Datasheet for the decision
of 17 April 2020

Case Number: T 1739/18 - 3.5.05

Application Number: 13832887.7

Publication Number: 2888838

IPC: H04L12/28, H04L9/00, G06F9/455, G06F9/50

Language of the proceedings: EN

Title of invention:
A FRAMEWORK FOR NETWORKING AND SECURITY SERVICES IN VIRTUAL NETWORKS

Applicant:
VMware, Inc.

Headword:
Services in virtual network/VMware

Relevant legal provisions:
EPC Art. 56

Keyword:
Inventive step - (yes)

Decisions cited:
Catchword:
Case Number: T 1739/18 - 3.5.05

DEcision
of Technical Board of Appeal 3.5.05
of 17 April 2020

Appellant: VMware, Inc.
(Applicant) 3401 Hillview Avenue
Palo Alto, CA 94304 (US)

Representative: Appleyard Lees IP LLP
15 Clare Road
Halifax HX1 2HY (GB)

Decision under appeal: Decision of the Examining Division of the European Patent Office posted on 9 February 2018 refusing European patent application No. 13832887.7 pursuant to Article 97(2) EPC.

Composition of the Board:
Chair: A. Ritzka
Members: P. Cretaine
D. Prietzel-Funk
Summary of Facts and Submissions

I. This appeal is against the decision of the examining division, posted on 9 February 2018, refusing European patent application No. 13832887.7. The application was refused for lack of inventive step (Article 56 EPC) of a main and an auxiliary request over the disclosure of


The following document is cited in the description:

"Scalable Cloud Networking with CISCO Nexus 1000V Series Switches and VXLAN", CISCO, Inc., White Paper, 2012. This document will be denominated "CISCO paper".

II. Notice of appeal was received on 6 April 2018 and the appeal fee was paid on the same day. The statement setting out the grounds of appeal was received on 18 June 2018. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the main request or the auxiliary request on which the decision was based. It also requested oral proceedings as an auxiliary measure.

III. A summons to oral proceedings was issued on 2 March 2020. By notification sent on 8 April 2020, the board informed the appellant that the oral proceedings were cancelled.

IV. Claim 1 of the main request reads as follows:

"A virtual infrastructure (102), comprising:
a plurality of hosts (110, 114) each having a virtual machine (105) executing therein and a virtual switch (130) in a virtual network (132); and
a virtual machine management server, VMMS (125),
characterised in that the VMMS (125) is configured to:
receive a service definition from a network service (150) offered for a physical network, the service definition including information about the network service (150) and configuration instructions for configuring a host (110) of the plurality of hosts (110, 114) to use the network service (150);
create one or more service profiles for the network service (150) based on the service definition of the network service (150), each of the one or more service profiles including the information about the network service (150) and the configuration instructions, and including parameters of the network service (150) for use on a virtual machine (105) of said plurality of virtual machines (105);
register the network service (150) by adding the one or more service profiles to a directory (170) of network services, the directory (170) indicating whether the service profile is available to the virtual machines (105); and
in response to receiving a selection of the service profile from the directory (170) and a selection of one of the virtual machines (105), enable the network service (150) for the selected virtual machine (105) by using the configuration instructions to configure the virtual switch (130) of the host (110) of the selected virtual machine (105) with rules and/or filters that forward packets from the selected virtual machine (105) to the network service (150) of the selected service profile.
The main request comprises further independent claims directed to a corresponding computer-readable storage medium (claim 7) and a corresponding method of registering a network service on a virtual network (claim 11).

Due to the outcome of the appeal, there is no need to give details of the claims of the auxiliary request.

**Reasons for the Decision**

1. The appeal is admissible (see point II above).

2. Prior art

2.1 D1 describes a virtual lab (see [0003]) which enables application development and test teams to create and deploy network configurations. D1 addresses, inter alia, the issue that two virtual machines (VMs) should not be instantiated with the same IP address on a local area network (see [0004]). Figure 1 shows hosts 106 supporting VMs 108. The virtual infrastructure 102 is managed by the virtual infrastructure server 104 (see [0022]). A virtual lab server 112 (see [0025]) manages and deploys virtual machine configurations into the hosts 106. Figure 7 shows how the virtual lab configuration 712 is created, by bringing a network template 708, which is a specification of network settings, together with a VM template 710 which specifies information relevant to a particular virtual machine (see [0042] to [0044]). Thus, each VM is configured with proper VM network connectivity, including specifically assigned local IP addresses for each VM, thereby avoiding the resource contention issue.
of two VMs having the same local IP address. A default
gateway (see [0034], 802 in Figure 8) is an element of
network information which is derived from the relevant
VM template 710 for each VM 108 (see [0034]). The
default gateway is determined by the primary Network
Interface Controller NIC setting for the virtual
machine and ais identified by the public IP address
10.6.1 in Figure 8. The default gateway is thus a
network configuration of the virtual machine, and not a
configuration of the host, that makes it possible to
allow the virtual machine to reach a wider network,
e.g. the internet.

2.2 The CISCO paper discloses a further development of the
VLAN standard IEEE802.1Q, denominated "VXLAN", aimed at
expanding the scalability of a virtual network beyond
the limit imposed by the 12-bit VLAN ID. In this
scheme, the original packet issued by a virtual
machine, i.e. the original Ethernet frame, is
encapsulated with an additional outer wrapper (see
VXLAN Encapsulation in Figure 1). For VXLAN traffic to
use network services on physical devices, such as a
physical firewall, the traffic needs to go through a
VXLAN gateway, as shown in Figure 4. However, the
original destination and source addresses (Inner MAC DA
and Inner MAC SA, respectively, in Figure 1) are now
hidden within the original Ethernet frame and obscured
by the encapsulation layer. Inspecting the presented
outer destination and source addresses (Outer MAC DA
and Outer MAC SA, respectively, in Figure 1) thus does
not reveal the original inner destination or source
addresses. As a result, the packet may pass through the
network according to the outer addresses of the
encapsulation and, in doing so, it bypasses the network
services on the underlying physical network.
Conversely, the virtual machines in the virtual network
may be unaware of the existence of the network services because the network services are not addressable by the VXLAN encapsulation and thus not visible for the virtual machines.

3. Inventive step

3.1 D1 was considered as the closest prior art in the impugned decision.

The constitutive elements of the virtual infrastructure defined in the preamble of claim 1 were read onto the elements of the virtual lab of D1, shown in Figure 1. In particular, the hosts of claim 1 were read into the hosts 108 of D1, the virtual machine of claim 1 was read into a virtual machine 108 of D1, and the virtual machine management server (VMMS) was read onto the virtual lab server 112 of D1.

The board agrees with the appellant that none of the characterising features of claim 1 is disclosed in D1. These features specify that the virtual machine management server is configured to:

(a) receive a service definition from a network service offered for a physical network, the service definition including information about the network service and configuration instructions for configuring a host of the plurality of hosts to use the network service;

(b) create one or more service profiles for the network service based on the service definition of the network service, each of the one or more service profiles including the information about the network service and the configuration instructions, and including
parameters of the network service for use on a virtual machine of the plurality of virtual machines;

(c) register the network service by adding the one or more service profiles to a directory of network services, the directory indicating whether the service profile is available to the virtual machines; and

(d) in response to receiving a selection of the service profile from the directory and a selection of one of the virtual machines, enable the network service for the selected virtual machine by using the configuration instructions to configure the virtual switch of the host of the selected virtual machine with rules and/or filters that forward packets from the selected virtual machine to the network service of the selected service profile.

The impugned decision interpreted the gateway, also denominated "default gateway", mentioned in D1 in paragraphs [0034], [0041], [0050], [0059] and [0062] and shown in Figures 7 and 8, as a network service. However, the board shares the view of the appellant that the default gateway does not represent a network service in the context of the whole application. Indeed, it was common knowledge at the priority date of the application in 2012 that every network device with access to the outside world is configured with a gateway address. In a VLAN, the gateway is the "next hop" address of a router for packets with destination addresses outside the local network segment, so that a virtual machine can send packets to the gateway router, which then forwards them and makes it possible for them to be routed out to the wider network, such as the internet. On the other hand, a network service is a functionality provided by an entity in the network to
computers which have access to the network, for instance through a gateway. This common understanding is used throughout the disclosure of the application, wherein a non-exhaustive list of examples consisting in load balancers, firewalls and virus scanners is recurrently mentioned in the description.

On the contrary, the default gateway in D1 is a configuration of the virtual machine - not a configuration of the host computer - which allows the virtual machine to reach a wider network. The default gateway is clearly defined in paragraph [0034] of D1 as an element of network information which is determined by the primary NIC setting for the virtual machine and identified by a public IP address.

Therefore, the presence of a network service which announces its own existence itself to the virtual machine management server of the virtual network, as defined in feature (a), is not disclosed in D1. Also, neither the creation of service profiles nor their registration in a directory by the virtual machine management server, as defined in features (b) and (c), are to be found in D1. Given that there is no directory of network services in D1, there can be no selection from it as defined in feature (d).

3.2 The technical effect of the characterising features (a) to (d) of claim 1 is that the network services offered on the physical network are now made available in a uniform manner for use by the virtual machines of the virtual network, and vice versa, and are managed by the VMMS 125 in relation to the ability and configuration of those services and to the needs of the VMs.

The objective technical problem can therefore be
formulated as how to modify the system of D1 to include a uniform method of allowing virtual machines in a virtual network to consume network services originally offered to physical networks.

D1 contains no explicit or implicit disclosure relating to how network services originally offered to physical networks could be enabled for use by VMs. As detailed above, D1 only contains disclosures relating to configuring VMs with specific network hardware-related information, such as which primary NIC a particular VM should use, and has no teaching relating to software network services. The skilled person would thus find no pointer in D1 towards the claimed solution.

For these reasons, the board holds that the subject-matter of claim 1 involves an inventive step over the disclosure of D1 (Article 56 EPC).

3.3 The CISCO paper, which was not addressed in the impugned decision, describes that some services are able to communicate with virtual networks of the VXLAN type, e.g. through the VXLAN Gateway mentioned in relation to Figure 4. However, this document does not provide a method for uniformly introducing and consuming network services within virtual networks, comprising, in particular, the announcement by a network service of its own existence itself to the virtual network management server, the creation of service profiles, their registration in a directory, and the configuration of the virtual switch of the host of the virtual machine by the virtual network management server, as defined by the characterising features of claim 1. The appellant plausibly argued that the virtual infrastructure defined in claim 1, when applied to a VXLAN network, additionally solves
the "visibility" problem that, due to the encapsulation of the Ethernet frame, the virtual network may be unaware of services existing in the physical network.

For these reasons, the board holds that the subject-matter of claim 1 also involves an inventive step over the disclosure of the CISCO paper (Article 56 EPC).

3.4 Independent claims 7 and 11 contain the same features as claim 1 but expressed in terms of a computer-readable storage medium and a method, respectively. Therefore, these claims also meet the requirements of Article 56 EPC. Claims 2 to 6, 8 to 10 and 12 are dependent claims and, as such, also meet the requirements of Article 56 EPC.
Order

For these reasons it is decided that:

1. The decision under appeal is set aside.

2. The case is remitted to the examining division with the order to grant a patent on the basis of the following documents:
   - Claims 1 to 12, filed as the main request by letter dated 11 December 2017;
   - Description:
     - pages 5 and 7 to 9 as originally filed;
     - pages 1 to 4, 6 and 10 as filed by letter dated 11 December 2017;
   - Drawing sheets 1/2 to 2/2 as originally filed.

The Registrar: The Chair:

C. Rodriguez Rodriguez A. Ritzka

Decision electronically authenticated