Title: MONITORING SYSTEM AND METHOD FOR ACCESSING A MONITORING DEVICE OF A MONITORING SYSTEM

Abstract: A Monitoring system and a method in a monitoring system comprising a public network 4, a private network 2, an access limiting device 6 arranged to limit the access of the private network 2 from the public network 4, and a control server 20, 22, 24 connected to the public network 4. The monitoring system further comprises a monitoring device 10 connected to the private network and being arranged to send an HTTP request to the control server 20, 22, 24. The control server 20, 22, 24 being arranged to send a HTTP response to the monitoring device 10 in response to the HTTP request, wherein the content length of the HTTP response is not defined or wherein the content length is set to a number that is large enough to enable transport of a plurality of future control messages as part of an over time stretched HTTP response resulting in an open path from the control server 20, 22, 24 to the monitoring device 10 through the access limiting device 6 and wherein the control server 20, 22, 24 is arranged to send control messages to the monitoring device 10 via said open path.
MONITORING SYSTEM AND METHOD FOR ACCESSING A MONITORING DEVICE OF A MONITORING SYSTEM

Technical Field of the Invention

The present invention relates to a monitoring system including a public network, a private network, and an access limiting device arranged to limit the access of the private network from the public network. Further the present invention relates to a method for accessing a monitoring device of such a monitoring system from the public network.

Background of the Invention

Monitoring systems for monitoring of premises, areas of particular interest and processes by means of cameras connected directly to computer networks are increasingly popular. One reason for this may be that these systems in great extent may utilize an existing network, if a computer network already is in place. Another reason may be that the network that has to be built for the monitoring system may be used to connect other types of equipment, e.g. computers, servers and peripherals.

In many cases the users of the monitoring system or a central control centre responsible for the monitoring of the premises, areas of particular interest or processes are located remotely from the monitored site. As a result of the monitoring system being based on a computer network a remote user or a remote control centre may be easily connected to the monitoring system via the Internet. However, most private networks, home networks, corporate networks, etc. are connected to the Internet via some device that limits the access to the network from the Internet. Such an access limiting device may be a firewall, a router implementing NAT (Network Address Translation) to provide additional IP addresses on the
private network, a proxy server or an Internet Service Provider (ISP) providing dynamic IP-addresses.

Thus, one problem of such a monitoring system is that many functions, e.g. control of the monitoring device or devices, require transactions initiated by either the control centre or the remote user and that the monitoring device or devices are arranged in a private network behind an access limiting device. Accordingly, the control centre or the remote user either are unable to penetrate the protection installed or do not have knowledge of the address of the monitoring device or devices. A firewall may be modified to pass through communication originating from outside the private network. Such modifications may however be difficult, either because the firewall is not within the control of the user, because the user do not want to open the firewall, or because the user do not know how or do not want to go through the trouble of modifying the firewall.

One way of making it possible for servers to communicate with clients otherwise inaccessible is described in the patent application US 2004/0044771 A1. The document describes that a persistent network connection from the client to the server is established. Further, it describes that such a scheme may work fine for a small number of clients, but that the server will soon be overloaded for a large number (i.e. thousands or more) of clients connecting to a single server.

However, the document do not describe how to implement a persistent network connection to otherwise inaccessible network devices.

Summary of the Invention

One object of the present invention is to provide an improved computer network based monitoring system.

The object is achieved by means of a method for accessing at least one monitoring device of a monitoring system according to claim 1 and by means of a monitoring
system according to claim 11. Embodiments of the invention are disclosed in the dependent claims.

In particular, according to a first aspect of the invention, the object is accomplished by means of a method for accessing at least one monitoring device of a monitoring system wherein the monitoring system comprises a public network, a private network, an access limiting device arranged to limit the access to the private network from the public network, a monitoring device connected to the private network, and a control server connected to the public network. The method comprises sending an HTTP request from the monitoring device to the control server, sending, in response to said HTTP request, an HTTP response in which the content length is not defined or in which the content length is set to a number that is large enough to enable transport of a plurality of future control messages as part of an over time stretched HTTP response, thereby achieving an open path from the server to the monitoring device through the access limiting device, and sending a plurality of control messages to the monitoring device from the control server via said open path.

According to a second aspect of the invention the object is accomplished by means of a monitoring system comprising a public network, a private network, an access limiting device arranged to limit the access of the private network from the public network, and a control server connected to the public network. The monitoring system being characterized by a monitoring device connected to the private network and being arranged to send an HTTP request to the control server, said control server being arranged to send a HTTP response to the monitoring device in response to the HTTP request, wherein the content length of the HTTP response is not defined or wherein the content length is set to a number that is large enough to enable transport of a plurality of future control messages as part of an over time
stretched http response resulting in an open path from the control server to the monitoring device through the access limiting device and wherein the control server is arranged to send control messages to the monitoring device via said open path.

One advantage of providing an open path from the control server to the monitoring device by means of responding to an http (Hyper Text Transport Protocol) request with an http response as described above is that the http request is a type of message that almost always are allowed to be sent out through a firewall or any other access limiting device. Therefore, the creating of the open path by sending the http request from the monitoring device to the control server and responding from the control server with said http response results in a simple and effective way to create the open path through the access limiting device from the control server to the monitoring device. Accordingly, the setup of the monitoring system becomes simple because there is no need for tampering with access limiting devices in order to make control server initiated transactions possible. Especially, the setup of the monitoring device becomes simple and the security of the private network do not need to be affected.

According to one embodiment the http request initiating the setup of the open path is sent from the monitoring device as soon as a network connection is detected. This makes it even more simple to setup the monitoring devices. The simplicity of setting up the monitoring device may be particularly interesting for small business or monitoring systems for homes.

According to a further embodiment said http request is sent to a control server indicated as a first choice in a list of control servers stored in the monitoring device. This feature also contribute to simplifying the installation of the monitoring device. Further, this may facilitate load control of the system.
According to yet a further embodiment the method further comprises the acts of:

sending a control message from a first server, which is currently enabled to send control messages to the monitoring device via the open path, wherein the control message includes instructions to the monitor device to move the open path from the first control server to a second control server,

terminating the connection that generated the open path and, thus, terminating the open path.

sending an http request from the monitoring device to the second control server,

sending, in response to said http request, an http response from the second control server in which the content length is not defined, thereby achieving an open path from the second control server to the monitoring device through the access limiting device, and

sending a plurality of control messages to the monitoring device from the second control server via said open path after the http response has been sent.

By providing a method like this it becomes possible to balance the network load of the system dynamically in spite of the fact that the monitoring device is arranged on a private network behind an access limiting device, i.e. if the load on the control server or on the public network path to the control server becomes to high.

According to a further embodiment the control server to move the open path to are selected by the monitoring device from a list of control servers stored in the monitoring device. The selected control server is then set to be the control server of first choice and the setting is stored in the list in the monitoring device. The advantage of this is that the risk of unnecessary load on the network or to specific servers are minimized, because the load of the control server initiating the move or the network path to that control server is probably high even after the monitoring device has been
disconnected and reconnected, in which event the monitoring device will connect to a control server experiencing less load.

A further scope of applicability of the present invention will become apparent from the detailed description given below. However, it should be understood that the detailed description and specific examples, while indicating preferred embodiments of the invention, are given by way of illustration only, since various changes and modifications within the spirit and scope of the invention will become apparent to those skilled in the art from this detailed description.

Brief Description of the Drawings

Other features and advantages of the present invention will become apparent from the following detailed description of a presently preferred embodiment, with reference to the accompanying drawings, in which

Fig 1 is a schematic diagram of one embodiment of a monitoring system according to the present invention,

Fig 2 is a timing diagram over one embodiment of the signaling between the monitoring device and the control server resulting in the open path,

Fig 3 is a timing diagram presenting a possible signaling scheme for checking the open path,

Fig 4 is a schematic diagram of one embodiment of a monitoring system according to the present invention,

Fig 5 is a schematic block diagram of one embodiment of the monitoring device.

Detailed Description of a Presently Preferred Embodiment

One embodiment of a monitoring system according to the invention is shown in Fig 1. The monitoring system includes a private network 2, e.g. a Local Area Network (LAN) arranged in a home, at an office, in a factory, in a park or a garden, at a car park, or in any
area or premises that is interesting to monitor. The private network 2 is connected to a public network 4, e.g. the Internet, via an access limiting device 6, e.g. a firewall, a NAT (Network Address Translation), a proxy server, an ISP (Internet Service Provider) providing dynamic addresses. The access limiting device 6 is limiting the access to the private network 2 from the public network 4 in different ways depending on the specific type of limiting device. For example, a firewall is generally arranged to prohibit access to devices in the private network from a public network.

Further, the system includes at least one monitoring device 10, which is associated with a specific area or a process, connected to the private network 2 for providing monitoring information via the private network. The monitoring device 10 is arranged to be controlled by a user by means of a terminal 14, 16 and the monitoring device may, for example, be a camera, a central unit of an alarm system, an IR-detector, a temperature sensor etc., which is enabled to communicate over the private network 2. The terminal 14, 16 may be a computer 14, a workstation 14, a computerized control centre, a mobile telephone 16, a PDA (Personal Digital Assistant), etc. and is connected to the public network 4.

Further, in order to enable the terminal 14, 16 to control and access the monitoring device 10 through the access limiting device 6 at least one control server 20 is connected to the public network 4.

As mentioned above the access to the devices on the private network 2 from devices on the public network 4 is barred by the access limiting device 6. In order to make it possible for the user to control the monitoring device the terminal 14, 16 of the user has to be able to initiate communication with the monitoring device 10. This should be enabled without affecting the available bandwidth on the network to any greater extent and, thus, this function should not involve unnecessary usage of
bandwidth. To make this possible a control connection from the server 20 to the monitoring device 10 through the access limiting device is set up by making the monitoring device 10 send an http request 52 to a control server 20 see Figs 1 and 2. The http request may be sent by the monitoring device 10 upon power up 50, upon detection of a network connection, upon pressing a button, upon keying a code, upon receipt of detection event indicating an alarm, etc. An event indicating an alarm may be a signal from an internally or externally, in relation to the monitoring device, arranged sensor or a state in a program triggering an alarm.

The control server 20 then respond to this request by sending an "endless" http response 54 to the monitoring device 10. The length of the content of the endless http response 54 is not specified or may be specified as a large number in the http response and, thereby, the underlying TCP connection is not terminated by the control server. This results in that the access limiting device 6 and the monitoring device 10 do not consider the response terminated and, thereby, an open path from the control server 20 through the access limiting device 6 and to the monitoring device 10 is created. In the case of the content length being specified as a large number, the response is not terminated until the amount of data corresponding to the large number has been sent. The control server utilizes the open path to control the monitoring device 10 by sending control messages 56 (control message 1-N) to the monitoring device, wherein N is an unlimited number. The control messages 56 may be initiated by the control server 20 by it self or by a user terminal 14, 16. As a result of the open path the control server 20 is able to send control messages 56 at any time, i.e. the server do not have to wait for any polling signal from the monitoring device and, thus, there is essentially no latency. Accordingly, a user requesting monitoring data
from a monitoring device 10 using a user terminal 14, 16 would essentially only experience the latency resulting from the transport of the request, the processing in the monitoring device and the transport back to the terminal. This also results in less traffic being transported in the network.

The http response, which is creating the open path, may also be described as an http response including a plurality of control messages 56 dispersed in time or as an http response in which the content length is set to a number that is large enough to enable transport of a plurality of future control messages as part of an over time stretched http response. This may be achieved by not defining the length of the content of the http response or by setting the length of the content of the http response to a large number. In the case of setting the length of the content to a large number, the large number is to be selected so large as a plurality of control messages 56 may be sent by means of the http response without termination of the http response and consequently the open path. In some cases such a large number may be 18 kilobytes, if the initial packet of the http response only is some bytes and if the subsequent control messages also are rather small. However, such a large number may also be two megabytes or greater if the control messages are of larger size. Additionally, the size of the length of the content also depends on the desired duration of the open path. In some applications the network load is not much affected if a new open path is set up once every hour, but in other applications it may be desirable to keep the open path open for a day or more in order not to noticeably affect the network load.

Accordingly, the open path is the communication link into the private network 2 for control server 20 or terminal 14, 16 initiated messaging, as depicted by the control message 56 I-N in Fig 2. The control messages 56 may be utilized to control the monitoring device from a
terminal of the user, such instructions are relayed or translated and sent via the open path by the control server. Further, the control messages 56 may be utilized to check the status of the monitoring device 10, to test that the monitoring device is operating correctly, to control the status of the open path connection, to provide configuration data to the monitoring device, to request the monitoring device 10 to set up a new or other connection or to request the monitoring device to deliver data, e.g. monitoring data or other data of interest, to a specific destination.

In one embodiment the control server 20 is arranged to frequently initiate a check of the open path connection in order to determine if the connection has been broken or for any reason terminated. The check is initiated by the control server which sends a control message 56, including instructions and data associated with the check, via the open path. The monitoring device is programmed to expect frequent reception of such a control message.

Such a check may be implemented in many different ways. For instance the server may be provided with a timer 106 triggering the sending of the control message 100, including check data, see Fig 3. The period set for the timer 106 may be $t_s$. The monitoring device may also be provided with a timer 108 that will be reset 104 each time the monitoring device receives the control message 100 including control data. The time period set for the monitoring device may be $t_m$, wherein $t_m = t_s + \Delta t$. $\Delta t$ is a short time period in relation to $t_s$, this time period $\Delta t$ only have to be long enough to compensate for possible delays in transmission of the control message.

In Fig 3 there is shown a control message 100 including checking data. At the same time as the control message 100 is sent the timer 106 is started. When the control message 100 is received at the monitoring device
the timer 108 at the monitoring device is started. Then, \( t_s \) time units after the timer 106 of the control server was started the timer 106 triggers the sending of the next control message 101, including checking data, and the timer 106 of the control server is restarted. When the control message 101, including checking data, is received at the monitoring device the timer 108 at the monitoring device is reset and restarted, before it has timed out. Then, \( t_g \) time units after the timer 106 of the control server was restarted the timer 106 triggers the sending of the next control message 102, including checking data, and the timer 106 of the control server is restarted once more. In this example the control message 102 does not reach the monitoring device for some reason and this leads to the timer 108 of the monitoring device timing out after \( t_m \) time units. When the timer 108 of the monitoring device has timed out the sending of a new HTTP request 52 is triggered in order to try to re-establish the open path between the control server and the monitoring device. If the control server is down or the HTTP request is not arriving at the control server the monitoring device may try to connect to another control server, e.g. in a manner as described in this description.

The check may be performed once every 2 minutes in order not to load the network to the extent that the check is decreasing the capacity of the network, i.e. \( t_s = 2 \) minutes. However, the check may be performed more frequently, e.g. once every 20 seconds \( (t_s = 20 \) seconds), if the check does not result in a load decreasing the capacity of the network noticeably.

According to one embodiment an address to the control server 20 is stored in the monitoring device 10 and the address is used by the monitoring device 10 when sending the HTTP request for setting up the open path for the control messages described in relation to Fig 2. The address may be an IP address (Internet Protocol address)
or an URL (Uniform Resource Locator). This embodiment may be used independently of how many control servers there are available on the public network.

Independent of embodiment the final responsibility for the open path lies in the monitoring device, because the open path may only be initiated from the monitoring device. Accordingly, if the connection is broken, for some reason, the monitoring device has to initiate the setup of a new connection.

In Fig 4 there is shown a monitoring system including a plurality of control servers. The monitoring system is identical to the system presented in Fig 1 with the difference that it includes a first control server 20, a second control server 22 and a third control server 24. The monitoring device 10 may be arranged to send the initiating message to one of the control servers 20, 22, 24 in accordance with the description above or in accordance with any of the descriptions below. In the figure there is shown three control servers 20, 22, 24.

However, the system may only include two control servers or the system may include four control servers. Depending on the circumstances it may be optimal to provide more than four control servers to the monitoring system.

In this embodiment a change of the control server associated with the monitoring device includes sending of a control message from the present control server 20, i.e. a first control server 20, to the monitoring device 10 including a request to terminate the connection to the first control server 20 and initiate a connection to an address provided in the control message, which may be the address of the second control server 22. Then the monitoring device 10 terminates the connection, including the open path, to the first control server and sends an http request to the address provided by the first control server. Then the second control server receives the http request and sets up the open path in accordance with the description of Fig 2. One advantage of providing a
plurality of control servers and the method of changing control servers is that it makes it possible balance the load of different parts of the network. Another advantage is redundancy of control servers, i.e. a control server may always be available even if some are not available. A control server may be unavailable because of overload, because it is out of order, because of interrupted network connection, etc. Yet, another advantage may be the use of specialized control servers. For instance, one subset of control servers may be specialized in handling video and one subset may be specialized for other purposes. In this way there is no need to pay for licenses relating to some specific functions, programs or hardware for all control servers.

In another embodiment a plurality of control server 20 addresses are stored in a list in the monitoring device 10. The addresses in the list are prioritized, i.e. there is a first choice address, a second choice address, etc., the number of addresses in the list are equal to or less than the number of control servers 20 on the public network associated with the monitoring system. In this embodiment the monitoring device is arranged to make the initial http request to the control server 20 that is the first choice according to the list in order to establish the open path from the control server 20, i.e. the first control server 20, to the monitoring device. If this attempt fails the monitoring device is arranged to make the initial http request to the control server 22 which is the second choice according to the list, i.e. the second control server. If there are more failures with the initial http request and if there are additional control servers in the list the procedure may continue until there is no further control servers or the open path has been established.

Further, assume the open path was established by the first control server 20, but the load on the control
server or the portion of the public network that the
first control server is connected to is too high. Then
the first control server may send a control message to
the monitoring device requesting it to connect to the
second control server 22 by requesting the monitoring
device to change control server. The monitoring device
then terminates the connection and sends the initial http
request to the second choice in the list stored in the
monitoring device 10.

By implementing said prioritized list of control
servers in the monitoring device there is less risk that
a monitoring device is not able to connect to a control
server as a result of one specific control server not
being currently available. Additionally, less data need
to be sent to the monitoring device 10 when a change of
control server is needed because of high load, thus,
minimizing the contribution to the high load condition.

When a change of server has been made for a
monitoring device 10 including a prioritized list, the
prioritized list may be amended. The second control
server 22 may, for example, be entered as the control
server of first choice and accordingly the first control
server is entered as a control server of lower priority.
The amended list is then stored in the monitoring
device 10. The advantage of such an amendment of the
prioritized list is that if the monitoring device is
powered down or disconnected from the network and then
powered up or reconnected to the network the setup
sequence of the open path does not have to be performed
towards a control server that possibly still is
experiencing a high load but to the same control server
from which the latest open path was established
successfully.

A redirecting message, including instructions
ordering the monitoring device to connect to another
control server, may be provided in a control message or
in the http response initiating the open path.
According to one embodiment the monitoring device is a network enabled camera. In cases of the monitoring device being a camera the load balancing becomes even more important because of the large amount of monitoring data, i.e. a video sequence, images, streaming video, etc., it may send to the control server upon request and, thus, introducing large loads to the portion of the public network where the control server is connected or to the control server itself.

According to one embodiment a monitoring device, which may be a camera, may comprise the following features, in addition to the features required to perform the specific task of the monitoring device: a control server communication program 202, a web-server 204, URL addressable storage means 205, and a network interface 211, see Fig 5. The web-server 204 and the control server communication program 202 may be implemented as software functions processed by a processor of the monitoring device, but may also be implemented by means of hardware. The control server communication program 202 is arranged to send the initial http request for setting up the open path and to translate instructions received via said open path to http messages for sending to the web-server 204. The monitoring device and, thus, the control server communication program 202 and the web-server 204 are connected to the private network 212, via the network interface 211. The web-server 204 handles the http requests by either loading or storing data in the URL addressable storage means 205: The URL addressable storage means may include a URL for first monitoring data 206, which may be one type of data generated by the monitoring device 10, a URL for second monitoring data 208, which may be another type of data generated by the monitoring device 10, and an URL for configuration data 210. Monitoring data may, for example, be video images or sequences.
According to another embodiment the monitoring device additionally may include a media server implementing RTSP (Real Time Streaming Protocol) or the web-server 204 may be replaced by such a media server.

An embodiment of a method to request monitoring information from a monitoring device 10 by means of a terminal 14, 16 by referring to Fig 1 will now be described. The method may be used in systems comprising a plurality of control servers 20, a plurality of monitoring devices and a plurality of terminals as well as in a system as depicted in Fig 1. The open path between the control server 20 and the monitoring device 10 has been set up in accordance with the description of Fig 2.

The user of the terminal 16 decides that he wants monitoring data from a specific monitoring device. The terminal 16 sends an http get to the control server 20 specifying the wanted data. The control server 20 receives the http get, assigns the connection established by the http get from the terminal a session identity, and translates the http get to a control message for sending via an open path to the specified monitoring device. The control message includes a command specifying the action to be taken, in this example the action is to retrieve data, a URL identifying the data to retrieve and a destination URL, specifying an address at a control server 20 to which the data are to be returned and specifying the session identity. The control message is sent to the monitoring device and the monitoring device performs the specified action by retrieving the monitoring data identified by the URL identifying the data to retrieve. The monitoring device then generates an http post directed to the destination URL included in the control message, thereby sending the data to the control server 20. The control server receives the http post including the monitoring data. Then the control server 20 uses the session identity of the URL in the http post
from the monitoring device 10 to generate a response to
the http get from the terminal 16 including the requested
data.

The monitoring device may include a program that
interprets the control message sent from the control
server in the example above. Such a program may be
arranged to identify the action to perform, in the above
case to retrieve data, and then translate the URL
identifying the data to retrieve to a location within the
monitoring device from which the requested data is
retrievable. Then the requested monitoring data is
included in a http post message sent to the destination
URL, as described in the above example.

According to another embodiment the monitoring
device may be a monitoring device that is designed as the
one described in Fig 5. When such a monitoring device is
used in the example of retrieving monitoring data above,
the monitoring device receives the data of the control
message, at the control server communication program 202,
and translates the data to an http get to the URL
identifying the data to retrieve. The http get is then
sent to the embedded web-server 204. The web-server 204
then handles the http get in a way known to the person
skilled in the art and returns the requested monitoring
data to the control server communication program 202
which generates and sends a http post, including the
monitoring data, to the destination URL.

In one embodiment the monitoring device 10 is
provided with an electronic serial number identifying the
device. The serial number may be stored in the monitoring
device 10 during manufacturing and may be used to
identify the monitoring device 10 during the setup of the
connection resulting in the open path.

Additionally, the monitoring device may be provided
with a unique key for encrypting messages to be sent or
for decrypting received messages. This key may also be
utilized to authenticate the camera during the setup of
the connection resulting in the open path. The control server is also provided with a key in order to be able to decrypt messages from the monitoring device, to encrypt messages sent to the monitoring device and to authenticate the monitoring device 10. Thereby all communication between the monitoring device and the control server may be encrypted. Preferably there is provided a unique key for each monitoring device produced and the key may be stored in the monitoring device during manufacturing of the device. The keys may be keys of a shared secret system or a public key system.

According to one embodiment a very large list of different keys are generated before the manufacturing of the cameras which are to be provided with these keys. The list should be of such a size that no new list has to be generated for years. Each control server is provided with the list of keys and during the manufacturing of a monitoring device the device will be provided with one of the keys. By providing the keys in this way there is no need for distribution of keys, which may be a safety hazard. Accordingly, authentication of monitoring devices and the distribution of keys may be simplified.
CLAIMS

1. Method for accessing at least one monitoring device of a monitoring system wherein the monitoring system comprises:
   a public network,
   a private network,
   an access limiting device arranged to limit the access to the private network from the public network,
   a monitoring device connected to the private network, and
   a control server connected to the public network,
   said method comprising:
   sending an http request from the monitoring device to the control server,
   sending, in response to said http request, an http response in which the content length is not defined or in which the content length is set to a number that is large enough to enable transport of a plurality of future control messages as part of an over time stretched http response, thereby achieving an open path from the server to the monitoring device through the access limiting device, and
   sending a plurality of control messages to the monitoring device from the control server via said open path.

2. Method according to claim 1, wherein the control messages is sent at different points in time via the same open path that has been initiated by the http request.

3. Method according to any one of claims 1 or 2, wherein said sending of the http request from the monitoring device to a control server is performed as soon as the monitoring device detects that it is connected to a network.
4. Method according to any one of claims 1-3, wherein the sending of the http request from the monitoring device to the control server is made to a control server that is indicated as the first choice in a list of control servers stored in the monitoring device.

5. Method according to any one of claims 1-4, wherein the method further comprises the acts of:

- sending a control message from a first server, which is currently enabled to send control messages to the monitoring device via the open path, wherein the control message includes instructions to the monitor device to move the open path from the first control server to a second control server,
- terminating the connection that generated the present open path and, thus, terminating the open path,
- sending an http request from the monitoring device to the second control server,
- sending, in response to said http request, an http response from the second control server in which the content length is not defined, thereby achieving an open path from the second control server to the monitoring device through the access limiting device, and
- sending a plurality of control messages to the monitoring device from the second control server via said open path after the http response has been sent.

6. Method according to claim 5, wherein the instructions in the control message from a first server regarding moving the open path to a second server includes an address to the second server.

7. Method according to claim 5, wherein the method further comprises the act of selecting, by the monitoring device, the second control server from a list of control servers stored in the monitoring device.
8. Method according to claim 7, wherein the method further comprises the act of placing the second control server as the first choice in said list of control servers and storing the amended list in the monitoring device.

9. Method according to any one of claims 1-8, wherein the method further comprises:
   receiving an http request at the server from a user terminal, said http request including a request for monitoring data,
   associating the http request from a user terminal with a session number,
   translating the request for monitoring data to a data source URL of the monitoring device identifying the location of the requested data in the camera,
   sending a control message from the server to the monitoring device, said control message including said data source URL and a destination URL, which identifies a network address of the control server and the session number,
   retrieving, at the monitoring device, the requested monitoring data in accordance with the source URL,
   sending an http message including the requested monitoring data from the monitoring device to the control server by using said destination URL, and
   sending an http response from the control server in response to the http request associated with the session number of the destination URL of the http message from the monitoring device, said http response including said requested monitoring data.

10. Method according to any one of claims 1-9, wherein the monitoring device is a network enabled camera.
11. Monitoring system comprising:
a public network,
a private network,
an access limiting device arranged to limit the
access of the private network from the public network, and
a control server connected to the public network,
the monitoring system being characterized by:
a monitoring device connected to the private network
and being arranged to send an HTTP request to the control
server,
said control server being arranged to send an HTTP
response to the monitoring device in response to the HTTP
request, wherein the content length of the HTTP response
is not defined or wherein the content length is set to a
number that is large enough to enable transport of a
plurality of future control messages as part of an over
time stretched HTTP response resulting in an open path
from the control server to the monitoring device through
the access limiting device and wherein the control server
is arranged to send control messages to the monitoring
device via said open path.

12. Monitoring system according to claim 11, wherein
the control server is arranged to send a plurality of
control messages from the control server to the
monitoring device via the open path and at different
points in time.

13. Monitoring system according to any one of claims
11-12, wherein the monitoring device is arranged to send
the HTTP request as soon as the monitoring device detects
that it is connected to a network.

14. Monitoring system according to any one of claims
11-13, wherein the monitoring device includes a list of
control servers, the priority of the control servers of
the list is indicated in the list, and wherein the monitoring device is arranged to send the http request initiating the open path to the control server that is indicated as being the first choice in the prioritized list.

15. Monitoring system according to any one of claims 11-15, wherein the monitoring device is a network enabled camera.
INTERNATIONAL SEARCH REPORT

PCT/SE2005/002026

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L, G08B, H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE, DK, FI, NO classes as above

Electronic database consulted during the international search (name of database and, where practicable, search terms used)

EPO-INTERNAL, WPI DATA, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>US 6553422 B1 (D.S. NELSON), 22 April 2003 (22.04.2003), paragraph (0027) - (0043)</td>
<td>1-15</td>
</tr>
</tbody>
</table>

[X] Further documents are listed in the continuation of Box C.  [X] See patent family annex.

* Special categories of cited documents:
  "A" document defining the general state of the art which is not considered to be of particular relevance
  "B" earlier application or patent but published on or after the international filing date
  "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
  "O" document referring to an oral disclosure, use, exhibition or other means
  "P" document published prior to the international filing date but later than the priority date claimed
  "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
  "X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
  "Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
  "&" document member of the same patent family

Date of the actual completion of the international search
21 April 2006

Date of mailing of the international search report
24 April 2006

Name and mailing address of the ISA/Swedish Patent Office
Box 5055, S-102 42 STOCKHOLM
Facsimile No. +46 8 666 02 86

Authorized officer
Anders Edlund / MN
Telephone No. +46 8 782 25 00
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
</table>
International patent classification (IPC)

H04L 29/06 (2006.01)
G08B 25/08 (2006.01)
H04L 29/08 (2006.01)
H04N 7/18 (2006.01)

Download your patent documents at www.prv.se
Cited patent documents can be downloaded at www.prv.se by following the links e-tjänster/anförda dokument. Use the application number as username. The password is knxf0q4w86.

Paper copies can be ordered at a cost of 50 SEK per copy from PRV InterPat (telephone number 08-782 28 85).

Cited literature, if any, will be enclosed in paper form.
| Country | Publication Number | Date      | Corresponding Application
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>20020194289</td>
<td>19/12/2002</td>
<td>NONE</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>US 7003798 B 21/02/2006</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>JP 2002328886 A 15/11/2002</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>JP 2002328887 A 15/11/2002</td>
</tr>
<tr>
<td>US</td>
<td>6349336 B1</td>
<td>19/02/2002</td>
<td>DE 10052945 A 30/08/2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>JP 2001273211 A 05/10/2001</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DE 10000589 A,C 02/11/2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FR 2792801 A 27/10/2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>JP 3375934 B 10/02/2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>US 6553422 B 22/04/2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FR 2792801 A 27/10/2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>JP 3375934 B 10/02/2003</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>US 6349336 B 19/02/2002</td>
</tr>
<tr>
<td>US</td>
<td>20020038371 A1</td>
<td>28/03/2002</td>
<td>GB 0019959 D 00/00/0000</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GB 2366163 A 27/02/2002</td>
</tr>
</tbody>
</table>