

TITLE

COMMUNICATION APPARATUS, METHOD FOR CONTROLLING COMMUNICATION BETWEEN DIFFERENT TYPES OF DEVICES, AND METHOD FOR ELIMINATING SPECIFICITY OF OPERATIONAL MANAGEMENT

5

BACKGROUND OF THE APPLICATION

Field of the Application

[0001] The present invention relates to a communication apparatus, a method for controlling communication between different types of devices, and a method for eliminating specificity of operational management.

10

Description of the Related Art

[0002] Until the middle 1980s, a computer was constituted by a combination of a universal machine and an input terminal. Using the central universal machine to process all processing is referred to as an application in a closed space.

15

[0003] However, LAN and WAN were introduced to connect a company's internal network environment. Using the Internet to connect the company's internal/external network environments has had an impact on computer systems since around 1995. Currently, a service called the cloud is employed. With continuing advances being made in this type of service, connections with the company's external resources or the network connections of business and globalization in numerous foreign currency denominations have further become general connections. Nowadays, it is becoming important to use a secure network to transmit data when working with numerous foreign currency denominations.

20

[0004] Although the cloud services use the Internet and matching, the Internet is

very dangerous from the point of view of security. Therefore, a secure network must be constructed. However, with secure network connections, there remain problems regarding the various complicated types of connections. To solve this problem, it is necessary to deal with expensive apparatuses, advanced network design, and advanced network specialization. Therefore, there are issues such as management of addresses and depletion of addresses, which highlight new challenges for security technicians.

[0005] Although there is one prior-art reference such as patent document 1, a proxy in Patent document 1 may change the length of an address defined by the Internet, LAN, WAN, etc., to a unique address length. However, in the present invention, the length of the address does not need to be changed. The length of the address defined by the network can be directly used without being set by the proxy, so that the operation becomes very simple. The problem of address duplication caused by the combination of LAN, WAN, etc. because of the combination of the companies can be solved.

RELATED ART DOCUMENT

PATENT DOCUMENT

[0006] [Patent document 1] Japanese Patent No. 4802295

BRIEF SUMMARY OF THE APPLICATION

PROBLEM TO BE SOLVED

[0007] To improve the efficiency of operation management, an independent distributed system must be formed, so that traffic is distributed to reduce the load on a relay device. The function of operation maintenance management is automated according to a self-learning function. In other words, what is needed is a technology able to independently build an encryption network on the Internet.

[0008] The integration of different networks where address conflicts occur needs

management of addresses. With current technology, it is not easy to design a secure network. To achieve a structure which works as fast as expected and is not complicated, effort must be expended to use a running network, as well as on network design. In the network design for re-allocating the addresses for each application, the network is no longer simple. There is a problem wherein a huge investment is necessary because it involves setting changes of the network equipment.

MEANS FOR SOLVING PROBLEMS

[0009] The present invention uses centralized management of addresses to achieve the capability for each terminal to be able to automatically add an address, or provide the capability to freely build a secure network by the self-learning function of a repeater without user expertise used to automate the function of operation maintenance management. The main technical feature and operation method provide everyone with the ability to easily build a secure network.

EFFECT OF THE INVENTION

[0010] The network environment maintenance system of the present invention has the advantage of simply building a free and secure network without user expertise.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011]

FIG. 1 is an entire configuration diagram according to an embodiment of the invention;

FIG. 2 is a method diagram illustrating initialization of a device;

FIG. 3 is a method diagram for determining an alive state of a device;

FIG. 4 is a method diagram for updating management information of a device;

FIG. 5 is a method diagram of administrator notification;

FIG. 6 is a method diagram of device connection authentication;

FIG. 7 is a method diagram of terminal software registration;

FIG. 8 is a method diagram of terminal software connection;

FIG. 9 is a method diagram 1 illustrating the terminal software cutting connection;

5 FIG. 10 is a method diagram 2 illustrating the terminal software cutting connection;

FIG. 11 is a method diagram 3 illustrating the terminal software cutting connection;

FIG. 12 is a method diagram of address conversion;

FIG. 13 is a transmission diagram for an address conversion;

FIG. 14 is a transmission diagram for an address conversion.

10 DETAILED DESCRIPTION OF THE APPLICATION

[0012] FIG. 1 is an overall schematic diagram of a network system according to one exemplary embodiment of the present invention.

The present invention is used to reduce the current complexity of network design, configuration, and workload management; to make networks logically isolated
15 from the Internet more efficient; and to provide the ability to protect against threats from the Internet via unified management network information. Operations center 101, certificate authority 102 and console 103 constitute the management network 104.

Terminal software 108 is software of the present invention which is installed in a PC or a terminal such as a multifunction portable terminal including a tablet, a
20 smartphone, and so on. PC 109 is a PC or a multifunction portable terminal including a tablet, a smartphone, etc., which does not install the software of the present invention connected to the network. Terminal software 108 and PC 109 are connected to the device 107 and the Internet 106 via a LAN 110. When the device 107 is connected to the operations center 101 via a management network 104 and is authenticated as a legitimate
25 user by a certificate authority 103, the device 107, etc., builds a real network 105, and

performs encryption communication and secure data exchange with terminal software 108 or PC 109 using a mesh-based real network 105.

[0013] Each software and device of the real network of the present invention named by the inventors and the applicants are described below.

5 **[0014]** · Operations center 101

The operations center 101 is used to manage network information, and has a real address management function used only in the real network of the present invention and used to construct a logically isolated network from the existing network. The operations center 101 includes a certificate authority 102 recording events occurring in
10 the network system 100 as a log, and a console 103 that allows the administrator to operate a GUI.

As shown above, the real addresses are re-managed in the present invention. When a communication apparatus, etc., operating in the present invention transmits data, identifiers of the apparatus, equipment, services, software, or the like used for specifying
15 destinations are used.

· Certificate authority 102

When the device 107, terminal software 108, PC 109, and so on, use the real network 105, the certificate authority 102 is a certification authority which has a public key certificate issuing and management function that is used to determine whether a
20 certificate is a certificate of the legitimate user.

· Console 103

The console 103 is a GUI client of the operations center 101, and is used to input, update, delete, refer and process data of the operations center 101, and apply the information of the operations center 101 to generate necessary information.

25 · Management network 104

To operate and manage the real network of the present invention, the console 103 is connected to the operations center 101, so that terminal software 108, PC 109, etc. obtain encrypted secure communication paths for certification from the certification authority 102 via the operations center 101.

5 · Real network 105

The real network 105 is a secure communication path of the present invention where encrypted communication is performed between the device 107 and the terminal software 108, PC109, etc.

 · Internet 106

10 The Internet 106 is a computer network using the Internet protocol.

 · Device 107

The device 107 has the ability to communicate with the operations center 101 and the ability to provide a security function and a control function of the real network 105 to control communication from the terminal software 108 and PC 109.

15 · Terminal software 108

The terminal software 108 is client software of the present invention, which is installed in the multifunction portable terminals including tablets, smartphones, etc.

 · PC 109

20 The PC 109 is a versatile device such as the multifunction portable terminals or the like, including tablets and smartphones.

 · LAN 110

The LAN 110 is a general local area network.

[0015] FIG. 2 is a diagram illustrating an initialization setting of the present invention. The purpose of the initialization setting is that operations center 101 sets the
25 owner information of the real network of the present invention which is safe and

constitutes a group under configuration of the owner when the real network of the present invention which is safe is newly built. The initialization setting installed in device 107 at each setting destination connects the device 107 at each setting destination to the Internet and reads an installation key to perform automatic settings, so that the device 107 is
5 connected to the management network for performing the settings.

[0016] In FIG. 2, an undertaker, a department name, a mail address, a FAX number, a TEL number, a general address, etc., are input as owner information of the operations center 101 by the owner information input 201. After receiving the owner information that has been input, a general address is converted to a unique real address used in the
10 real network of the present invention using a hash function, and real network information, such as a real network name, etc., which is used in the real network, is automatically generated. The owner information and the real network information are registered in the management information of the operations center 101 by the owner information registration 202. A device information input 203 illustrates inputting a setting position, a
15 serial number, and connection conditions for the general network as the device information of the device 107. Device information registration 204 illustrates that the received device information, protocols, gateways, etc., used as connection information for connecting the device 107 to the operations center 101 are registered into a database of the operations center 101. A temporary ID, a password, certificate information, etc.,
20 which are automatically generated, are used as the verification information, and are registered into an encryption database of the certificate authority 102. Connection information encryption 206 illustrates that the connection information used by the device 107 connected to the operations center 101 is encrypted by a common key encryption, and the encrypted information is written into the media. In this way, since the device 107
25 can perform the connection everywhere to connect to the operations center 101 by using

the connection information, the work efficiency can be increased if a position is set by the console 103. Furthermore, in the present invention, since the connection information is used as the initialization key when the device 107 is connected to the operations center 101, the encrypted connection information can be considered as the initialization key. An
5 transmission for mailing the initialization key 207 illustrates that the initialization key is transmitted to the administrator of the device which sets the destination through a mail. The connection information is encrypted via an encryption key by the encryption connection information 206. The encryption key is generated and shared by an independent algorithm. Mailing 208 illustrates that the management information written
10 into the operations center 101 is transmitted to the administrator of the device 107 which sets the destination by a mail. Information fetching 210 illustrates that the device 107 which sets the destination writes the initialization key received by the mail into an external memory medium. The external memory medium is connected to the device 107, and the initialization key and a common encryption key stored in the external storage
15 medium are read by decryption of the initialization key 211. Decryption of the initialization key 211 illustrates that the common encryption key in the external storage medium is used to decrypt the encrypted initialization key in the external storage medium, and obtains the information used for connecting the device 107 to the operations center 101. Connection to operations center 212 illustrates that the decrypted initialization key is
20 used for connecting the device 107 to the operations center 101 by encrypted communication. Authentication 213 illustrates that the temporary ID, the password and the certificate transmitted from the device 107 are used to identify the device 107. When the device 107 cannot be authenticated, error processing 214 is performed and error contents are output to the log. When the device 107 can be authenticated, the existing
25 address of the device 107, the real address of the present invention, etc., are generated by

a real network transmission 215. The real network information of the present invention is transmitted to the device 107. The device 107 receives the real network information by real network reception processing 216, and performs the initialization setting by device configuration processing 217, so that the device itself can be connected to the real network.

[0017] FIG. 3 is a diagram illustrating a device performing alive monitoring according to the present invention.

The operations center 101 and other devices 107 determine the alive state of the device 107. When the operations center 101 and other devices 107 determine that the device 107 is not suitable as a member of the real network, the device 107 referred to as a target is removed from the real network, and the remaining devices 107 are used to rebuild the real network of the present invention. The execution status is recorded in the log to notify the administrator of the status.

[0018] The status detection 301 of FIG. 3 shows that the device 107 regularly performs a self-detection by itself, checks the status of the device 107, and encodes the operational status predetermined with the operations center 101. The status notification 305 is that the encoded operational status is regularly transmitted to the operations center 101. Notification detection 306 illustrates waiting for notification of the operational status from the device 107 during a predetermined period of time. When notification of the operational status has not been received from the device 107 within the predetermined period of time, or when notification of the operational status has not been received from the device after transmitting a notification request for the operational status to the device 107, the information used to identify the device 107, which can be the setting position of the device 107 or the real address, etc., of the device 107 determined according to the present invention, is used as notification information of a non-operational status, and is

output to an error log. When notification of the operational status is received from the device 107 and the notification of the operational status contains errors, the information used to identify the device 107 can be used as error information and is output to the error log. When the notification information of the operational status from the device 107 contains a fatal error, the notification information of the operational status is considered as a fatal error and is recorded in the management information. When devices 107 other than device 107 generate the notification, since the device 107 generating the notification is unusable, all information illustrating that the device 107 is eliminated from the real network can be utilized. For notification detection 306, when the notification of the operational status from device 107 is received within a period of time and no error is contained in the notification of the operational status or when the information indicates that the setting content of the device 107 has changed, the operations center 101 compares the information of the device 107 stored in itself with the changed information and uses the changed information as new information of the device 107. Information change processing 314 illustrates that the management information of the operations center 101 is updated.

[0019] FIG. 4 shows that devices 107 in the same group obtain the management information from the operations center 101 to build a new real network when the management information of the operations center 101 is updated.

[0020] It is determined whether the management information is updated using management information determination 401. When it is determined that the management information has been updated, the management information is used as the transmission data by the management information conversion 402. The device 107 requests that the operations center 101 transmit the management information in a management information transmission request 403. The operations center 101 receiving the request transmits the

management information to the device 107 via a management information transmission 404. The device 107 receiving the management information executes a determination command of a communication status to the OS of the device 107 to obtain the latest information about how the communication status of device 107 is constituted, and
 5 compares the received management information with the communication status of the device 107 itself to recognize an increase or decrease in other devices 107. When a device 107 is removed from the management information, the device 107 cannot communicate with the device 107 which is the target. The operation center 101 is notified of an exclusion report of the subject device in an exclusion processing completion report
 10 410.

When a device is added, a device adding processing is performed. (Refer to FIG. 6).

The console performs a forced exclusion processing of the device 107 by a forced cut 412. Other devices 107 in the group of the device 107 which has been forcibly excluded are notified that the device 107 has been forcibly excluded. The console 107 receiving the
 15 notification cannot immediately perform any communication with the device 107 which has been forcibly excluded and notifies the operations center 101 of the exclusion report of the subject device in the exclusion processing completion report 410.

[0021] FIG. 5 illustrates that the operations center 101 reports an urgent error to the administrator when an emergency state is confirmed in the most recent log.

[0022] In a log processing of the operations center 101, the operations center 101 regularly confirms the logs stored in a database of the operations center 101. When a new log is added after the last confirmation, the operations center 101 reads the new log. When it is determined that the content of the new log is urgent by urgency determination processing 503, the urgent content is edited by notification content editing processing 504.
 25 Notification destination ensuring processing 505 is used to ensure notification of the

destination, and to notify the administrator via email, etc.

[0023] FIG. 6 illustrates that a new device 107 is confirmed and authenticated to be physically connected to the other device 107 for becoming a member of the new real network when the new device 107 is added to the same group.

5 **[0024]** When the new device 107 is added by using an alive confirmation, etc., the new device 107 can communicate with other device 107 to change the firewall settings in firewall setting 601 and firewall setting 603. The connection request 602 illustrates that the other device 107 transmits a communication connection request. Although the communication connection request is transmitted from each other, the device 107 on the
10 side that receives the communication connection request immediately switches to perform a connection response processing 604. The connection response processing 604 illustrates that the device 107 on the other side issues a notification of the connection preparation completion. The device 107 receiving the connection preparation completion from the device 107 at the other side transmits the ID, password, certificate, etc., to the
15 device 107 at the other side according to change management information received from the operations center 101 by authentication 605. The device 107 receiving the ID, password, certificate, etc., compares and confirms the change management information received from the operations center 101 with the ID, password and certificate by authentication OK 606. When the comparison confirmation cannot be performed, the
20 firewall setting is changed by an FW communication failure 607 to forcibly cut communication with the device 107 at the other side. When the comparison confirmation can be performed, the device 107 at the other side transmits communication permission in communication permission 608, and establishes an encryption communication in encryption connection 609 and encryption connection 610. The device 107 reports that
25 the encryption connection has been established to the operations center 101 by an

encryption connection completion report 611 and an encryption connection completion report 612. The operations center 101 receives the encryption connection completion report by receipt of the encryption connection completion report 613, and records a device adding completion record into the management information of the operations center 101 by a device adding processing completion record 614.

[0025] The purpose of FIG. 7 is to illustrate that the operations center 101 is instructed by the console 103 to publish a certificate of terminal software 108 and to encrypt the published certificate when the terminal software 108 is newly installed. The encrypted certificate and the connection completion used as the new terminal software 108 are transmitted to administrators who add a PC, etc.

[0026] A client certificate issue instruction 701 and a client certificate issue processing 702 indicate that when the new terminal software is installed in a PC and a multifunction portable terminal including tablets, smartphones, etc., the console 103 instructs the operations center 101 or the certificate authority 102 to perform client certificate issue processing 702 to create a version of the certificate. The certificate authority 102 assigns unique serial numbers to number the certificates and creates signatures for public key certificates, etc., as the certificates of the terminal software 108. Set information connection 703 is used to connect and use the certificates issued by the client certificate issue processing 702, the information of the operations center and the extended setting information as terminal software connection information. The terminal software connection information is encrypted by encryption 704. The terminal software connection information 705 is transmitted to the administrator of the terminal software 103 by transmission 705 using an email of the terminal software connection information, etc., or the encrypted terminal software connection information is written into the external memory medium and is transmitted by mail or another means. The administrator

of the terminal software 103 receives the terminal software connection information in the mail or by other means by reception 706 of the terminal software connection information, such as mailing, etc. The administrator of the terminal software 103 installs the terminal software in a PC or a multifunction portable terminal including tablets, smartphones, etc., by terminal software installation processing 707. Next, the administrator of the terminal software 103 inputs the encrypted terminal software connection information to a PC, or a multifunction portable terminal including tablets, smartphones, etc. for decryption to set the terminal software 103 by connection information decryption 708. ID creation 710 is used to create a unique ID of a PC, or a multifunction portable terminal including tablets, smartphones, etc., set by the terminal software. The terminal software connection information is used to connect to the operations center 101 by terminal software control center authentication 711. The authentication is requested, and the authentication confirmation is performed by authentication OK 712. When the authentication is confirmed, the terminal software is used as registration information by terminal software registration 713. Individual information, etc., of a PC, or a multifunction portable terminal including tablets, smartphones, etc., is registered into a database of the operations center 101, and terminal software 108 is notified that registration is completed. When the authentication fails by the authentication OK 712, the authentication which has failed is output to the error log, and the communication conforming to the terminal software is cut.

[0027] FIG. 8 illustrates cases where the terminal software 108 cuts the connection with the real network via the device 107, the device 107 performs operations according to a new situation notified by the operations center 101 when the console 103 adds or deletes a device 107, the device 107 is changed because of inappropriate factors, or the device 107 periodically issues a request to the operations center 101 and the operations

center 101 replies to the requests.

[0028] An authentication request 801 of FIG. 8 is used to request authentication connection from the terminal software 108 to the operations center 101. When authentication can be performed, the operations center 101 checks whether there is a device 107 connected to the terminal software 108 by a connection destination device confirmation 803. When no device 107 is connected to the terminal software 108, a destination without connection is transmitted to the terminal software 108 to cut the connection. When multiple devices 107 are connected to the terminal software 108, an optimal device 107 having a minimum number of connections at present is determined by an optimal device search 804. The connection information of the terminal software 108, such as global IP addresses and so on, is transmitted to the device 107 by a connection permission instruction 806. The firewall settings can be changed to accept communication with the terminal software 108 by connection preparation processing 807. In the stage at which the setting is completed, the device 107 reports to the operations center 101 and terminal software 108 that the connection preparation is completed by sending a connection preparation completion report 808. The operations center 101 indicates the connection methods, such as a general address for the device 107, to the terminal software 108 by notification of a connection destination device 809. The terminal software 108 determines a communication protocol in accordance with the received connection method, and transmits the ID, password, certificate, etc., to the device 107 by the transmission of connection authorization information 810. The operations center 101 confirms the received ID, password, certificate, etc., and transmits the confirmation to the terminal software 108 when the received ID, password, certificate, etc., can be confirmed. The terminal software 108 performs encryption communication with the device 107 by encryption data communication 812 and encryption data

communication 813. The device 107 transmits the received data to the destination.

[0029] The purpose of FIG. 9, FIG. 10 and FIG. 11 are to illustrate the connection being cut according to any indication or aggravation of connection status.

[0030] In FIG. 9, there is a connection cutting instruction in the terminal software 108 by a connection cutting instruction 901. A connection cutting message is transmitted to the device 107 by a connection cutting message 902. The device 107 receiving the connection cutting message cuts the connection to shut down a connection port of the terminal software 108 by a connection cutting processing 903. In a cutting report 904, the device 107 reports to the operations center 101 that the connection with the terminal software 108 has been cut.

[0031] FIG. 10 illustrates that the device 107 cannot communicate with the terminal software 108 according to aggravation of the connection status, etc., in the communication between the terminal software 108 and the device 107. It is determined whether the connection is interrupted by no response determination 1001. The device 107 performs alive monitoring to the terminal software 108 by confirmation 1002. The device 107 performs a cutting processing by cutting 1004 when the communication cannot be performed within a predetermined period of time. A cutting report is transmitted to the operations center 101 by a cutting report 1005.

[0032] In FIG. 11, the console 103 generates a cutting instruction for cutting the connection between the terminal software 108 and the device 107 by using a cutting instruction 1101. The console 103 instructs the device 107 to connect to the terminal software 108 via the operations center 101. The device 107 that receives the instruction performs the cutting processing using terminal software cutting 1104. The device 107 transmits a cutting report to the operations center 101.

[0033] FIG. 12 is used to solve the problem of duplicate network addresses which

occurs when a plurality of different networks are integrated into a single network based on different technical ideas, and is used to access addresses of multiple servers having different addresses by using a single real address of the present invention to achieve the purpose of reducing the number of addresses and reducing the cost, thereby simplifying the operation management.

[0034] An explanatory diagram illustrates that the terminal software 108 or the PC 109 transmits the data to the server 112 configuring the data for different networks. The terminal software 108 or PC 109 transmits the data to the device 107 by transmission 1201. The transmitted data is analyzed using data format analysis 1202 to determine if the data was transmitted to the server of the present invention or was transmitted to the general external network. The determination method is that the transmission destination address of the transmitted data is compared with a conversion table stored in device 107 in advance. When the transmission destination address is registered, the data is transmitted in the network of the present invention. When the transmission destination address is not registered, the data is transmitted in the general external network. When it is determined that the transmission is performed in the general external network, general network processing is performed and the data is transmitted to the external network.

When it is determined that the transmission is performed in the network of the present invention, a communication from the terminal software 108 or PC 109 to the server is performed at the real address which the opposing device 107 has. The real address is an address which does not exist in the network to which terminal software 108 or PC 109 (becoming a transmission source) belongs. By using this method, although the terminal software 108 or PC 109 and the server have duplicate addresses because of the duplicate networks to which the terminal software 108 or PC 109 and the server belong, the communication can be performed.

The device 107 performs an address conversion according to the conversion table stored in the device 107 in advance by address conversion A 1205, and transmits the address to the opposing device 107. Examples of conversion methods are described in FIG. 13. The reason for conversion is to enable a path from the device 107 to the opposing device 107 to be a communication path used in the general Internet, etc., so that a common communication apparatus can transmit the data to the opposing device 107. When the destination corresponds to the address in the conversion table, the device 107 receiving the data converts the address according to the conversion table using address conversion B 1205 and transmits the data to the server 112 which is the destination. In the invention, a match for the destination must be found in the conversion table since the data is divided into multiple packets for transmission/reception and status processing is performed. The server 112 receiving the data processes the data using data reception 1207, and generates reply data in a data reply 1208. The transmission destination address of the reply data is a transmission source for receiving the data. The transmission source is the server's own address, and it is used to transmit the reply data to the device 107. The device 107 receiving the reply data performs status processing via address conversion C 1209, converts the address, and transmits the data to the opposing device 107. Examples of the conversion methods are described in FIG. 14. The device 107 receiving the reply data performs the address conversion through the status processing by the address conversion D 1210, and transmits the data to the terminal software 108 or PC 109 which is a destination. The terminal software 108 or PC 109 receives the data via data reception 1211.

INDUSTRIAL APPLICABILITY

[0035] In the future, since more and more confidential communication technologies

related to the cloud services and cloud spaces used in Japan and abroad are expected to become popular, an installation operation which makes installation easy for persons without specialized knowledge is needed.

What is claimed is

1. A communication technology, used in a system for generating a unique address automatically to a dedicated network where an address has already been set to each PC, server, etc.,

5 managing addresses which have been set to the PC, the server, etc., and two addresses set in the present invention;

without changing the addresses which have been set, and using the addresses which have been set or the addresses set in the present invention for communication with safe confidentiality.

10 2. An address management technology, setting an address of a network where a device is installed to the device when the device is configured; storing the address set in the device by a control center;

creating multiple real addresses based on the addresses set to the device, and storing the real addresses in the device and the control center;

15 using the real addresses kept in the device and the control center as the real addresses of a PC, a server, etc., which is connected to the device;

dual-managing the addresses originally allocated from the existing network to the PC, the server, etc.

20 3. An automatic address-generation technology, automatically investigating, analyzing addresses and port numbers or identifiers in use and sifting addresses and port numbers or identifiers which are not in use based on addresses which have been allocated to the existing network;

using the addresses and port numbers or the identifiers as new addresses.

25 4. A communication technology, which is a technology integrating multiple different networks into a single network based on different technical ideas and ensuring data with safe confidentiality for communication;

receiving, by a device, a transmission request from a server, PC or terminal

software, etc., wherein the device analyzes the received data;
comparing the received data with a conversion table stored in the device;
transmission is performed in the server, PC, etc., which are set in the present
invention when a transmission destination address is registered;
5 transmission is performed in a general external network when the
transmission destination address is not registered;
when the transmission is performed in the general external network, the data
is transmitted to a general network like the same operation
performed by a general communication apparatus;
10 when the transmission is performed in the server, PC, etc., which are set in
the present invention,
to avoid address duplication which the general communication apparatus has
or violation of regulations of the general communication apparatus, a
transmission destination address and a transmission source address
15 of the data transmitted to the general network are converted into a
unique address which is stored in the device and is used for the
general communication apparatus to transmit the data to an opposing
device at the destination, and the data is transmitted to the opposing
device;
20 the opposing device receives the data, analyzes the transmission destination
address of the received data and uses a table stored in the device to
convert the transmission source address to an address which can be
recognized by a network which the opposing device belongs to, and
transmits the data to a server, PC, etc., at the destination, and the
25 server, PC, etc., receives the data;
the server, PC, etc., which receives the data, uses the same method used in
the general network communication to transmit reply data;
the transmission source used to receive the data is set as the transmission
destination, and the transmission destination is set to the addresses
30 which the server, or PC, etc., has; since the reply data is transmitted

to the opposing device, the opposing device receives the reply data to perform a status processing, converts the address, and transmits the reply data to the device; and the opposing device which receives the reply data performs the same processing, wherein the opposing
5 device converts the addresses by status processing, and transmits the data to the server, PC, or terminal software, etc., at the transmission source which is the destination;

the server, PC, or terminal software, etc., at the transmission source receives the data.

**COMMUNICATION APPARATUS, METHOD FOR CONTROLLING
COMMUNICATION BETWEEN DIFFERENT TYPES OF DEVICES, AND
METHOD FOR ELIMINATING SPECIFICITY OF OPERATIONAL
MANAGEMENT**

5

ABSTRACT

PROBLEM TO BE SOLVED: to achieve the maintenance, operation and monitoring of a network environment by: eliminating the specificity and complexity of operational management accompanying the connection of different networks; eliminating on-site installation/adjustment operations; and improving security.

10

SOLUTION: addresses for use only within a system are used to perform communications without using any addresses for use on the Internet or the like; any person can easily configure a network space on a group-by-group basis, e.g., a company-by-company basis, a department-by-department basis, or a project-by-project basis; path information or the like is registered with a center that manages a network; any connection between different types of devices can be implemented; relay apparatuses acquire path information and perform mutual verifications; and all information flowing through the paths are encrypted.

15

FIG. 1