(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 028 794 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
25.02.2009 Bulletin 2009/09

(51) Int Cl.:
H04L 12/28 *(2006.01)* ***H04L 12/56*** *(2006.01)*

(21) Application number: **07114926.4**

(22) Date of filing: **24.08.2007**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC MT NL PL PT RO SE SI SK TR
Designated Extension States:
AL BA HR MK RS

(71) Applicant: **Hopling Group B.V.**
1322 BC ALMERE (NL)

(72) Inventors:
- **Stam, Michel**
  3453 TJ, De Meern (NL)
- **Muns, Willem Sebastiaan**
  1271 NJ, Huizen (NL)

(74) Representative: **van Looijengoed, Ferry Antoin Theodorus et al**
De Vries & Metman
Overschiestraat 180
1062 XK Amsterdam (NL)

(54) Network discovery protocol

(57) The invention provides a network discovery protocol in a layer 2 frame comprising a Sub-network Access Protocol, header. The invention enables discovery protocol information elements to be transmitted from a first communication device to a second communication device in a secure and enhanced manner.

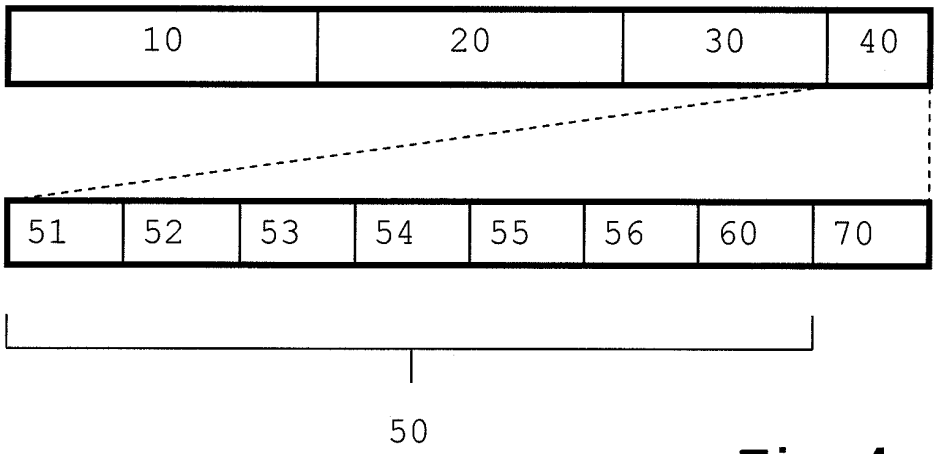

Fig. 4

EP 2 028 794 A1

Description

Field of the invention

[0001] The invention relates to a method for a first communication device to transmit network discovery information to a second communication device, a method for a second communication device to process network discovery information, a first communication device arranged for transmitting network discovery information to a second communication device, a second communication device arranged for processing network discovery information, and a layer 2 network discovery protocol.

Background of the invention

[0002] A growing popularity of wireless networking opens up a new market for service providers to offer Internet access to users. Mesh networking allows a service provider a way of extending the coverage area of a wireless network without the need of a wired distribution system. Products that offer mesh functionality often require manual configuration on the part of the service provider. This requires knowledge of Wi-Fi networking in general and specific knowledge about the products. This knowledge is not always available, which complicates the installation process.

[0003] It is known that networks can be configured using discovery protocols. Examples of such protocols are Cisco Discovery Protocol (CDP), Foundry networks FDP and IEEE 802.1AB. A drawback of these discovery protocols is that they carry information in an unsecured manner, i.e. it is possible to tap and interpret network traffic that is sent using discovery protocols.

[0004] Ethernet is a known protocol on layer 2 of the OSI model. The layer 2 Ethernet implementation known as "Ethernet IEEE 802.3 SNAP" defines a frame format that enables protocol extensions to the Ethernet standard. Hereto the Ethernet IEEE 802.3 SNAP frame includes an IEEE Organizationally Unique Identifier (OUI) followed by a 2-bytes Protocol ID, indicating the presence of a protocol extension.

[0005] US 7,099,295 B1 discloses an apparatus and method for bridging a wired network and wireless devices. A bridge apparatus is provided for interfacing or bridging between a wired network having wired communication devices and wireless devices. US 7,099,295 B1 does not disclose a secure discovery protocol.

Summary of the invention

[0006] It is an object of the invention to provide a secure discovery protocol with enhanced functionality.

[0007] According to an aspect of the invention a method is provided for a first communication device to transmit network discovery information to a second communication device. The method comprises the step of providing a layer 2 frame comprising a sub-header, wherein the sub-header comprises an identifier field indicating the presence of a discovery protocol in the layer 2 frame. Ethernet can be used as a layer 2 frame and IEEE 802.2 Sub-network Access Protocol (SNAP) can be used as sub-header. Alternatively, any other OSI layer 2 protocol supporting a sub-header such as LAN and Frame Relay, or any other OSI layer 2 protocol supporting protocol extensions can be used. The method further comprises the steps of providing at least one discovery protocol information element comprising network discovery information and encrypting the at least one discovery protocol information element. This advantageously enables discovery information to be included in the layer 2 frame in a secure manner. Preferably a shared secret is used for encryption, but the invention is not limited to the use of a shared secret. It is possible to use e.g. public key cryptography or any other form of cryptography. The method further comprises the steps of providing a discovery protocol header and the encrypted at least one discovery protocol information element to the layer 2 frame, and transmitting the layer 2 frame to the second communication device. This advantageously enables the transmission of the discovery information in a secure manner.

[0008] The embodiment of the invention as defined in claim 2 advantageously enables verification of decryption at a receiver. After decryption, verifying the checksum will ensure that the packet has been decrypted correctly. The checksum is placed within the encrypted part of the data packet to advantageously prevent giving away information which can be used to crack the encryption key.

[0009] The embodiment of the invention as defined in claim 3 advantageously allows for various information fields with information for the second communication device.

[0010] The embodiment of the invention as defined in claim 4 advantageously enables differentiation of network discovery information.

[0011] The embodiment of the invention as defined in claim 5 advantageously enables transmission of discovery information in fragmented packets, i.e. when there are more discovery protocol information elements than can be fit in a single layer 2 frame. Ethernet e.g. has a maximum frame size of 1536 bytes. It should be acknowledged that this embodiment may or may not use encryption of the information element.

[0012] The embodiment of the invention as defined in claim 6 advantageously enables the transmission of the discovery information in a secure manner.

[0013] The embodiment of the invention as defined in claim 7 advantageously increases security by removing repetition patterns in the order of discovery protocol information elements by the shuffling step. This makes it more difficult for malicious interceptors to decrypt packets. Moreover, the grouping step advantageously minimizes the amount of layer 2 frames needed to transmit all discovery protocol information elements. Preferably shuffling and/or grouping are performed prior to encryption.

[0014] The embodiment of the invention as defined in claim 8 advantageously enables encryption algorithms to receive an aligned block of input data which is then subsequently encrypted using a block cipher.

[0015] The embodiment of the invention as defined in claim 9 advantageously improves the strength of encryption.

[0016] The embodiment of the invention as defined in claim 10 advantageously enables a unique identification of a set of layer 2 frames belonging together.

[0017] The embodiment of the invention as defined in claim 11 advantageously enables management applications to address one device. This is e.g. achieved by using an unicast address as a destination address in the layer 2 frame.

[0018] The embodiment of the invention as defined in claim 12 advantageously prevents having to process acknowledgement packets every time the layer 2 frame with discovery information is sent. Advantageously, by periodically resending the layer 2 frame the delivery of the layer 2 frames can be ensured.

[0019] According to an aspect of the invention a method is provided for a second communication device to process network discovery information. The method comprises the step of receiving from a first communication device at least one encrypted discovery protocol information element transmitted by the first communication device according to the method, or one of its embodiments, as described above. The method further comprises the steps of decrypting the at least one discovery protocol information element and configuring the second communication device using the received network discovery information. This advantageously enables the second communication device to be configured using enhanced discovery information that is exchanged in a secure manner between the first communication device and the second communication device. Alternatively or in addition the method comprises the step of storing the received network discovery information for network management purposes. This advantageously enables in the second communication device management and tracking of the status of the first communication device using enhanced discovery information that is received in a secure manner from the first communication device.

[0020] The embodiment of the invention as defined in claim 14 advantageously enables the detection of devices that are down temporarily and/or permanently.

[0021] According to an aspect of the invention a first communication device is provided arranged for transmitting network discovery information to a second communication device. The first communication device comprises a processor, a memory and a transmitter to advantageously perform one or more of the steps of the method performed by the first communication device as described above.

[0022] According to an aspect of the invention a second communication device is provided arranged for processing discovery information. The second communication device comprises a processor, a memory and a transmitter to advantageously perform one or more of the steps of the method performed by the second device as described above.

[0023] According to an aspect of the invention a layer 2 discovery protocol in a layer 2 frame is provided. Ethernet can be used as the layer 2 protocol. Alternatively, any other OSI layer 2 protocol supporting a sub-header such as the Sub-network Access Protocol (SNAP), e.g. LAN and Frame Relay, or any other OSI layer 2 protocol supporting protocol extensions can be used. The discovery protocol advantageously comprises the discovery protocol header and discovery protocol information elements as described above.

[0024] The invention can advantageously be used in wireless mesh networks, but is not limited to use in such networks. The invention can be used in any network that is capable of transporting packets in accordance with the IEEE 802.2 Sub-network Access Protocol (SNAP), such as an Ethernet network or IEEE 802.16 Wi-MAX network, or more generally in any network capable of layer 2 protocol extensions.

[0025] Further advantageous embodiments and advantages of the invention are defined in the dependent claims and the following description.

[0026] The invention will be further illustrated with reference to the attached drawings, which schematically show preferred embodiments according to the invention. It will be understood that the invention is not in any way restricted to these specific and preferred embodiments.

Brief description of the drawings

[0027] The invention will be explained in greater detail by reference to exemplary embodiments shown in the drawings, in which:

Fig.1 shows a simplified example of a network architecture;

Fig.2 shows the first four layers of the Open Systems Interconnection basic reference model (OSI model), as known in the prior-art;
Fig.3 shows the frame format of a layer 2 Ethernet implementation known in the prior art as "Ethernet IEEE 802.3 SNAP";
Fig.4 shows a discovery protocol frame of an exemplary embodiment of the invention;
Figs.5a-5c shows shuffling and grouping of discovery protocol information elements of an exemplary embodiment of the invention;
Fig.6 shows a mesh network of an exemplary embodiment of the invention.

Detailed description of the drawings

[0028] The invention enables a secure exchange of information between devices to enable a device to configure itself for optimal communication with a neighbouring device. As an additional benefit, it allows mechanics and NOC (Network Operating Centre) technicians to get a view of the network from the perspective of the devices (which is not necessarily the network as its designer intended), as well as to obtain information about the availability or performance of a device.

[0029] The network protocol according to the invention is a socalled discovery protocol for exchanging network discovery information.

[0030] The discovery protocol is designed such that it fulfils requirements of efficiency, flexibility and security.

[0031] With regard to efficiency, the discovery protocol is designed to not overly affect the network it is providing information about. If the amount of overhead in the discovery protocol or the amount of information sent for management purposes takes up a significant amount of bandwidth it would invalidate its purpose. Secondly, the discovery protocol is light-weight. A complex protocol would consume too much system resources.

[0032] With regard to flexibility, the discovery protocol is designed to be future-proof. In other words, it is possible to extend the discovery protocol beyond its initial design, adding information to it which was not included in the original specification. Secondly, to enable servers to support wireless access gateways, the discovery protocol can be used on both wired and wireless networks. IP connectivity is not always available on a device; therefore the discovery protocol is not dependent on the IP protocol.

[0033] Especially with multiple wireless networks coexisting, care must be taken that information from one wireless network does not reach another wireless network. With regard to security, due to the sensitive nature of some of the data in the information exchanged by the discovery protocol, the discovery protocol according to the invention prevents unauthorized access to the data.

[0034] Fig.1 shows a simplified example of a wireless network that is connected to a fixed network. In Fig.1 a first communication device 1000 is wirelessly connected to a second communication device 2000. The first communication device and second communication device are e.g. wireless routers, base stations or gateways. Together, the first communication device 1000 and the second communication device 2000 form a wireless network. The first communication device comprises a transmitter 1001 and a memory 1003, which are connected to a processor 1002. Using the memory 1003 and processor 1002 the first communication device 1000 is capable of processing information and transmitting the information using the transmitter 1001. The second communication device comprises a receiver 2001 and a memory 2003, which are connected to a processor 2002. Using the memory 2003 and processor 2002 the second communication device 2000 is capable of receiving information using the receiver 2001 and processing the information. The first communication device 1000 has a connection to the Internet 3000 through a fixed link. A computer 4000 at a NOC (Network Operating Centre) can communicate with the first communication device 1000 via a fixed network 3000.

[0035] It will be understood that instead of wireless communication devices fixed-line communication devices can be used. The communication devices then form a fixed-line network instead of a wireless network. Hybrid networks comprising both wireless and fixed-line communication devices are also possible.

Transport mechanism

[0036] In Fig.2 the Open Systems Interconnection basic reference model (OSI model), as known in the prior-art, is shown for layers 1-4.

[0037] The transport layer 4 provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The transport layer 4 controls the reliability of a given link through flow control, (de)segmentation, and error control. The Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are examples of transport layer protocols.

[0038] The network layer 3 provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks while maintaining the quality of service requested by the transport layer 4. The network layer 3 performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors. The best known example of a layer 3 protocol is the Internet Protocol (IP).

[0039] The data link layer 2 provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the physical layer 1. This layer manages the interaction of devices with a shared medium. It arranges bits from the physical layer into logical chunks of data, known as frames. At layer 2 bridges and switches operate. Connectivity is provided only among locally attached network nodes forming layer 2 domains for unicast or broadcast forwarding. Other protocols may be imposed on the data frames to create tunnels and logically separated layer 2 forwarding domain. Ethernet (IEEE 802.3) is a known example of a layer 2 protocol.

[0040] The physical layer 1 defines the electrical and physical specifications for devices. In particular, it defines the relationship between a device and a physical medium. This includes the layout of pins, voltages, and cable specifications. Hubs, repeaters and network adapters are examples of physical-layer devices.

[0041] The layer 2 Ethernet implementation known as "Ethernet IEEE 802.3 SNAP" defines a frame format as shown in Fig.3. The Ethernet IEEE 802.3 SNAP frame comprises of an IEEE 802.3 Data Link header 10, an IEEE 802.2 Logical Link Control (LLC) header 20, an IEEE 802.2 Sub-network Access Protocol (SNAP) header 30 and payload data 40.

[0042] The Data Link header 10 comprises of a 6-bytes destination address 11, a 6-bytes source address 12 and a 2-bytes packet length 13 indicating the length of the Ethernet frame following the packet length 13.

[0043] The LLC header 20 comprises a 1-byte Destination Service Access Point (DSAP) 21, a 1-byte Source Service Access Point (SSAP) 22 and a 1-byte control field 23. Because the SNAP header follows the LLC header, DSAP has a fixed value of 0xAA (i.e. the value AA in hexadecimal formal), SSAP has a fixed value of 0xAA and the control field has a fixed value of 0x03.

[0044] The SNAP header 30 comprises of a 3-bytes IEEE Organizationally Unique Identifier (OUI) 31 followed by a 2-bytes Protocol ID 32.

[0045] The payload data 40 has a maximum length of 1492 bytes.

[0046] The discovery protocol is a light-weight protocol without dependency on IP connectivity. It uses the next-lower layer below IP in the OSI model, i.e. the discovery protocol is a layer 2 protocol based on Ethernet IEEE 802.3 SNAP. A benefit of this is that the discovery protocol bypasses any OSI layer 3 firewall.

[0047] To prevent conflicts between Ethernet packets using the discovery protocol and other Ethernet packets, the SNAP header 30 is used. The OUI part 31 of the SNAP header 30 can be registered with IEEE. The OUI for Hopling Technologies is e.g. registered with IEEE as 0x0019AE. The protocol identifier part 32 of the SNAP header 30 can be set to a predefined value, e.g. 0x0001.

[0048] Several options exist to transfer Ethernet packet using the discovery protocol to recipients: via unicast, broadcast and/or multicast. From the perspective of the sending device 1000, multicast and broadcast are far less time-consuming than using unicast Ethernet packets (addressing every potential station individually). For management applications, it is possible to address one device 2000 instead of being required to address all devices (for instance to get network device maps); hereto unicast can be used. By using multicast as well, it is ensured that the information is sent only to devices that wish to receive discovery protocol data, as opposed to broadcast, where the information is sent to all devices. The same OUI 31 which is used to differentiate from other packet types also provides a range of destination multicast addresses, one of which all discovery protocol supporting devices can subscribe to.

[0049] By not acknowledging traffic sent, the sender 1000 is spared the burden of having to process a potential packet-storm every time the Ethernet packet with discovery protocol information is sent. Consequently delivery of packets is not guaranteed. To ensure delivery, the packet is periodically re-sent. This works especially well given the fact that receiving devices 2000 might not be available at the time a packet is sent.

[0050] Changes to the network can be contained in the packet if the packet is not retained in the receiving device 2000 indefinitely. To this end, two extra timers are attached to every received packet. One timer defines the time after which a node 1000 is to be considered down temporarily, and another timer defines the time after which a node 1000 is to be considered down permanently. The first timer is set to a multiple of the period with which packets are received. The second timer is even larger, i.e. a multiple of the first timer is preferable.

[0051] To prevent issues with various hardware platforms in a network with a different endianness at the CPU level, data is sent in network byte order (i.e. most significant byte first).

Encryption

[0052] To prevent unauthorized access, data is encrypted. While this would be possible using (for instance) public key cryptography, this is far too complex for the discovery protocol to remain light-weight. Therefore a shared secret is used between the participating devices 1000,2000 to ensure that the data is not immediately accessible. An additional benefit of using a shared secret key is that multiple networks co-existing can only receive each others' discovery protocol data if the encryption keys are identical. Decryption failures are either silently ignored, or preferably, a notification is sent to the system, for instance using the syslog protocol of RFC 3164.

[0053] To verify whether a discovery protocol packet has been decrypted correctly, the data packet contains a CRC-32 checksum 60. After decryption, verifying the checksum 60 ensures that the packet has been decrypted correctly. The

checksum 60 is placed within the encrypted part of the data packet to prevent giving away information which can be used to crack the encryption key.

[0054] Because a static key is used, static discovery protocol data such as packet version information is not included in the encrypted part of the packet.

[0055] Preferably a strong encryption cipher such as AES is used. The cipher can impose minimum and maximum lengths on the encryption key, which may require padding or clipping.

Discovery protocol frame format

[0056] Network discovery information sent using the discovery protocol is encoded in a variable manner. This is done by using Type-Length-Value Information Elements (TLV IEs) and concatenating these elements to form the payload part of the discovery protocol packet. This allows flexibility; future additions to the discovery protocol do not require a redesign of the protocol itself. A TLV IE used in the discovery protocol is called discovery protocol information element 70.

[0057] Fig. 4 shows a discovery protocol frame. The discovery protocol frame has a discovery protocol header part 50 and a payload part. The payload part comprises of discovery protocol information elements 70.

[0058] The discovery protocol header 50 defines the information transferred and contains one or more of the following fields: version 51, period 52, fragmentation 53, sequence 54, subject 55, network 56 and checksum 60. The order of the fields can be arbitrary.

[0059] The version field 51 indicates the version of the discovery protocol and is set to e.g. 0x0001 in case of version 1.

[0060] The period field 52 contains the packet transmission interval in seconds.

[0061] Packets can be fragmented when there are more discovery protocol information elements than can be fit in a single Ethernet frame of 1536 bytes. Fragmentation may only occur on boundaries of discovery protocol information elements 70, i.e. no partial discovery protocol information elements may be left in the packet. When fragmentation occurs, the most significant 4 bits of the fragmentation field 53 contain the number of fragments in the entire data frame. The least significant 4 bits of the fragmentation field 53 contain a counter running from 0 and incremented by 1 for every fragment sent. The receiving end 2000 is responsible for reassembly and may drop the entire frame if a fragment is not received within the amount specified in the period field 52. If fragmentation is not used, the entire fragmentation field 53 can be set to 0x00. If more data is received than can fit into 16 fragments, any remaining data may be dropped.

[0062] The sequence field 54 contains a unique number identifying one frame.

[0063] The subject field 55 contains an identifier for the data contained in the frame. Examples of values for the subject field are 0000 for general information, 0001 for system information, 0002 for mesh information and 0003 for management nodes. The subject field 55 can be used to give a general indication to the recipient 2000 of the type of discovery protocol information elements 70 that are contained in the data packet. This may be used by recipient 2000 to discard data before decryption if it is deemed not interesting, or on embedded platform to only implement a subset of the full discovery protocol.

[0064] The network field 56 contains an integer number identifying the logical network the host 1000 belongs to. The Network field 56 can be used to logically split up one layer 2 network into several layer 2 networks. Discovery protocol packets for which the network field value does not match its own network can be ignored by the receiver 2000.

[0065] The checksum 60 is a bitwise little-endian IEEE 802.3 CRC-32 checksum over all discovery protocol information elements 70 in this fragment. Of all fields, only the checksum 60 and the discovery protocol information elements 70 are encrypted. This hides any data which can be used in a cracking attempt, and also returns one field which can be used after decryption to check whether the decryption key used was correct. Encryption can be performed using e.g. an AES-256 cipher.

[0066] Security is less strong when concatenating the various discovery protocol information elements 70 in the same order every time a packet is sent across the network. After encrypting, this provides a form of repetition in the data stream which could theoretically be used to crack the encryption. Therefore security is increased by concatenating the discovery protocol information elements 70 in a random order (shuffling) before encryption is applied. Furthermore the discovery protocol information elements 70 are grouped such that the amount of Ethernet frames needed to transmit all discovery protocol information elements 70 is minimized.

[0067] In Figs.5a-5c an example of shuffling and grouping is shown. In Fig.5a a set 7a of discovery protocol information elements 71-75 is provided. In Fig.5b the discovery protocol information elements 71-75 are shuffled and form a shuffled set 7b of discovery protocol information elements. Next, the discovery protocol information elements 71-75 are provided to Ethernet frames in the order of presence in the shuffled set 7b, as shown in Fig.5c. A first Ethernet frame is provided with discovery protocol information element 72. The first Ethernet frame further comprises a Data Link header 10, a LLC header 20, a SNAP header 30 and a discovery protocol header 50. A second Ethernet frame is provided with discovery protocol information elements 74 and 71. The discovery protocol information elements 74 and 71 are grouped together because they fit within a single Ethernet frame. The second Ethernet frame further comprises a Data Link header 10, a LLC header 20, a SNAP header 30 and a discovery protocol header 50. A third Ethernet frame is provided with discovery protocol information element 73. The third Ethernet frame further comprises a Data Link header 10, a LLC header 20,

a SNAP header 30 and a discovery protocol header 50.

[0068] It is evident that it is possible to perform shuffling without grouping.

[0069] The discovery protocol information elements 70 contain 4 fixed fields, and a free-form data field. The first field is the Organization field (a 32-bit integer dword), uniquely identifying the company defining the information element. The numbers used are according to the IANA SMI Network Management Private Enterprise Codes. The value 0, which is designated by IANA as being 'Reserved' is used to indicate a General organization. The second field is the Entity field (a 16-bit word), a system-arbitrary integer which can be used to group discovery protocol information elements 70 belonging to a single logical host. The third field is the Type field (a 16-bit word), describing the type of information contained in the information element. The fourth field is the Length field (a 16-bit word), which specifies the number of bytes in the data portion of the discovery protocol information element 70 (in other words the entire information element except the Organization, Type, Length and Entity fields).

[0070] Frames which are too small to reach the minimum Ethernet frame size of 64 bytes use a 'padding' information element to make sure that the frame conforms to the Ethernet specification. The padding information element is also used for encryption algorithms to receive an aligned block of input data which is then subsequently encrypted using a block cipher (for instance, CBC). The padding information element contains the fields Organization = 0x00000000, Entity Type = 0x0000, Length = size (Pad) and Pad. The Length field comprises the size of the Pad field in bytes. The Pad field itself comprises random data, so as to prevent recurring data in the encrypted data stream (which could then be used to crack the encryption key) and improve the encryption strength of the encrypted data stream.

[0071] The 'last seen' information element contains the fields Organization = 0x00000000, Entity Type = 0x0001, Length = 0x0004 and Timestamp (32-bit dword). The Last seen IE contains a time stamp in seconds since the information contained in the entire discovery protocol data packet for this entity 1000 was last updated.

[0072] The 'device name' information element contains the fields Organization = 0x00000000, Entity Type = 0x0002, Length = size (Name) and Name. The Device name information element contains an ASCII C-style string with the host name of the device 1000 sending the information. The Length field comprises the length of the ASCII string, including the terminating 0x00.

[0073] The 'address' information element contains the fields Organization = 0x00000000, Entity Type = 0x0003, Length = 0x0003 + size (Address), Group (1 byte), Mask length (1 byte), Protocol (1 byte) and Address (varies). This information element contains the address at which a device 1000 can be reached for management (and related) traffic. The information element comprises of four fields; the Group field, the Mask length field, the Protocol field and the Address field. The Group field indicates the nature of the Address field. The Mask length field indicates the mask hexadecimal mask that is applied to the Address field to obtain a network address using a bit-wise AND, or to obtain the broadcast address using a bit-wise OR. The mask to apply to the address is calculated as: 2^(Mask Length - 1). The Protocol field indicates the protocol family the address belongs to, and an Address field, which contains the address itself. The size in bytes of the address depends on the protocol family in question.

[0074] The 'software release' information element contains the fields Organization = 0x00000000, Entity Type = 0x0005, Length = size (Release) and Release. The software release information element contains an ASCII C-style string with the human readable software release (including the software flavour) of the currently running software. The Length field comprises the length of the ASCII string, including the terminating 0x00.

[0075] The 'device information' information element contains the fields Organization = 0x00000000, Entity Type = 0x0006, Length = 0x0007, Uptime (32-bit dword), Load (16-bit word), Memusage (8-bit word). This information element contains three fields describing the operational status of a system. The first field contains the time the device 1000 has been operational in seconds. The second field contains the system load multiplied by 100. The third field contains the percentage of unused memory relative to the total amount of memory available on the device 1000. The Length field comprises the uptime (4 bytes), load (2 bytes) and memusage (1 byte).

[0076] The 'serial number' information element contains the fields Organization = 0x00000000, Entity Type = 0x0007, Length = size (Serial) and Serial. The Serial number information element contains an ASCII C-style string with the serial number of the device 1000 sending the information. The Length field comprises the length of the ASCII string, including the terminating 0x00.

[0077] The 'interface identification' information element contains the fields Organization = 0x00000000, Entity Type = 0x0008, Length = size (Interface) and Interface. The Interface ID information element contains an ASCII C-style string with the human readable interface name of the device 1000 sending the information. The Length field comprises the length of the ASCII string, including the terminating 0x00.

[0078] The 'first seen' information element contains the fields Organization = 0x00000000, Entity Type = 0x0009, Length = 0x0004 and Timestamp (32-bit dword). This information element contains a time stamp in seconds since discovery protocol information for this entity 1000 was first received.

[0079] The 'Receiving Interface ID' information element contains the fields Organization = 0x00000000, Entity Type = 0x000A, Length = size (Interface) and Interface. This information element contains an ASCII C-style string with the human readable interface name of the device which received the information. The Length field comprises the length of

the ASCII string, including the terminating 0x00.

[0080] The 'event URI' information element contains the fields Organization = 0x0000699A, Entity Type = 0x0001, Length = size (URI) and URI. The Event URI information element contains an ASCII C-style string with the URI to which devices can send events. The Length field comprises the length of the ASCII string, including the terminating 0x00.

[0081] The 'signal strength' information element contains the fields Organization = 0x0000699A, Entity Type = 0x0002, Length = 0x002C, Frequency (32 bits), Address (48 bits), SNR (8 bits), Connected (1 bit), discovery protocol (1 bit), HAM (1 bit), HEM (1 bit), Radio (4 bits) and SSID (256 bits). This information element contains nine fields. The first is the channel frequency in MHz on which the mesh node 2000 has been seen by the sender 1000. The second field is the 48-bit IEEE 802.3 Ethernet address of the mesh node 2000 seen by the sender 1000. The third field is an indicator, containing the SNR the sender 1000 has observed from the mesh node 2000. The SNR is measured in dB above the noise floor, as specified by the IEEE 802.11 specification. The fourth field is a flag, which indicates whether the sender 1000 has established a logical link with the mesh node 2000. The fifth field indicates whether the node 2000 is capable of responding to discovery protocol packets. The sixth field (HAM) indicates whether the node 2000 is capable of automatically establishing a mesh. The seventh field (HEM) indicates whether the node 2000 is capable of setting up an Encrypted Mesh link (HEM). The eighth field indicates the radio device on which the node 2000 was seen. This is an integer number which arbitrarily indicates a unique interface on a node. The value 0xF indicates that the radio device is unknown. The ninth field contains the SSID ("Service Set Identifier") at which the node 2000 was seen sending IEEE 802.11 beacons. The Length field comprises the Frequency (32 bits), Address (6 bytes), SNR (1 byte), Connected (1 bit), discovery protocol (1 bit), HAM (1 bit), HEM (1 bit), Radio (4 bits) and SSID (32 bytes) fields. This information element describes the signal strength for a different mesh node 2000. If a device 1000 detects the same potential mesh node candidate on multiple radios, it reports the strongest possible radio link. When determining the SNR, implementations are suggested to read the value from the network driver, send a significant amount of data traffic to the Address the SNR is determined for, then read the value from the network driver again. This will give a more accurate value.

[0082] The 'associated stations' information element contains the fields Organization = 0x0000699A, Entity Type = 0x0003, Length = 0x0009, Address (48 bits), SNR (8 bits), Radio (4 bits), Virtual Gateway (4 bits), Mode (4 bits) and Flags (4 bits). This information element describes the wireless stations (clients) associated to the node 1000 and contains six fields. The first field is the 48-bit IEEE 802.3 Ethernet address of the associated station. The second field contains the SNR in dB from the perspective of the node 1000. The third field contains a 0-based value with the radio device on the node 1000 the station is associated to. This value is determined on a per-node basis. The value 0xF indicates that the radio device is unknown. The fourth field contains the Virtual Gateway number. This describes a virtual access point on a radio. The number is 0-based and determined on a per-node basis. The value 0xF indicates that the virtual gateway is unknown. The fifth field contains the authentication mode. The sixth field contains flags. The Length field comprises the Address (6 bytes), SNR (1 byte), Radio (4 bits), Virtual Gateway (4 bits), Mode (4 bits) and Flags (4 bits) fields.

[0083] The 'location' information element contains the fields Organization = 0x0000699A, Entity Type = 0x0004, Length = 0x0008, Longitude degrees (1 byte), Longitude minutes (6 bits), Longitude seconds (6 bits), Latitude seconds (6 bits), Latitude minutes (6 bits), Latitude degrees (1 byte), Longitude direction (1 bit), Latitude direction (1 bit), Height valid (1 bit), Flags (5 bits) and Height (2 bytes). This information element contains eleven fields to identify the geographic location of a device 1000. The first, second and third fields contain the degrees, minutes and seconds longitude, respectively. The value 0xFF for degrees and 0x3F for minutes or seconds indicate that the parameter is unknown. The fourth, fifth and sixth fields contain the seconds, minutes and degrees latitude, respectively. The value 0xFF for degrees and 0x3F for minutes or seconds indicate that the parameter is unknown. The seventh field is non-zero if the location lies in the eastern hemisphere (or 0 if it is located in the western hemisphere). The eighth field is non-zero if the location lies in the northern hemisphere (and 0 if the location lies in the southern hemisphere). The tenth field is a flag field. The eleventh field marks the height in meters above sea level, as a signed integer value. The tenth field indicates whether the height value has any meaning. The Length field comprises the Longitude degrees (1 byte), Longitude minutes (6 bits), Longitude seconds (6 bits), Latitude seconds (6 bits), Latitude minutes (6 bits), Latitude degrees (1 byte), Longitude direction (1 bit), Latitude direction (1 bit), Height valid (1 bit), Flags (5 bits) and Height (2 bytes) fields.

[0084] The 'device type' information element contains the fields Organization = 0x0000699A, Entity Type = 0x0005, Length = 0x0005, Hardware (2 bytes), Software (2 bytes) and Revision (1 byte). This information element contains three fields. The first is the Hardware field which contains an integer number specifying the type of device 1000 sending the data. The second field is the Software field which contains an integer number specifying the software running on the device 1000. The third field contains the Revision field, which can be used to designate a particular hardware revision of a device 1000. This revision field should not be confused with the software release, which is part of another information element. The Length field comprises the Hardware (2 bytes), Software (2 bytes) and Revision (1 byte) fields.

[0085] The 'wireless' information element contains the fields Organization = 0x0000699A, Entity Type = 0x0006, Length = 0x0014, Address (48 bits), Frequency (32 bits), Transmit Power (10 bits), Radio (4 bits), Elevation (9 bits), Azimuth (9 bits), PHY rate (16 bits), Antenna (16 bits) and Noise (16 bits). This information element contains nine fields which describe a radio device of the device 1000. The first field contains the 48-bit IEEE 802.3 Ethernet address of the

radio device. The second field contains the frequency in MHz at which the radio operates. A value of 0 indicates an unknown frequency. The third field contains the radio's transmission power in units of 0.1 dBm. Note that this is excluding cable and antenna gain/loss. A value of 0 indicates an unknown transmission power. The fourth field is an integer number which arbitrarily indicates the radio device uniquely on the device. The value 0xF indicates that the radio device is unknown. The fifth field contains the inclination angle of the antenna's emission point in degrees above the horizon. This would be 90 degrees on most outdoor setups using an omni-directional antenna, for example. A value of 0x0FF indicates an unknown elevation. The sixth field contains the deviation of the antennas emission point in degrees from the compass North. A value of 0x0FF indicates an unknown azimuth. The seventh field contains the maximum data rate the radio is capable of achieving in units of 0.1 Mbps. A value of 0 indicates an unknown transmission rate. The eighth field contains the antenna connected to the radio device. The ninth field contains a signed 16-bit value with the radio noise floor in dB. A value of 0x7FFF indicates an unknown noise floor. The Length field comprises the Address (6 bytes), Frequency (4 bytes), Transmit Power (10 bits), Radio (4 bits), Elevation (9 bits), Azimuth (9 bits), PHY Rate (2 bytes), Antenna (2 bytes) and Noise (2 bytes) fields.

[0086] The 'virtual gateway' information element contains the fields Organization = 0x0000699A, Entity Type = 0x0007, Length = 0x0022, Radio (4 bits), Virtual Gateway (4 bits), Authentication Mode (4 bits), SSID Hidden (1 bit), Clients Allowed (1 bit) and SSID (256 bits). The virtual gateway information element is used to define one or multiple virtual communication device(s) on the first communication device 1000. Each virtual communication device can be configured separately. This information element contains seven fields which describe a point of access on a radio. The first field is an integer number which arbitrarily indicates the radio device uniquely on the first communication device 1000. The value 0xF indicates that the radio device is unknown. The second field contains the Virtual Gateway number. This describes a virtual access point on a radio device. The number is 0-based and determined on a per-node basis. The value 0xF indicates that the virtual gateway is unknown. The Third field contains the authentication mode. The fifth field is a flag which indicates whether the SSID contained within this information element is hidden from clients 2000 (in other words, not transmitted in the IEEE 802.11 Beacon). The sixth field is a flag which indicates whether clients 2000 are allowed to associate with this gateway 1000. The seventh field contains the IEEE 802.11 SSID which the node is configured to respond to. The Length field comprises the Radio (4 bits), Virtual Gateway (4 bits), Authentication Mode (4 bits), SSID Hidden (1 bit), Clients Allowed (1 bit) and SSID (256 bits) fields.

[0087] The 'bandwidth' information element contains the fields Organization = 0x00000000, Entity Type = 0x000B, Length = 0x001A, Local (48 bits), Peer (48 bits), Up Bytes Mantissa (16-bit word), Down Bytes Mantissa (16-bit word), Up Packets Mantissa (16-bit word), Down Packets Mantissa (16-bit word), Up Bytes Exponent (8-bit word), Down Bytes Exponent (8-bit word), Up Packets Exponent (8-bit word), Down Packets Exponent (8-bit word), Subinterface (12 bits), Subinterface Valid (1 bit), Standby (1 bit) and Up (1 bit). The Bandwidth IE contains 15 fields. The first field contains the 48-bit IEEE 802.3 Ethernet address on the local end of a mesh link. The second field contains the 48-bit IEEE 802.3 Ethernet address of the remote end of the mesh link. This value may be set to 00:00:00:00:00:00 to indicate that this IE describes a point-to-multipoint link. The third to sixth fields as well as the seventh to tenth fields are encoded values for the amount of traffic generated over the last packet transmission interval. The values are calculated as Mantissa * 10^Exponent. Exponent can be a negative value. The exponent value of -127 is reserved and indicates that the value is invalid. The values are:

Mantissa	Exponent	Meaning
3rd field	7th field	Average of bytes per second transmitted from local to peer
4th field	8th field	Average of bytes per second transmitted from peer to local
5th field	9th field	Average of packets per second transmitted from local to peer
6th field	10th field	Average of packets per second transmitted from peer to local

The eleventh field contains an arbitrary index number indicating an interface related to the primary interface (which has this value set to 0). The twelfth field is set to 0 and ignored upon reads. The thirteenth field indicates whether the eleventh field is valid. The fourteenth field indicates whether a link is configured as a hotspare link (for redundancy). The fifteenth field indicates whether this link is currently operational. The Length field comprises the length of the Local (48 bits), Peer (48 bits) Up Bytes Mantissa (16 bits), Down Bytes Mantissa (16 bits), Up Packets Mantissa (16 bits), Down Packets Mantissa (16 bits), Up Bytes Exponent (8 bits), Down Bytes Exponent (8 bits), Up Packets Exponent (8 bits), Down Packets Exponent (8 bits), Subinterface (12 bits), Subinterface Valid (1 bit), Standby (1 bit) and Up (1 bit) fields.

Automatically configuring a mesh network

[0088] A mesh network 100 as shown in Fig.6 is a network in which several nodes 102-105 are interconnected. The first communication device 1000 in Fig.1 is one of the nodes 102-105, while the second communication device 2000 in

Fig.1 is another one of the nodes 102-105. Each node 102-105 covers an area 101. There is a distinct advantage in redundancy. As long as every node 102-105 has at least one redundant link to another node, a single failing node should not affect traffic in the entire mesh network. Node 103 e.g. has two links to node 104. The first link is a direct link. There is a redundant link from node 103 to node 104 via node 105.

[0089] The invention enables automatically configuring a mesh network 100. In order to automatically configure the mesh network 100, the nodes 102-105 in the mesh need to know who its neighbours are and if these neighbours are meant to be part of the mesh network. The discovery of neighbours can e.g. be done through the reception of IEEE 802.11 beacons. When it is determined that the neighbouring node can be part of the mesh network, discovery protocol information elements 70 are used to send discovery information. When running a Linux operating system, it is possible to extract this information using ioctls ("input/output controls" that allows an application to control or communicate with a device driver). In the mesh network information is obtained containing the signal strength with which a device sees other devices. However, while this does indicate how well a node receives signals from its neighbours, nothing is said about how well the neighbour receives signals from the node. Thus, a small paradox is created as a connection needs to be configured in order to configure a connection. This means that devices 102-105 need to discover all mesh-capable neighbours.

[0090] In order to quickly retrieve information about (potential) neighbouring mesh nodes, all auto-mesh capable devices send out a 'mesh capabilities' information element. This mesh capabilities information element is, in case of an IEEE 802.11 network, a special IEEE 802.11 information element in a management frame transmitted by a IEEE 802.11 radio device in the mesh-capable device. It will be understood that in other type of networks, which can be fixed and/or wireless networks, another but similar management frame is used. The mesh capabilities information element contains the following fields: Element ID (8 bits), Length (8 bits), OUI (24 bits), Type (8 bits), Version (8 bits), discovery protocol (1 bit), HAM (1 bit), HEM (1 bit), Mesh count (8 bits), Mesh links (8 bits) and Mesh ID (16 bits). Element ID is an IEEE 802.11 Element ID, set to 221 decimal. Length is the size of the entire element in bytes. OUI is set to the vendor OUI, e.g. 0x0019AE. Type is the type of vendor specific IEEE 802.11 information element and is set to e.g. 0x01. Version is the version of the frame, set to e.g. 0x01. Element ID, Length, OUI, Type and Version are IEEE 802.11 specific fields and can be different or absent in other types of networks. Discovery protocol indicates whether the sending device understands the discovery protocol. HAM indicates whether the device is capable of automatically establishing mesh connectivity. HEM indicates whether the device encrypts the mesh link. Mesh count is the number of mesh connections the device is capable of establishing. Mesh links is the number of mesh connections the device has established. Mesh ID is a 16-bit integer value identifying the mesh network number the host is servicing. All nodes in a mesh network use identical mesh ID strings.

[0091] This capabilities information is used by neighbouring nodes 2000 to see the capabilities of a given device 1000. Any device not sending out this mesh capabilities information element can be considered not to be capable of auto-meshing. Any node broadcasting the same mesh ID, and supporting the discovery protocol can be connected to the mesh network. Whether the device supports the discovery protocol can be determined by evaluating the HAM field in the mesh capabilities information element or in the signal strength information element. In order to see whether a connection can be established to the neighbour, unicast transmissions are used to query the signal strength information. Alternatively node 1000 receives the signal strength information from neighbouring node 2000 via multicast or broadcast.

[0092] To discover signal strength information, a special discovery protocol information element called the 'signal strength' information element has been created. The signal strength information element is described under the section 'Discovery protocol frame format' above. Using signal strength information that is detected from a neighbouring node 2000, the node 1000 creates the signal strength information element. This makes it is possible to inform the neighbouring node 2000 about how the node 1000 perceives the neighbour 2000 and how the neighbour 2000 perceives the node 1000. Since the discovery protocol is capable of providing information of other wireless capable devices, it is even possible to obtain signal strength information from nodes the device is normally not capable of perceiving (thus information can be gained from devices from which no data can be received, but which might receive information from the device itself). Should a device not respond to the discovery protocol queries, it is possibly using a different encryption key. In any case, a device which does not respond can be considered as a device not supporting the discovery protocol or auto-meshing.

[0093] When the mesh connection has been established, retaining the connection becomes easier. As every node 102-105 implementing the discovery protocol will use layer 2 multicasting to periodically advertise its presence on the network 100, the existing mesh will ensure that every node 102-105 receives advertisements from all of the other nodes. In the established network, network discovery information elements as described above are transmitted between the nodes and from nodes to computers 4000 to maintain the mesh network.

[0094] One of the mesh nodes can be a bridge to a wired network. Preferably this is a device with a wired connection, if possible as close as possible to the Internet gateway. In Fig.1 the first communication device 1000 is an example of a device connected to a fixed network 3000. In Fig.1 the second communication device is an example of a mesh node without a wired connection.

[0095] A method for configuring a mesh network, a first communication device that is arranged to transmit network discovery information to a second communication device, and a mesh network are described in a separate patent application of the present applicant, titled "Configuring a mesh network", which is filed on the same date as this patent application and is incorporated herein by reference.

Claims

1. Method for a first communication device (1000) to transmit or retransmit network discovery information to a second communication device (2000), the method comprising the steps of:

   providing a layer 2 frame comprising a sub-header (30), the sub-header (30) comprising an identifier field (31) indicating the presence of a discovery protocol in the layer 2 frame,

   characterized by:

   providing at least one discovery protocol information element (70) comprising network discovery information;
   encrypting the at least one discovery protocol information element (70);
   providing a discovery protocol header (50) and the encrypted at least one discovery protocol information element (70) to the layer 2 frame; and
   transmitting the layer 2 frame to the second communication device (2000).

2. Method according to claim 1, the method further comprising the steps of:

   calculating a checksum (60) over the at least one discovery protocol information element (70) prior to encrypting the at least one discovery protocol information element (70);
   encrypting the checksum (60); and
   providing the encrypted checksum (60) to the layer 2 frame.

3. Method according to any of the preceding claims, the method further comprising the step of providing one or more of the following fields to the discovery protocol header (50):

   a version field (51) comprising data indicating a version of the discovery protocol;
   a period field (52) comprising data indicating a packet transmission interval;
   a subject field (55) comprising data indicating a type of discovery information;
   a network field (56) comprising data indicating a logical network the first communication device (1000) belongs to.

4. Method according to any of the preceding claims, the method further comprising at least one of the steps of:

   providing a type field to the at least one discovery protocol information element (70), the type field comprising data indicating a type of the discovery information comprised in the discovery protocol information element (70);
   providing a length field to the at least one discovery protocol information element (70), the length field comprising data indicating a length of the discovery information comprised in the discovery protocol information element (70).

5. Method according to the preamble of claim 1, wherein, if there are two or more discovery protocol information elements (70), the method further comprises the steps of:

   determining if the two or more discovery protocol information elements fit within the layer 2 frame,
   and if the outcome of the determination step is positive:

      providing a discovery protocol header (50) and the two or more discovery protocol information elements (70) to the layer 2 frame; and
      transmitting the layer 2 frame to the second communication device (2000),
      and if the outcome of the determination step is negative:

         providing a discovery protocol header (50) and at least one discovery protocol information element (70) to the layer 2 frame;
         providing a further layer 2 frame comprising a further sub-header (30), the further sub-header (30)

comprising the identifier field (31);
providing a further discovery protocol header (50) and an at least one further discovery protocol information element (70) to the further layer 2 frame;
providing a fragmentation field (53) to the discovery protocol header (50) and to the further discovery protocol header (50), the fragmentation field (53) comprising data indicating a total number of layer 2 frames, the fragmentation field (53) further comprising data indicating a counter that is incremented for every layer 2 frame sent; and
transmitting the layer 2 frame and the further layer 2 frame to the second communication device (2000).

6. Method according to claim 5, the method further comprising the steps of:

if the outcome of the determination step is positive,
encrypting the two or more discovery protocol information elements (70),
if the outcome of the determination step is negative:

encrypting the at least one discovery protocol information element (70); and/or
encrypting the at least one further discovery protocol information element (70).

7. Method according to any of the claims 5-6, the method further comprising at least one of the steps of:

shuffling the two or more discovery protocol information elements;
grouping the two or more discovery protocol information elements such that the two or more discovery protocol information elements fit in a least amount of layer 2 frames.

8. Method according to any of the claims 5-7, the method further comprising the step of:

providing a padding information element as a discovery protocol information element and/or further discovery protocol information element, such that within the layer 2 frame and/or further layer 2 frame the length of the discovery protocol information elements including the padding information element fits within a block boundary for encryption.

9. Method according to claim 8, the method further comprising the step of providing the padding information element with a random data.

10. Method according to any of the claims 5-9, the method further comprising the step of:

providing a sequence field (54) to the discovery protocol header (50) and/or further discovery protocol header (50), the sequence field (54) comprising data identifying a set of layer 2 frames.

11. Method according to any of the claims 1-10, wherein the method comprises the step of transmitting the layer 2 frame using unicast addressing.

12. Method according to any of the claims 1-11, wherein the method comprises the steps of transmitting the layer 2 frame in an un-acknowledged mode and resending the layer 2 frame periodically.

13. Method for a second communication device (2000) to process network discovery information, the method comprising the steps of:

receiving from a first communication device (1000) at least one encrypted discovery protocol information element (70) transmitted by the first communication device (1000) according to any of the claims 1-12; and
decrypting the at least one discovery protocol information element (70),
the method further comprising at least one of the steps of:

configuring the second communication device (2000) using the received network discovery information;
storing the received network discovery information for network management.

14. Method according to claim 13, the method further comprising the steps of:

starting a first timer and a second timer upon receiving the at least one encrypted discovery protocol information element;
comparing the first timer with a predefined first maximum time indicating when the first communication device (1000) is to be considered down temporarily;
comparing the second timer with a predefined second maximum time indicating when the first communication device (1000) is to be considered down permanently.

15. A first communication device (1000) arranged for transmitting network discovery information to a second communication device (2000), the first communication device (1000) comprising a processor (1002), a memory (1003) and a transmitter (1001) to perform the steps of the method according to any of the claims 1-12.

16. A second communication device (2000) arranged for processing network discovery information, the second communication device (2000) comprising a processor (2002), a memory (2003) and a receiver (2001) to perform the step of the method according to any of the claims 13-14.

17. A layer 2 discovery protocol in a layer 2 frame, the layer 2 frame comprising a sub-header (30), the sub-header (30) comprising an identifier field (31) indicating the presence of the discovery protocol in the layer 2 frame, the discovery protocol comprising:

a discovery protocol header (50); and
one or more discovery protocol information elements (70) comprising network discovery information,

wherein the at least one of said discovery protocol information elements (70) is encrypted.

18. A layer 2 discovery protocol according claim 17, wherein the discovery protocol header (50) comprises a checksum (60) over the at least one discovery protocol information element (70) and wherein the checksum (60) is encrypted.

19. A layer 2 discovery protocol according to any of the claims 17-18, wherein the layer 2 frame is an Ethernet frame.

20. A layer 2 discovery protocol according to any of the claims 17-19, wherein the discovery protocol header (50) further comprises one or more of the following fields:

a version field (51) comprising data indicating a version of the discovery protocol;
a period field (52) comprising data indicating a packet transmission interval;
a subject field (55) comprising data indicating a type of discovery information;
a network field (56) comprising data indicating a logical network a first communication device (1000) belongs to.

21. A layer 2 discovery protocol according to any of the claims 17-20, wherein the at least one discovery protocol information element (70) comprises:

a type field, the type field comprising data indicating a type of the discovery information comprised in the discovery protocol information element (70); and
a length field, the length field comprising data indicating a length of the discovery information comprised in the discovery protocol information element (70).

22. A layer 2 discovery protocol according to any of the claims 17-21, wherein the discovery protocol header (50) further comprises a fragmentation field (53), the fragmentation field (53) comprising data indicating a total number of layer 2 frames, the fragmentation field (53) further comprising data indicating a counter that is incremented for every layer 2 frame sent.

23. A layer 2 discovery protocol according to claim 22,
wherein the discovery protocol further comprises a padding information element as a discovery protocol information element (70), such that within the layer 2 frame the length of the layer 2 protocol information elements, including the padding information element, fits within a block boundary for encryption.

24. A layer 2 discovery protocol according to any of the claims 22-23, wherein the discovery protocol header (50) further comprises a sequence field (54), the sequence field (54) comprising data identifying a set of layer 2 frames.

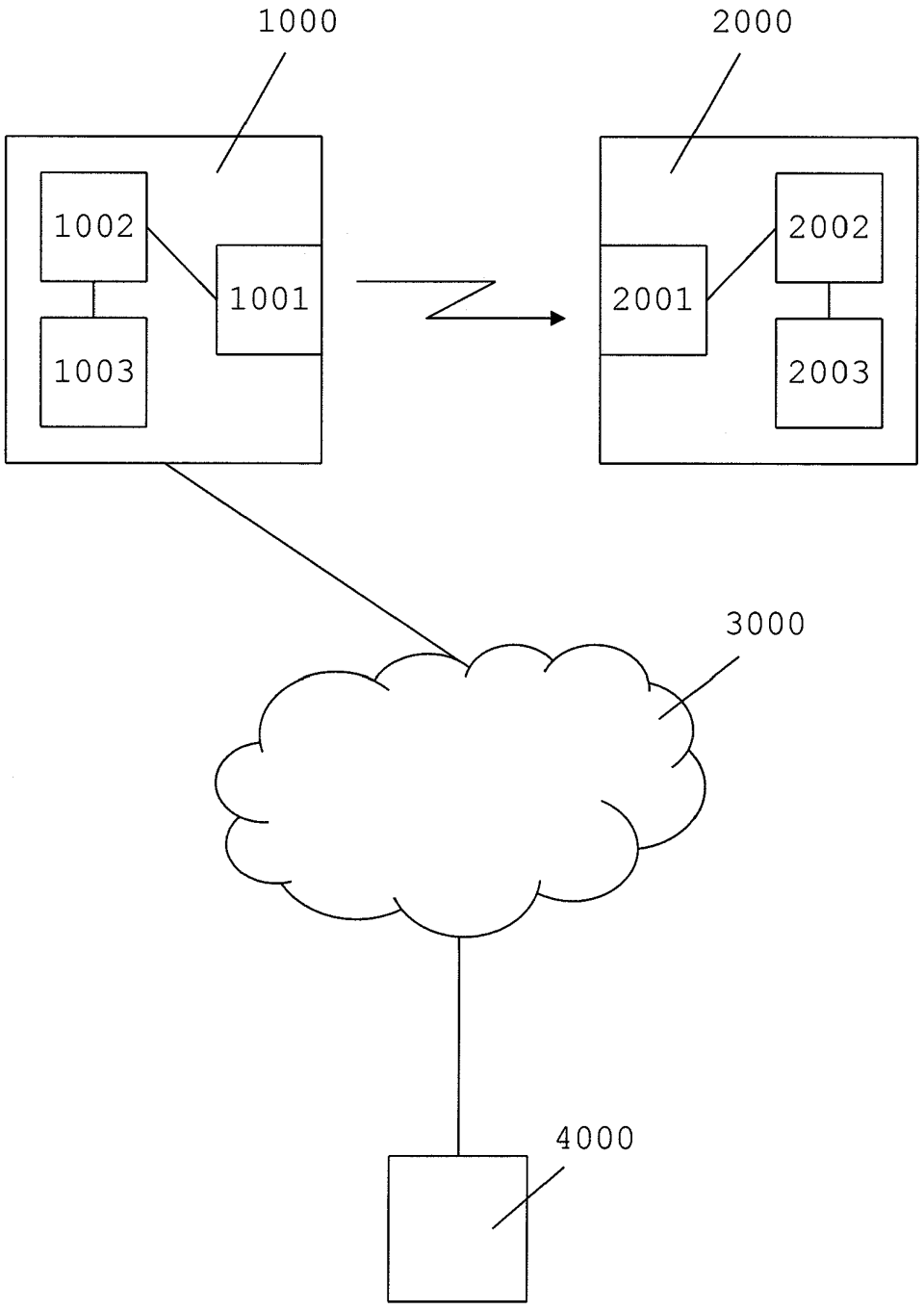

Fig.1

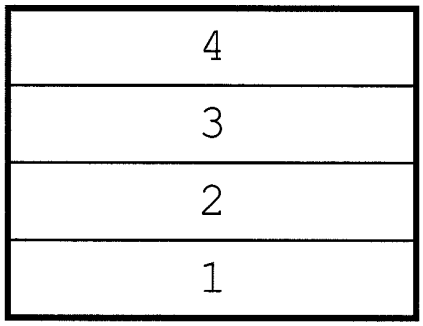

Fig.2

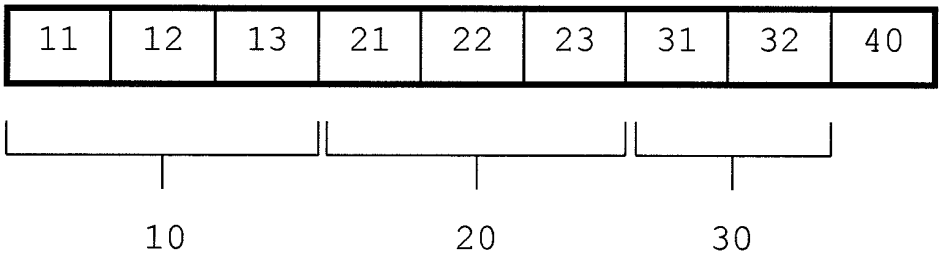

Fig.3

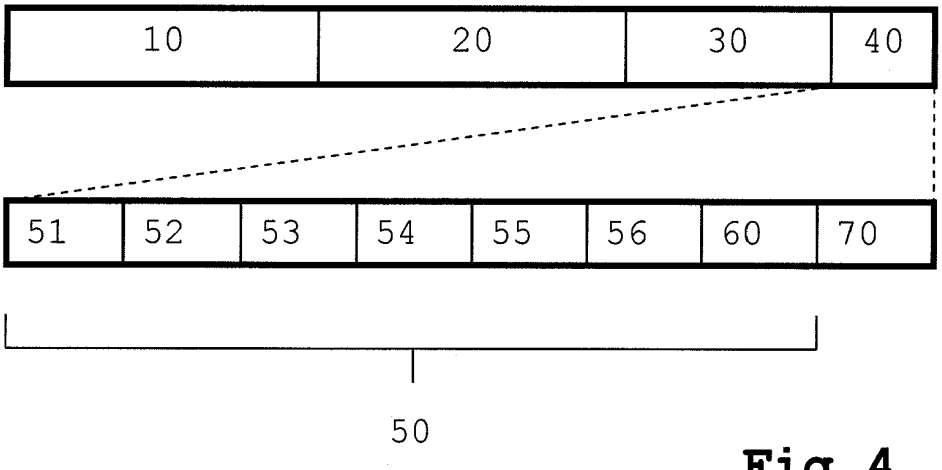

Fig.4

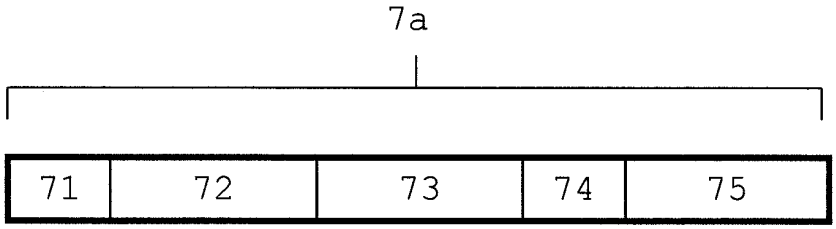

Fig.5a

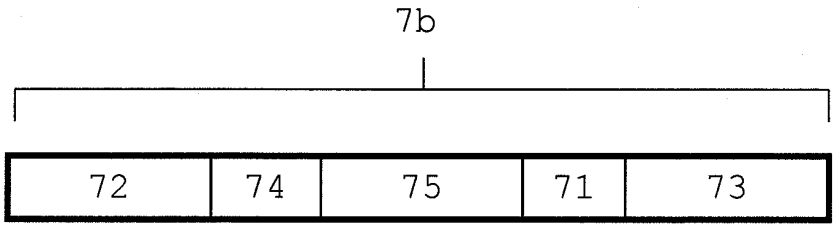

Fig.5b

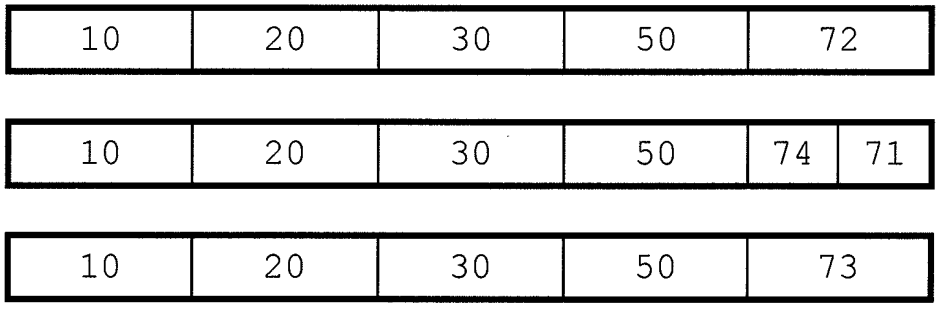

Fig.5c

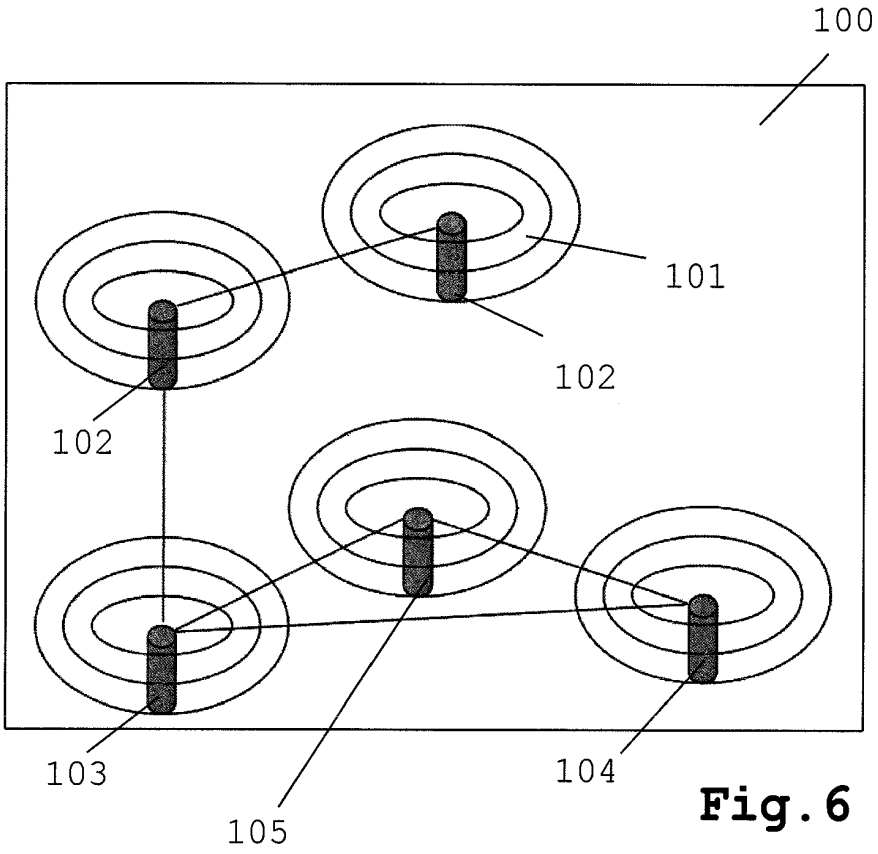

Fig.6

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 07 11 4926

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X A	WO 2007/048247 A (NORTEL NETWORKS LTD [CA]; WANG GUO QIANG [CA]; WU SHIQUAN [CA]) 3 May 2007 (2007-05-03) * abstract * * page 1, line 5 - page 8, line 9 * * page 10, line 4 - page 13, line 5 * * page 16, line 15 - page 17, line 30 * * page 25, line 16 - page 30, line 30 * * figures 1-5 * -----	1-6,10, 11,13, 15-22,24 7-9,12, 14,23	INV. H04L12/28 H04L12/56
X A	US 2007/141984 A1 (KUEHNEL THOMAS W [US] ET AL) 21 June 2007 (2007-06-21) * abstract * * paragraphs [0002] - [0010], [0018], [0022] - [0055] * * figures 1-5 * -----	1-6,10, 11,13, 15-22,24 7-9,12, 14,23	
X A	CALHOUN P ET AL: "CAPWAP Protocol Binding for IEEE 802.11; draft-ietf-capwap-protocol-b inding-ieee80211-04.txt" IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, vol. capwap, no. 4, 11 June 2007 (2007-06-11), XP015051122 ISSN: 0000-0004 * abstract * * page 3, line 1 - page 14, line 3 * * page 19, line 1 - page 32, line 43 * * figures 1-7 * -----	1-6,10, 11,13, 15-22,24 7-9,12, 14,23	TECHNICAL FIELDS SEARCHED (IPC) H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
Munich	22 January 2008	Mariggis, Athanasios

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 07 11 4926

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

22-01-2008

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2007048247 A	03-05-2007	US 2007097945 A1	03-05-2007
US 2007141984 A1	21-06-2007	WO 2007075968 A2	05-07-2007

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 7099295 B1 **[0005] [0005]**