the controller that controls the OpenFlow switch where the migrating node MN has migrated to, i.e., the controller that controls the network to which the locator address belongs to;
- Correspondent Controller CC is a controller that controls one or more correspondent switches CS.

The architecture depicted in Fig. 2 is flexible enough to enable a single controller to play one, two or all the roles for the same migrating node, e.g. because the same controller is in charge of managing multiple networks. This approach guarantees also the possibility to adapt the number of used controllers in the network to face the actual network load: it is possible to use a scale-out approach, increasing the number of access networks, and consequently reducing the number of nodes per access network. Then, each controller can be assigned at managing a number of access networks, wherein the range is from one to all the access networks, with the aim of sharing the overall load.

Fig. 3 is sequence diagram illustrating interactions for migration set up between a home controller HC and a foreign controller FC according to an embodiment of the present invention. When migrating node MN migrates to a foreign network, the home controller HC is notified about the migration and informs the foreign controller FC that the migrating node MN is migrating to a network that foreign controller FC itself is managing. Since foreign controller FC is in charge of managing the network to which the locator belongs to, it is leaved to foreign controller FC the responsibility to generate the locator address for migrating node MN. The locator address could be obtained by interacting with a network management system or with a DHCP (Dynamic Host Configuration Protocol) server, for example. Once the locator is defined, it is sent back to the home

controller HC so that both FMC Controllers, i.e. the home controller HC and the foreign controller FC, have the complete information about the identifier/locator mapping to perform the required configurations. So far, just home controller HC and foreign controller FC are informed and configured to support the migration.

Fig. 4 is a schematic view illustrating a conceptual overview of a procedure to reactively update identifier/locator mapping at correspondent controller CC in case a correspondent node CN starts the communication. When a correspondent node CN sends a packet to migrating node MN, correspondent CN always uses the identifier address as the packet's destination. Since the correspondent switch CS does not know yet about the updated identifier/locator mapping, it performs no rewriting on the packet, which is therefore forwarded along the route to migrating node's home network. Once the packet reaches the home switch HS, it is intercepted and a message to update the identifier/locator mapping at the correspondent controller CC is sent. The packet is then forwarded by substituting the identifier with the locator, using triangular routing. Fig. 4 shows an overview of the operations.

Fig. 5 shows the details of the interactions among home controller HC and correspondent controller CC, and thus an embodiment of the invention for the reactive update of identifier/locator mapping at the correspondent controller in case a correspondent node CN starts the communication.

Fig. 6 illustrates a distributed algorithm to handle the migration of a network node from the foreign network back to the home network. When migrating node MN migrates back to its home network, or to a new network illustrated in Fig. 7, all the identifier/locator mapping information distributed at different FMC controllers are no longer valid. As for any other migration node migration, when home controller HC is informed that migrating node MN is migrating, it updates the "old" foreign controller FC about the migrating node MN location change. During this interaction, foreign controller FC sends its local list of updated correspondent controllers to home controller HC. Then, the home controller HC updates the identifier/locator mapping information on any previously updated correspondent controller according the sequence diagram of Fig. 7.

Fig. 8 illustrates a conceptual overview of the procedure to reactively update identifier/locator mapping at correspondent controller in case a migrating node MN starts the communication. When migrating node MN starts the communication with a correspondent node CN, it has to be considered that the foreign switch FS is already applying the identifier/locator mapping. Since, on the other hand, the correspondent switch CS does not know yet about the identifier/locator mapping, the packet would reach the correspondent node CN using the locator address as source, then, correspondent node CN would use the locator address to communicate with the migrated node. If no more migrations happen for migrating node MN, there are no problems with this behavior, but, if a new migration happens, then the locator changes, hence, the communication with the correspondent node CN is lost.

Because of this issue, it should be ensured that any entity always uses the identifier as destination address. To provide the aforementioned property, foreign controller FC has to intercept any packet that is sent by the migrated node and is destined to a correspondent node CN, whose network's FMC controller is still not updated about the identifier/locator mapping for the migrating node. This way, foreign controller FC is able to send updated identifier/locator information for migrating node MN to correspondent controller CC. Further, it is noted that the foreign controller FC does not inform home controller HC about updated correspondent controller CC while migrating node MN is still located in its administrative domain. Instead, foreign controller FC maintains a local list of updated correspondent controllers that is sent back to home controller HC when a new migrating node migration happens. Fig. 8 shows an overview of the operations.

Fig. 9 shows the details of the interactions among foreign controller FC and correspondent controller CC, and thus an embodiment of the invention for the reactive update of identifier/locator mapping at the correspondent controller in case a migrating node MN starts the communication. Thus, Fig. 9 illustrates a distributed algorithm according to the embodiment of Fig. 8 to reactively update

the identifier/locator mapping at correspondent controller CC in case a migrating node starts the communication.

According to the embodiments of the present invention algorithms that are executed by each role may be defined. Since the migrating node's identifier address belongs to a network managed by the home controller HC, the home controller HC is always involved in any migration node migration, and is in charge of managing the information and coordinating the migration for the migrating node MN while it is migrating to other locations.

A controlling entity playing the role of a home controller HC may perform the following algorithm:

1. When MN migrates to a network B according to Fig. 3:
   a. inform FC by providing MN information (e.g. the identifier address) and obtaining the locator address;
   b. set up HS by installing OpenFlow rules defined by FMC;
2. Upon the reception of any packet destined to the identifier address according to Fig. 4 and Fig. 5:
   a. find the CC that is in charge of managing the network from which the packet comes from;
   b. inform the CC about the updated LOC/ID mapping (i.e. identifier/locator mapping) and store the information that CC has been updated;
   c. rewrite the packet destination address using the LOC/ID mapping, and reroute it.
3. When MN migrates back to the network A according to Fig. 6:
   a. inform FC and any updated CC of the migration;
   b. reset HS to default FMC configuration
4. When MN, that is already migrated, migrates to a new network according to Fig. 7:
   a. inform new-FC by providing MN information (e.g. the identifier address) and obtaining the locator address;
   b. inform the old-FC and any updated CC of the new migration;

c. set up HS by installing OpenFlow rules defined by FMC;

A controlling entity playing the role of a foreign controller FC may perform the following algorithm:

1. When a message, informing that MN is migrating to this controller managed network, is received from HC according to Fig. 3:
   a. generate a new locator address;
   b. set up FS installing OpenFlow rules defined by FMC ;
2. Upon the reception of any packet with the identifier address as source address according to Fig. 8 and Fig. 9:
   a. find the CC that is in charge of managing the network to which the packet is destined to;
   b. only if the CC is not in the local list of already updated CC, inform the CC about the updated LOC/ID mapping and store in the local list the information that CC has been updated;
   c. rewrite the packet source address using the LOC/ID mapping, and reroute it;
   d. set up FS with OpenFlow rules, so that subsequent packets destined to the same network are handled directly at FS;
3. When a message, informing that MN is migrating to a new network, is received according to Fig. 6 and Fig. 7:
   a. send all the informations about updated CC back to HC;
   b. delete the configuration entries of the FS related to MN;

A controlling entity playing the role of a correspondent controller FC may perform the following algorithm:

1. Upon reception of a message updating the location information of MN, i.e. providing information like the identifier and locator address:
   a. set up CS installing OpenFlow rules defined by FMC;

It is noted that in several steps of the algorithms there is the need to retrieve a CC network address using a correspondent node's IP address as search key.

Many modifications and other embodiments of the invention set forth herein will come to mind the one skilled in the art to which the invention pertains having the benefit of the teachings presented in the foregoing description and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

Claims

1. Method for supporting mobility of end-points in a network, in particular a TCP/IP network,

wherein said network includes access networks and a core network,

wherein said access networks are connected to said core network via a switch, preferably being configured to use the OpenFlow protocol,

wherein said core network provides connectivity among said access networks,

wherein an end-point – migrating node (MN) – connected to one of said access networks – home network – migrates to another one of said access networks – foreign network –,

wherein one or more controller entities, in particular OpenFlow Controllers, are employed for controlling the switches of said access networks,

wherein said one or more controller entities are able to play the roles of

- a home controller (HC) that controls a home switch (HS) of said home network,
- a foreign controller (FC) that controls a foreign switch (FS) of said foreign network and/or
- a correspondent controller (CC) that controls a correspondent switch (CS) of a correspondent network,

wherein, after migration of said migrating node (MN) from said home network to said foreign network, a new IP address – locator – belonging to said foreign network is assigned to said migrating node (MN),

wherein said locator is employed to find the current location of said migrating node (MN) in the network,

wherein said migrating node's original IP address – identifier – belonging to said home network is employed to identify said migrating node (MN), and

wherein an identifier/locator mapping is employed and reactively updated at the controllers.

2. Method according to claim 1, wherein said identifier is used by said migrating node (MN) itself and by any correspondent node (CN) of said correspondent network that is communicating with said migrating node (MN).

3. Method according to claim 1 or 2, wherein said locator is used in said core network to forward packets to the correct location of said migrating node (MN).

4. Method according to any of claims 1 to 3, wherein, for the purposes of the migration set-up, said home controller (HC) sends information about said migrating node (MN), in particular the identifier of said migrating node (MN), to the foreign controller (FC) of said foreign network, wherein said foreign controller (FC) generates the locator of said migrating node (MN) and sends said locator to said home controller (HC), and wherein the identifier/locator mapping is stored at said home controller (HC) and at said foreign controller (FC).

5. Method according to any of claims 1 to 4, wherein OpenFlow rules based on the identifier/locator mapping are installed on the home switch (HS) by said home controller (HC) and on the foreign switch (FS) by said foreign controller (FC).

6. Method according to any of claims 1 to 5, wherein, upon reception of a packet that is destined to the identifier of said migrating node (MN) that is already migrated to said foreign network, said home controller (HC) performs the steps of:

determining the correspondent controller (CC) that is in charge of managing the correspondent network from which said packet comes from,

informing the correspondent controller (CC) about the identifier/locator mapping and designating the correspondent controller (CC) in a local list as updated,

rewriting the destination address of said packet by using the identifier/locator mapping, and

rerouting the rewritten packet to said migrating node(MN).

7. Method according to any of claims 1 to 6, wherein, upon reception of a packet comprising said identifier as source address, said foreign controller (FC) performs the steps of:

determining the correspondent controller (CC) that is in charge of managing the correspondent network to which the packet is destined to,

checking in a local list indicating updated correspondent controllers if the correspondent controller (CC) is designated as updated,

in case the correspondent controller is not designated as updated, informing the correspondent controller (CC) about the identifier/locator mapping and designating the correspondent controller (CC) in said local list as updated;

rewriting the source address of said packet by using the identifier/locator mapping; and

rerouting the rewritten packet to the destined correspondent network.

8. Method according to claim 7, wherein said foreign controller (FC) further performs the step of setting up the foreign switch (FS) by installing OpenFlow rules for being able to handle directly subsequent packets destined to the same correspondent network.

9. Method according to any of claims 1 to 8, wherein said home controller (HC) informs said foreign controller (FC) when said migrating node (MN) migrates back from said foreign network to said home network,

wherein said foreign controller (FC) sends its local list of updated correspondent controllers to said home controller (HC),

wherein said home controller (HC) informs any updated correspondent controller (CC) about the remigration of said migrating node (MN), and

wherein said home controller (HC) resets the home switch (HS) to the default configuration by installing the original OpenFlow rules.

10. Method according to any of claims 1 to 9, wherein in case said migrating node (MN) being already migrated to said foreign network migrates to a new foreign network, said home controller (HC) sends information about said migrating node (MN), in particular the identifier of said migrating node (MN), to the new foreign controller of said new foreign network, wherein said new foreign controller generates the new locator of said migrating node (MN) and sends said new locator to said home controller (HC), and wherein the identifier/locator mapping is stored at said home controller (HC) and at said new foreign controller.

11. Method according to claim 10, wherein said home controller (HC) informs said foreign controller (FC) and any updated correspondent controller (CC) about the new migration of said migrating node (MN).

12. Method according to any of claims 1 to 11, wherein upon receiving updated identifier/locator mapping for said migrating node (MN), said correspondent controller (CC) sets up the correspondent switch (CS) by installing OpenFlow rules based on the received identifier/locator mapping.

13. Method according to any of claims 1 to 12, wherein a single controller entity of said one or more controller entities plays one, two or all of said roles for said migrating node.

14. Method according to any of claims 1 to 13, wherein the number of access networks is increased in order to reduce the number of end-points per access network, wherein said controller entities are assigned to manage multiple access networks.

15. Controller entity, in particular an OpenFlow controller, for executing a method according to any of claims 1 to 14 for supporting mobility of end-points in a network, being configured to play the roles of

- a home controller (HC) that controls a home switch (HS) of said home network,
- a foreign controller (FC) that controls a foreign switch (FS) of said foreign network and/or
- a correspondent controller (CC) that controls a correspondent switch (CS) of a correspondent network.

16. Network, in particular a TCP/IP network, for supporting mobility of end-points, preferably for carrying out the method according to any one of claims 1 to 14, comprising a core network and access networks,

wherein said access networks are connected to said core network via a switch, preferably being configured to use the OpenFlow protocol,

wherein said core network provides connectivity among said access networks,

wherein an end-point – migrating node (MN) – connected to one of said access networks – home network – migrates to another one of said access networks – foreign network –,

wherein one or more controller entities, in particular OpenFlow Controllers, control the switches of said access networks,

wherein said one or more controller entities are able to play the roles of

- a home controller (HC) that controls a home switch (HS) of said home network,
- a foreign controller (FC) that controls a foreign switch (FS) of said foreign network and/or
- a correspondent controller (CC) that controls a correspondent switch (CS) of a correspondent network,

wherein, after migration of said migrating node (MN) from said home network to said foreign network, a new IP address – locator – belonging to said foreign network is assigned to said migrating node (MN),

wherein said locator is employed to find the current location of said migrating node (MN) in the network,

wherein said migrating node's original IP address – identifier – belonging to said home network is employed to identify said migrating node (MN), and

wherein an identifier/locator mapping is employed and reactively updated at the controllers.

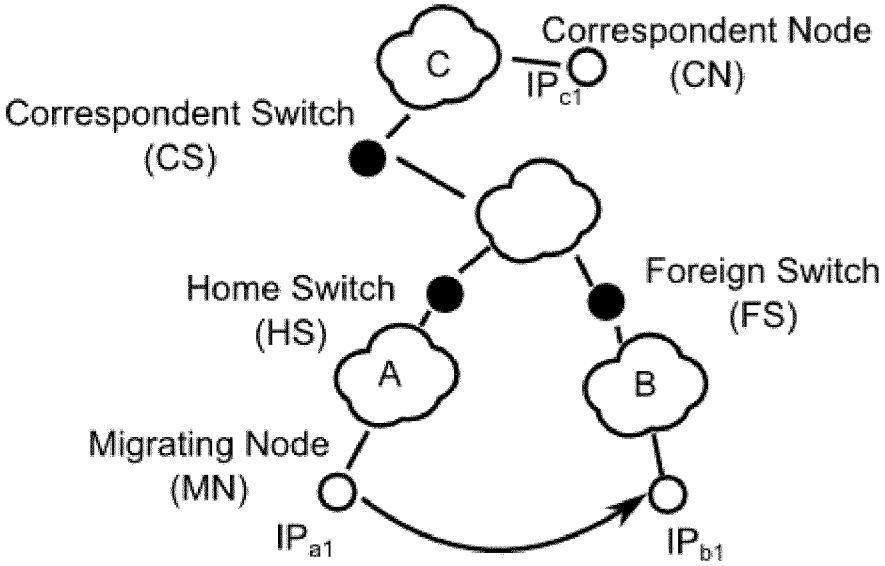
C
Correspondent Node
(CN)
IPc1
Correspondent Switch
(CS)
Home Switch
(HS)
Foreign Switch
(FS)
A
B
Migrating Node
(MN)
IPa1
IPb1

Fig. 1

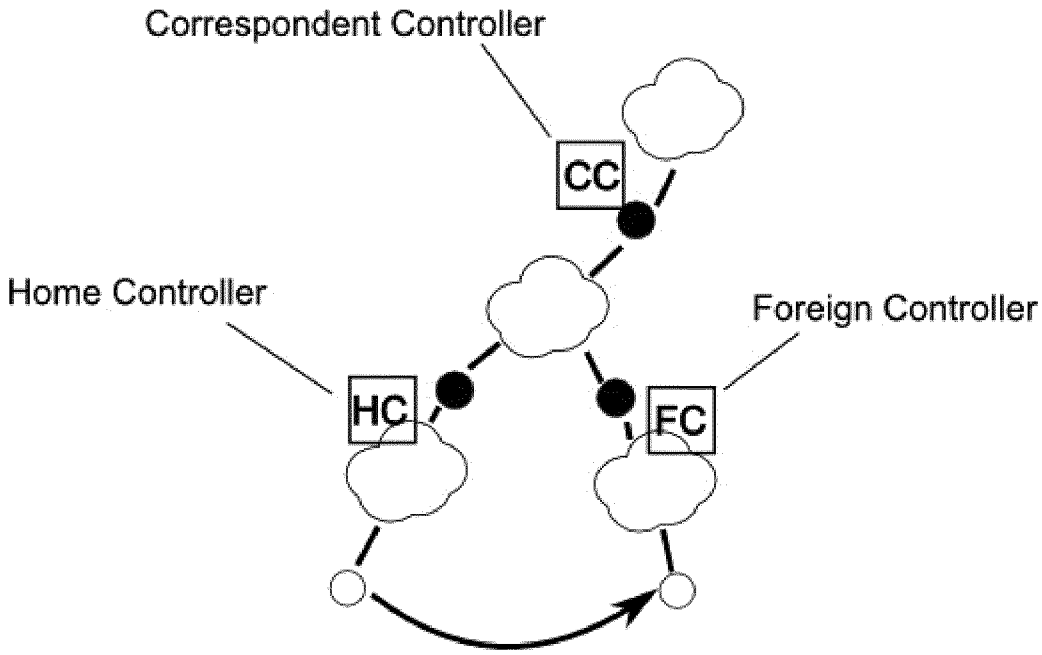
Correspondent Controller
CC
Home Controller
HC
Foreign Controller
FC

Fig. 2

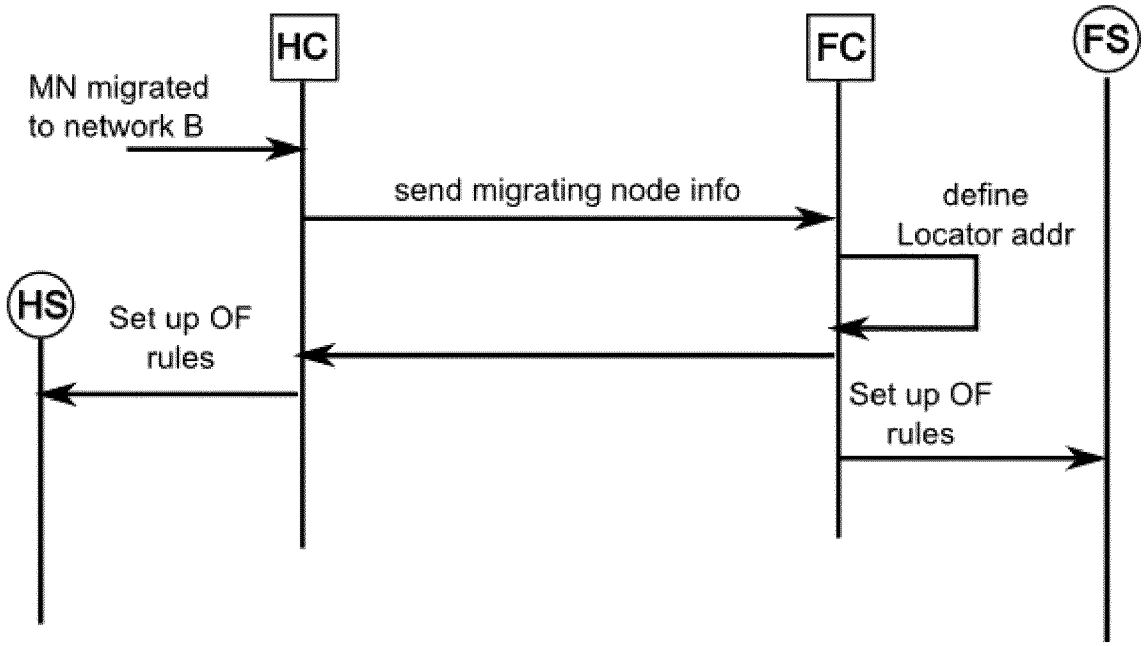
HC
FC
FS
HS
MN migrated
to network B
send migrating node info
define
Locator addr
Set up OF
rules
Set up OF
rules

Fig. 3

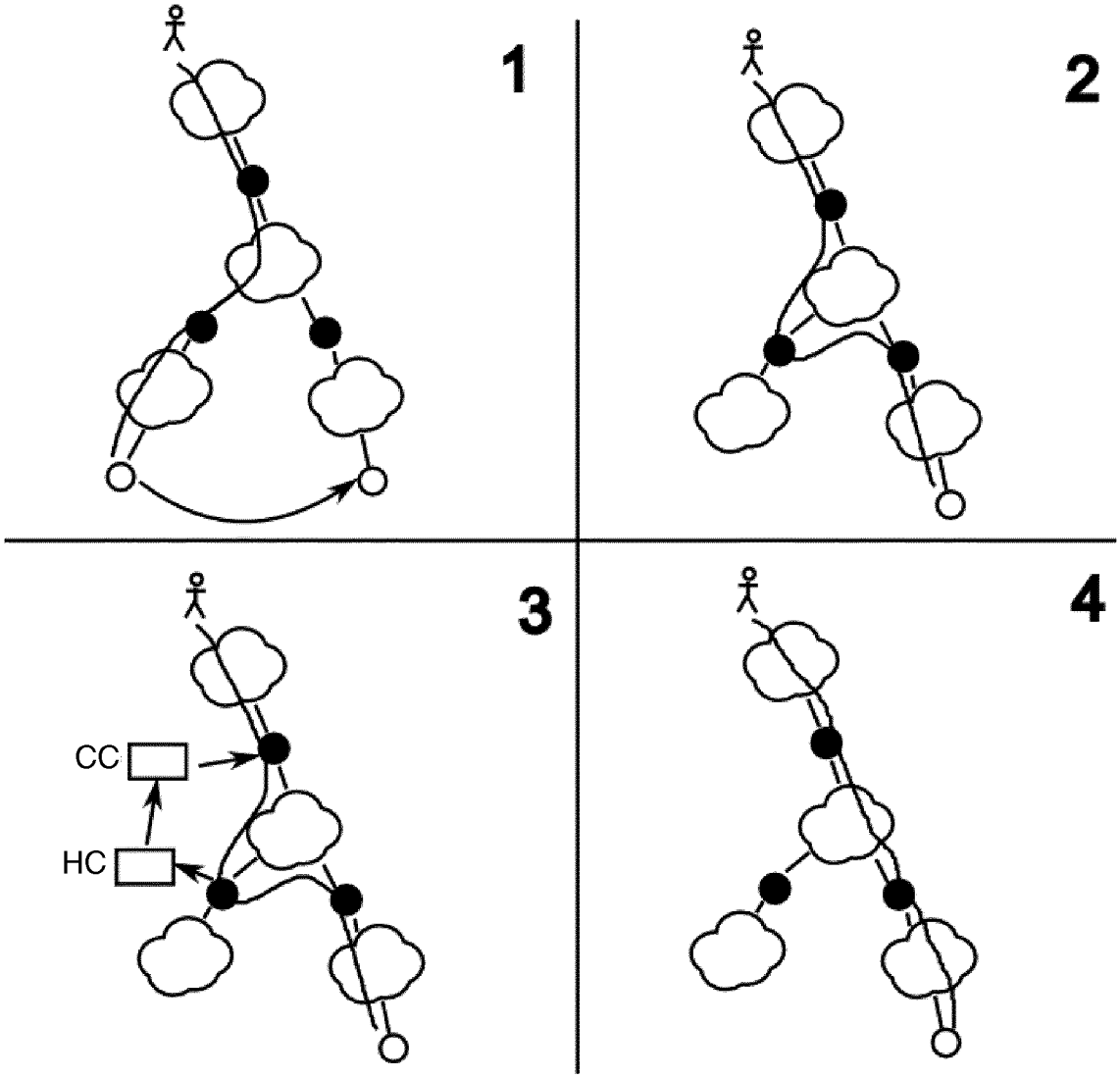

Fig. 4

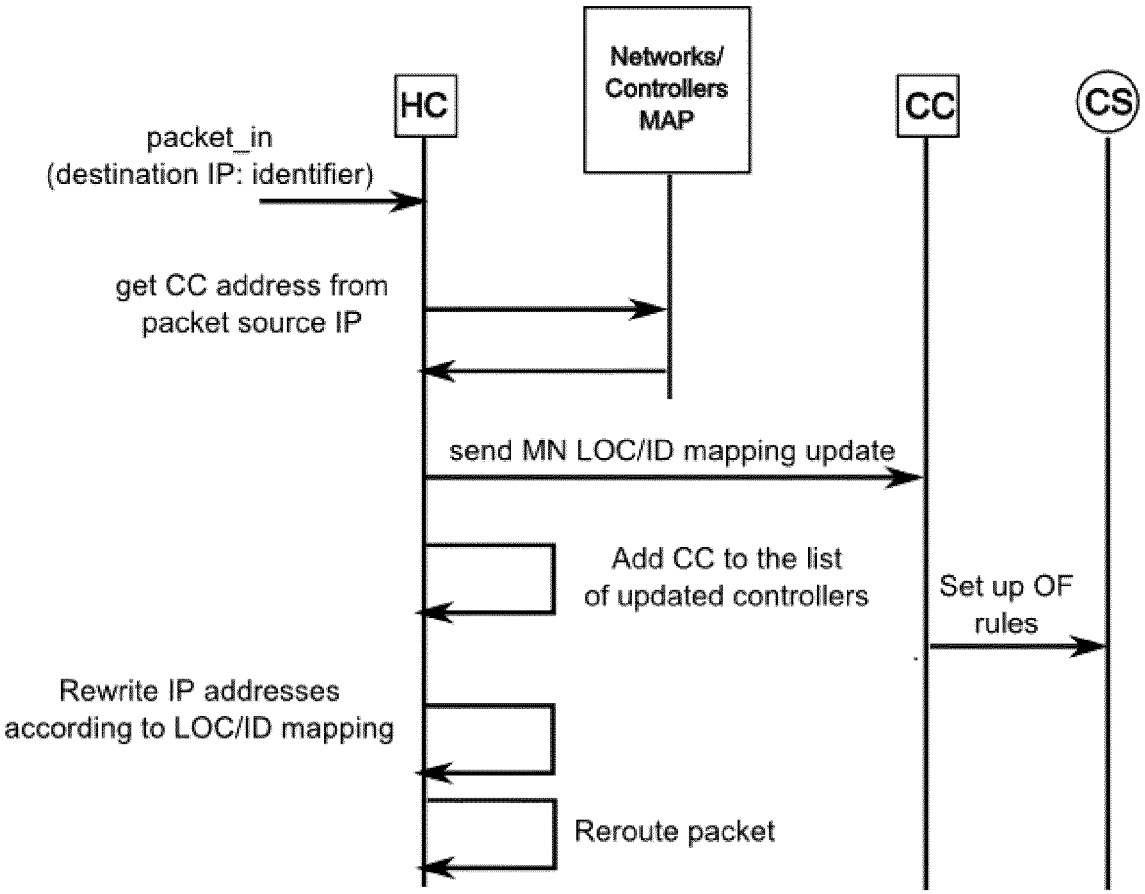
Networks/
Controllers
MAP
HC
CC
CS
packet_in
(destination IP: identifier)
get CC address from
packet source IP
send MN LOC/ID mapping update
Add CC to the list
of updated controllers
Set up OF
rules
Rewrite IP addresses
according to LOC/ID mapping
Reroute packet

Fig. 5

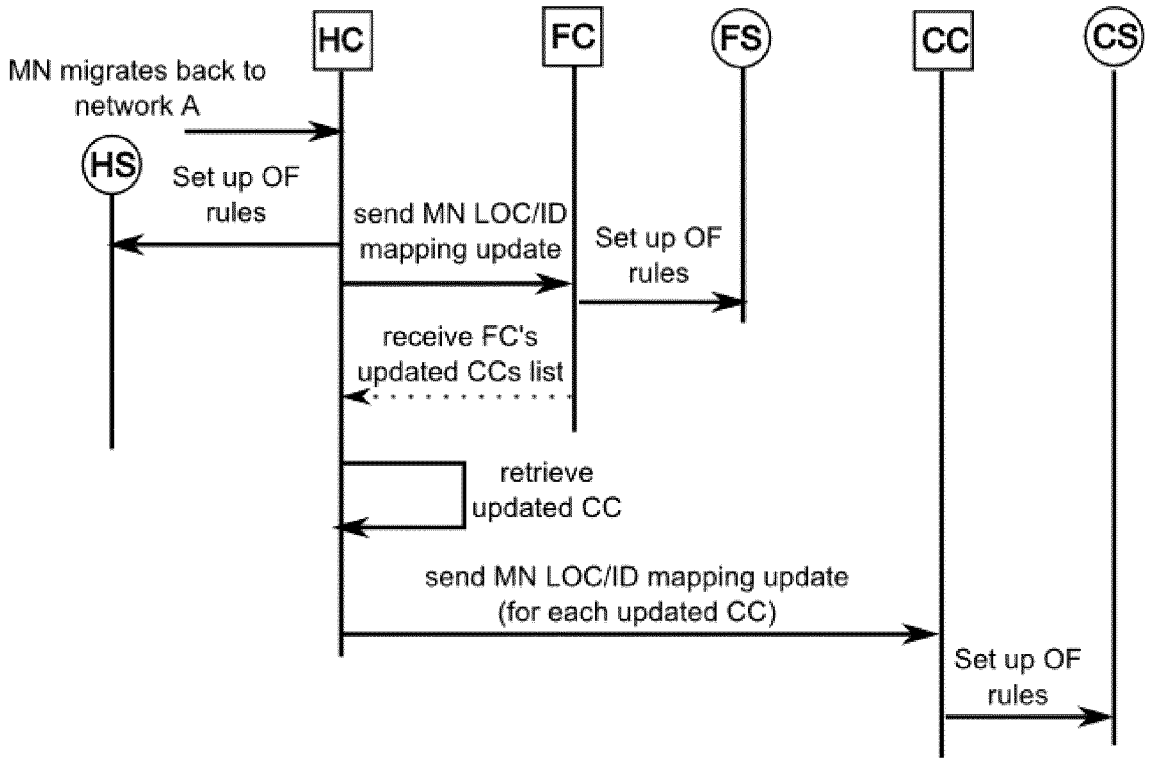
HC
FC
FS
CC
CS
HS
MN migrates back to network A
Set up OF rules
send MN LOC/ID mapping update
Set up OF rules
receive FC's updated CCs list
retrieve updated CC
send MN LOC/ID mapping update (for each updated CC)
Set up OF rules

Fig. 6

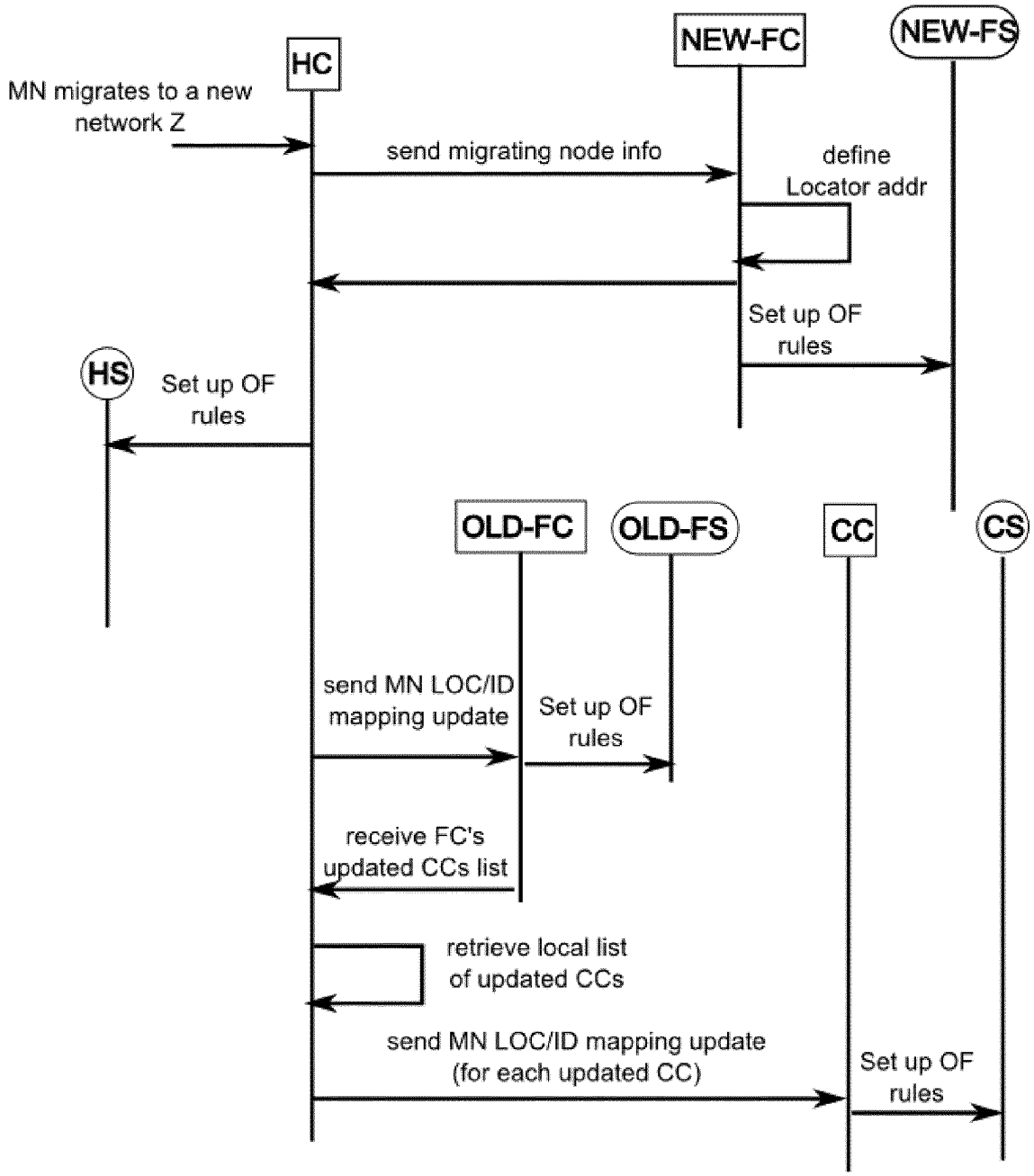
HC
NEW-FC
NEW-FS
MN migrates to a new network Z
send migrating node info
define Locator addr
Set up OF rules
HS
Set up OF rules
OLD-FC
OLD-FS
CC
CS
send MN LOC/ID mapping update
Set up OF rules
receive FC's updated CCs list
retrieve local list of updated CCs
send MN LOC/ID mapping update (for each updated CC)
Set up OF rules

Fig. 7

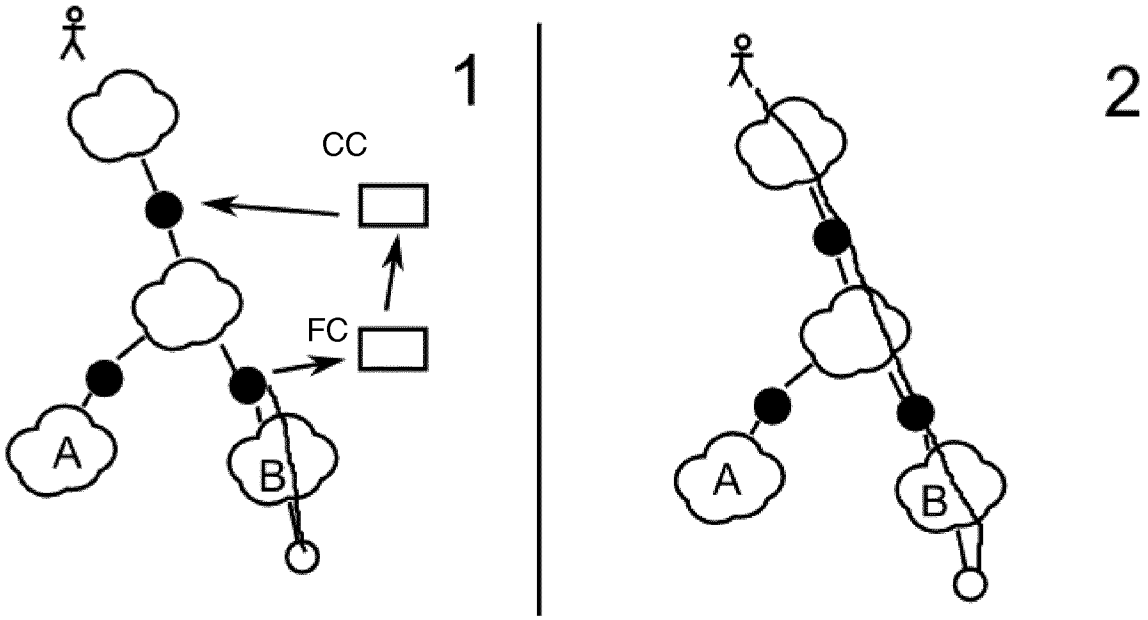

Fig. 8

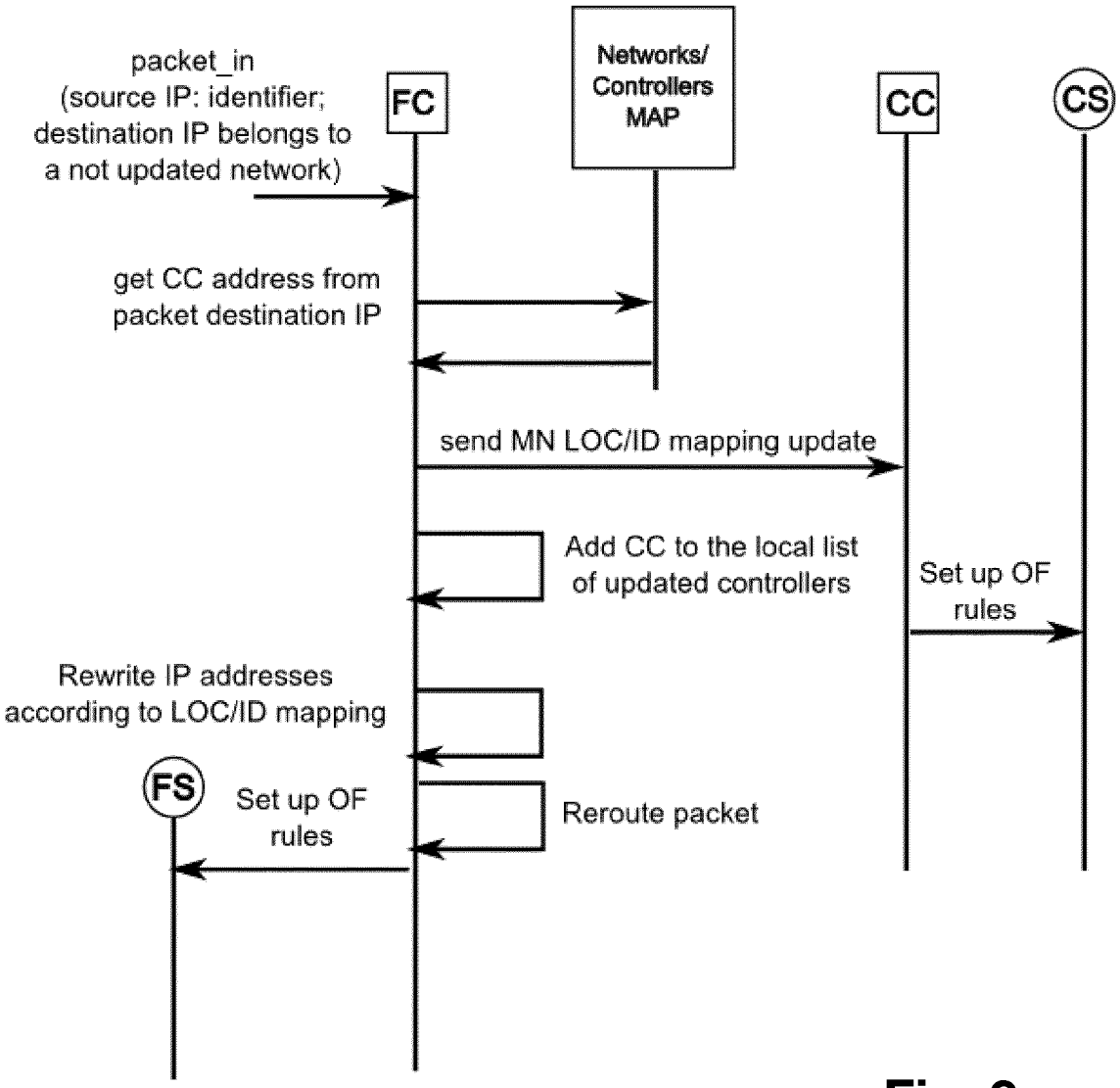
packet_in
(source IP: identifier;
destination IP belongs to
a not updated network)
FC
Networks/
Controllers
MAP
CC
CS
get CC address from
packet destination IP
send MN LOC/ID mapping update
Add CC to the local list
of updated controllers
Set up OF
rules
Rewrite IP addresses
according to LOC/ID mapping
FS
Set up OF
rules
Reroute packet

Fig. 9

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2013/056142

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W8/08 H04W8/12 H04L29/12
ADD. H04W8/04 H04W8/06 H04W80/04

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)
H04W H04L

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)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 2 178 265 A1 (ALCATEL LUCENT [FR]) 21 April 2010 (2010-04-21) paragraph [0013] paragraph [0019] paragraph [0026] - paragraph [0027] -----	1-16
X	EP 2 408 144 A1 (ZTE CORP [CN]) 18 January 2012 (2012-01-18) paragraph [0008] -----	1,16

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* 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	Date of mailing of the international search report
7 June 2013	14/06/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Kahl, Marcus

2

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FARINACCI V FULLER D MEYER D LEWIS CISCO SYSTEMS D: "Locator/ID Separation Protocol (LISP); draft-ietf-lisp-22.txt", LOCATOR/ID SEPARATION PROTOCOL (LISP); DRAFT-IETF-LISP-22.TXT, INTERNET ENGINEERING TASK FORCE, IETF; STANDARDWORKINGDRAFT, INTERNET SOCIETY (ISOC) 4, RUE DES FALAISES CH- 1205 GENEVA, SWITZERLAND, 12 February 2012 (2012-02-12), pages 1-97, XP015080597, [retrieved on 2012-02-12] chapter 10 -----	1-16

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2013/056142

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 2178265 A1	21-04-2010	CN 101730166 A	09-06-2010
		EP 2178265 A1	21-04-2010
		JP 2012506180 A	08-03-2012
		KR 20110069878 A	23-06-2011
		US 2010097994 A1	22-04-2010
		WO 2010043349 A1	22-04-2010
EP 2408144 A1	18-01-2012	CN 101730101 A	09-06-2010
		EP 2408144 A1	18-01-2012
		US 2012040690 A1	16-02-2012
		WO 2010118604 A1	21-10-2010