

**SECURITY OF DATA THROUGH WIRELESS ACCESS POINTS
SUPPORTING ROAMING**



G00002

Field of the Invention

5

This invention relates to the field of wireless communications, and wireless access to the resources of wired networks. It relates particularly to the security of data transmitted through wireless access points that support roaming of wireless devices.

10



159159

Background of the Invention

Wireless communications is a burgeoning field. Personal computers, laptops, personal digital assistants, telephones and remote control devices are but a few of the types of device that are being used in a wireless environment.

In office and, to a lesser extent, home environments, such devices are supported by wireless Local Area Networks (LANs). A contemporary international Standard for wireless LANs is IEEE 802.11b. In the 802.11b Standard, wireless client stations (STA) connect to the access points (AP) to access services in the wired backbone. Access points are essentially STAs that provides access to the distribution systems (DS, or more commonly known as the wired LAN, such as Ethernet). This Standard thus provides a similar set of services offered by a physical Ethernet point but at the wireless level. Together with this, the Standard also defines an Extended Service Set (ESS) to allow multiple LAN to form a single virtual AP.

The advantage of wireless LAN systems is that a user enjoys the benefits of Ethernet while at the same time is free to roam within the serviced area. The approximate wired equivalent of this scenario is a user being able to move about and plug his Ethernet cable into any available network point.

However, the wireless LAN environment also presents new security issues that need to be addressed. Unlike wired LAN systems, wireless LAN systems do

not recognize physical wall boundaries. In a wired LAN system, an outsider cannot easily gain access to the internal network because of the physical security available (e.g. walls and security guards). However, outsiders can easily access wireless LAN systems since walls do not block the passage of radio frequency (RF) signals of wireless LAN systems to the outside world. Because of this, the IEEE 802.11 Standards Committee also defined an optional Standard called Wireless Equivalent Privacy (WEP) to provide data confidentiality for a 802.11 wireless LAN system. The problem is that WEP is weak and can be easily broken. Another problem with WEP is that its integrity is difficult to maintain because it is based on a shared secret key system; it is easy for one person to keep a secret, but it is not practical for a company with hundreds of employees to try to keep a secret.

One known solution to the security problem is to implement a firewall router at APs. The idea is to limit the number of services offered to wireless LAN users. The wireless LAN users can only access a wider range of services by creating a virtual private network (VPN) by tunneling a VPN protocol through this wireless firewall router. The VPN solves the problem of privacy and confidentiality, as an outsider who attempts to gain access to the wireless LAN systems will be blocked at the firewall. Also, any attempts to 'sniff' or eavesdrop on the data packets will be frustrated, as these packets will be encrypted within the VPN tunnel.

Examples of known VPN solutions include Point-to-Point Tunneling Protocol (PPTP) and IPSec, which interface to TCP/IP (i.e. at the network layer). Many Windows™ operating systems have built-in PPTP clients.

The problem with a firewall router AP solution, however, is that the users will no longer enjoy seamless roaming over the wireless LAN system. A firewall router operates at the network layer (or the IP layer in the case of the TCP/IP standard). When the user moves out of the range of one AP to another AP they will need to reconnect because the network layer address (e.g. IP address) will have changed.

Typical firewall implementations that are available from open sources (freeware) are Linux™, FreeBSD and OpenBSD. These implementations work by filtering network layer packets. They are also capable of stateful inspection of VPN packets such as PPTP and IPSec.

5

The present invention is directed to overcoming the problem of security of data and, at the same time, avoiding the deficiency of the firewall router approach so far as roaming is not possible.

10 Summary of the Invention

Therefore, the invention discloses a method for establishing data access for a wireless device to a wired network resource via a wireless access point, comprising the steps of:

- 15 establishing a firewall, at or above the data link layer, in said access point to pass only virtual private network data packets;
- connecting the wireless device to a server on said wired network via said access point at the data link layer;
- allocating a network layer address to the wireless device; and
- 20 establishing a virtual private network connection between the wireless device and the server, via the access point bridging packets between the wireless device and the server, above the network layer, for data access to a network resource.

- 25 The invention further discloses a method for providing a wireless device with roaming data access to a wired network resource via wireless access points, the method comprising the steps of:

- establishing a firewall, at or above the data link layer, in said access points to pass only virtual private network data packets;
- 30 connecting the wireless device to a server on the wired network via a said access point at the data link layer;
- allocating a network layer address to the wireless device; and
- establishing a virtual private network connection between the wireless device and the server above the network layer, via the access point bridging data

packets between the wireless device and the server, for data access to a network resource; and

wherein, upon the wireless device roaming to another access point, the method comprises the further steps of:

5 connecting the wireless device to said server via said other access point at the data link layer, the wireless device retaining the currently allocated network layer address and the virtual private network layer connection; and

continuing data access to a network resource by said virtual private network connection via said other access point.

10

The invention yet further discloses an access point for a wireless communications network supporting roaming, in which wireless devices connect via said access point with a server on a wired network to access a network resource, the access point comprising:

15 a wireless transceiver for communications with a wireless device;
a wired network interface for communications with a server; and
a processor, interfacing between said transceiver and said network interface, and being programmed to connect a wireless device to the wired network at the data link layer by bridging packets between the wireless and wired network, and to
20 implement a firewall which operates to pass only virtual private network data packets existing above the data link layer.

The invention yet further discloses a wireless network in which a wireless client device can connect to a server on a wired network to access network
25 resources by one of a plurality of access points, and roam between said access points while maintaining network connection with the server, the network comprising:

a said wireless client device;
a plurality of said access points, each implementing a firewall which
30 operates to pass only virtual private network data packets existing above the data link layer; and
a said server supporting a virtual private network and network addressing;
and

wherein said wireless client device connects to said server via a said access point at the data link layer, said server allocates a network layer address to the wireless client device and the wireless client device establishes a said virtual private network connection with the server above the network layer, via the access point bridging data packets between the wireless client device and the server, for data access; and

further wherein, upon the wireless device roaming to another access point, the wireless device connects to said server via said other access point at the data link layer, and retains the currently allocated network layer address and the virtual private network layer connection, and continues data access to a network resource by said virtual private network connection via said other access point.

Brief Description of the Drawings

In the accompanying drawings:

Fig. 1 is a schematic block diagram of a wireless access point;

Fig. 2 shows a typical wireless LAN data packet format;

Fig. 3 is a schematic block diagram of a physical wireless network;

Fig. 4 is a logical network diagram;

Fig. 5 is a wireless access layer model embodying the invention;

Fig. 6 is a schematic block diagram, similar to Fig. 3, showing one implementation;

Figs. 7a and 7b are block flow diagrams relating to Fig. 6;

Fig. 8 is a schematic block diagram, also similar to Fig. 3, showing another implementation;

Figs. 9a and 9b are block flow diagrams relating to Fig. 8;

Figs. 10a and 10b are block flow diagrams relating to a pre-allocated IP addressing regime; and

Figs. 11a and 11b are block flow diagrams relating to the processing of packets at a wireless access point.

Detailed Description and Best Mode

Embodiments of a wireless access points, a wireless communications network, firewall router and method for providing data access to a wireless access point will be described.

5 In this description, reference to a "firewall" or "firewall software" is to be understood in the widest context. It includes the meaning of a mechanism to pass only wanted data packets in accordance with established rules. Reference to a "virtual private network" (VPN) similarly takes the broadest meaning, and includes a secure architecture that authenticates an authorised user and enables
10 secure data exchange through the use of encryption. A reference to "bridging software" includes an electrical and low level functional interface between the wireless domain and the wired domain. Where reference is made to "computer program" or "programmed", this is to be understood as including equivalent implementations such as ASICs which perform the same functionality.

15

Wireless Access Point

Fig. 1 shows the block diagram of a typical wireless access point 10 (e.g. providing an IEEE 802.11b AP). A wireless client 12 connects to the wireless
20 access point 10 via a wireless chip/card 14 therewithin. The CPU 16 receives a data packet 30 from the wireless client 12 which typically is of the format shown in Fig. 2, and communicates via a network chip 18 with the network bus 20. The data packet 30 contains a MAC layer header 32, a Network layer header 34, a Transport layer header 36 and a payload 38. The wireless chip/card 14 and the
25 network chip 18 perform the physical layer interfacing functions in a conventional manner. The CPU 16 functionality in providing security and supporting roaming will be described below.

Wireless Communications System

30

Fig. 3 is at a functional level, and concerns the implementation of a transparent firewall bridge 50 (i.e. within the CPU 16 of Fig. 1). It shows the wireless client device 12 connecting to AP1, one of a number of wireless access points 10,10',10'', to gain access to the VPN server 40. The client device 12 has

the capability to roam from AP1 to AP2 and AP3 and still attain connection to the intranet resources 42 via a secured VPN tunnel. Fig. 4 shows the corresponding logic network diagram, where the VPN tunnel is indicated by reference numeral 44.

5

Layer Model

Referring now to Fig. 5, the method of connection will be described. If it is a new session of the client with the VPN server 40, then a set-up takes place.

10 Bridging and firewall software 50, resident in the access point CPU 16, is provided. The firewall software is configured to pass only virtual private network data and, depending upon the form of addressing (i.e. pre-allocated or dynamic), network addressing configuration data. The bridging software transfers packets between the wireless and wired domains, operating at the data link layer. In the
15 set up (or establishment) operation, the client 12 connects to the access point 10 at the data link and physical layers by way of the wireless protocol. The client 12 then obtains (i.e. is issued with) a network layer address by traditional means - in the TCP/IP standards this address can be a predetermined fixed IP address or by some automatic process like DHCP (Dynamic Host Control Protocol). The server
20 40 also establishes a VPN connection with the client 12. The set up is now complete, and the client is able to access intranet resources 42 via the VPN server 40 (as shown in Fig. 4) with the security offered by a tunneled VPN (situated above the network layer). Communications may take place in a secure manner in that only VPN packets are passed by the AP 10.

25

As the client moves from AP1 (10) to AP2 (10'), the physical and data link layer connections are re-established with AP2. However, the network layer connection is not broken, as the client 12 retains its network layer address. Hence, any application using the VPN connection during roaming does not need to re-
30 establish the network layer connection. This means that any file transfer can continue to take place while the client roams from AP1 (10) to AP2 (10'). The VPN connection exists above the (maintained) network layer meaning that the connection remains established notwithstanding the client 12 having roamed to another AP.

First Specific Implementation

Fig. 6 shows a wireless communications system in a form similar to Fig. 3. Like elements are shown with the same reference numerals. The file server 40' is the protected resource. There can, of course, be many other such protected resources on the Ethernet 20. The server 40 thus acts much as a gateway, in that it does not itself hold the resources being sought by the wireless device. Fig. 6 will be described in conjunction with the block flow diagram of Figs. 7a and 7b.

The steps of implementing the secure wireless system are as follows, firstly with reference to Fig. 7a:

Step 60. Assume that the internal wired network 20 is subnetted as 192.168.3.x (i.e. with netmask 255.255.255.0).

Group Step 62. Set up a PPTP server 40 (e.g. using the known techniques described above). This involves the sub-steps as follows:

- configure the Ethernet interface to IP address 192.168.3.1 with network mask 255.255.255.0 (step 64).
- configure the same Ethernet interface to an alias IP address 192.168.2.1 with network mask 255.255.255.0 (step 66) (i.e. the alias address is needed to support the subsequent VPN tunneled addressing).
- configure the PPTP server (group step 68) to:
 - allow user A with password <P> to login to network (step 70).
 - Its end of the PPTP tunnel is set to be 192.168.3.128 (step 72).
 - give out IP addresses of range 192.168.3.129-192.168.3.150 to PPTP clients (step 74).
 - perform proxy ARP for PPTP clients (step 76).

Step 78. Set up the DHCP server 40 to give out IP addresses to wireless clients of the form, say 192.168.2.129 – 192.168.2.199.

Step 80. Install secure 802.11b AP 10. This specific implementation will be described in greater detail below.

Now with reference to Fig. 7b:

5

Step 81. The wireless client 12 connects to the AP 10.

Step 82. The wireless client requests and obtains an IP address from the DHCP server 40. Here it is assumed the client obtains IP address 192.168.2.129.

10

Step 84. The wireless client 12 runs PPTP client software to connect to PPTP server 40, by the substeps of:

- the wireless client 12 is configured to connect to a PPTP server with IP address 192.168.2.1 (step 86).
- 15 - logs in as user A with password <P> (step 88).
- after successful login, a new IP address 192.168.3.129 is obtained for its end of the PPTP tunnel (step 90).

Step 92. Data packets will then be tunneled through the secure PPTP tunnel.

20

Steps 94 and 96. As the wireless client 12 roams from one AP to another, it reassociates itself with the new AP, but retains the IP address 192.168.2.129. Hence, the network layer address will not be broken.

25 *Second Specific Implementation*

Fig. 8 shows a wireless communications system in a form similar to Fig. 3. Like elements are shown with the same reference numerals. Fig. 8 will be described in conjunction with the block flow diagram of Figs. 9a and 9b. The principal difference is that the file server 40' (i.e. the protected resource) exists on
30 a separate subnet to the AP.

The steps to implementing the secure wireless system are as follows:

Step 100. Assume that the internal wired network 20 is subnetted as 192.168.3.x (i.e. with netmask 255.255.255.0).

Step 102. Set up a PPTP server 40 , by the substeps of:

- 5 - configure the protected Ethernet interface (on the protected network 20' where file server 40' is located) to IP address 192.168.3.1 with network mask 255.255.255.0 (step 104).
- configure the other Ethernet interface to IP address 192.168.2.1 with network mask 255.255.255.0 (step 106) (i.e. no alias is required in this implementation).
- 10 - configure PPTP server (step 108) to:
 - allow user A with password <P> to login to network (step 110).
 - Its end of the PPTP tunnel to be 192.168.3.128 (step 112).
 - give out IP addresses of range 192.168.3.129-192.168.3.150 to
 - 15 PPTP clients (step 114).
 - perform proxy ARP for PPTP clients (step 116).

Step 118. Configure DHCP server to give out IP addresses to wireless clients of the form, say 192.168.2.129 – 192.168.2.199.

20

Step 120. Install secure 802.11b AP 10, as described below.

With reference to Fig. 9b:

25

Step 121. The wireless client 12 connects to the AP 10.

Step 122. The wireless client requests and obtains an IP address from the DHCP server 40. Here it is assumed the client obtains IP address 192.168.2.129.

30

Step 124. The wireless client 12 runs PPTP client to connect to PPTP server, by the substeps of:

- wireless client configured to connect to a PPTP server with IP address 192.168.2.1 (step 126).
- log in as user A with password <P> (step 128).
- after successful login, a new IP address 192.168.3.129 is obtained for its end of the PPTP tunnel (step 130).

Step 132. The data packets will then be tunneled through the secure PPTP tunnel.

Steps 134 and 136. As the wireless client roams from one AP to another, it reassociates itself with the new AP, but retains the IP address 192.168.2.129. Hence, the network layer address will not be broken.

Third Specific Implementation

Another implementation is based on using a pre-allocated IP address for each wireless client device where the IP address is already hard-coded in each wireless client device. The network setup is similar to that of Figs. 6 and 8, except that DHCP services need not be run on the server in such an implementation.

There could be other instances where some wireless client devices use pre-allocated IP addresses and other wireless client devices use dynamic IP addressing (i.e. a mixed addressing scheme). In such environments, the implementation will be a dynamic IP addressing-only environment.

With reference to Figs. 10a and 10b, the steps to implementing the secure wireless system are as follows:

Step 200. Assume that the internal wired network 20 is subnetted as 192.168.3.x (i.e. with netmask 255.255.255.0).

Step 202. Assume, for the sake of the example, that the wireless client device is pre-allocated a device address of 192.168.2.129.

Step 204. Set up a PPTP server 40, by the substeps of:

- 5 - configure the protected Ethernet interface (on the protected network 20' where file server 40' is located) to IP address 192.168.3.1 with network mask 255.255.255.0 (step 206).
- configure the other Ethernet interface to IP address 192.168.2.1 with network mask 255.255.255.0 (step 208) (i.e. this could be an alias IP address depending on whether protected resources are on the same network segment as the wired network of the AP).
- 10 - configure PPTP server (step 210) to:
 - allow user A with password <P> to login to network (step 212).
 - Its end of the PPTP tunnel to be 192.168.3.128 (step 214).
 - give out IP addresses of range 192.168.3.129-192.168.3.150 to PPTP clients (step 216).
- 15 - perform proxy ARP for PPTP clients (step 218).

Step 220. Install secure 802.11b AP 10, as described below.

Step 222. The wireless client 12 connects to the AP 10.

20

Step 224. The wireless client 12 runs PPTP client to connect to PPTP server, by the substeps of:

- 25 - wireless client configured to connect to a PPTP server with IP address 192.168.2.1 (step 226).
- log in as user A with password <P> (step 228).
- after successful login, a new IP address 192.168.3.129 is obtained for its end of the PPTP tunnel (step 230).

Step 232. The data packets will then be tunneled through the secure PPTP tunnel.

30

Steps 234 and 236. As the wireless client roams from one AP to another, it reassociates itself with the new AP, but retains the IP address 192.168.2.129. Hence, the network layer address will not be broken.

Common Processing of Packets at Access Points

This is the common processing of installing a secure 802.11b AP, that
5 occurs for the implementations described above, in respective steps 80, 120 and 220.

For packets received from the *wireless* interface. Packets received on
wireless interface consists of 802.11b header + IP packet. With reference to Fig.
10 11a:

Step 140. Check, from the MAC layer header packet, that the packet is to be
received by this AP for devices connected to the AP in either the wired or wireless
network – if not, throw it away (step 142).

15

Step 144. Save the source and destination MAC address in 802.11b header.

Step 146. Strip away 802.11b header.

20 Step 148. Put IP packet through firewall in accordance with the following rules:

- [N.B. this step is not required if pre-allocated IP addresses are used for
the wireless client devices] Is it DHCP packet (step 150)? If yes – go to
step 156, if no – go to step 152.
- Is it PPTP packet (step 152)? If yes – got to step 156 (these are encrypted
25 packets).
- Else, throw it away (intruder packets will get thrown away here) (step
154).

Step 156. Add in appropriate header to IP packet in accordance with the
30 following rules:

- Is the destination address in the Ethernet network (step 158)? - If yes,
add Ethernet header filled with the source and destination MAC address
retrieved in step 144 (step 160). The destination can be any resource

supported on the Ethernet network, of which the file server 40' is but one instance.

- Is the destination address in the wireless network (step 162)? - If yes, add 802.11b header filled with the source and destination MAC address retrieved in step 144 (step 164).
- Else, throw it away (step 166).

Step 168. Transmit packets on the appropriate interface.

- 10 For packets received from the *Ethernet* interface. Packets received on Ethernet interface consists of Ethernet header + IP packet. With reference to Fig. 11b:

- Step 170. Check, from the MAC layer header, that the packet is to be received by wireless clients associated with this AP – if not, throw it away (step 172).

Step 174. Save the source and destination MAC address in Ethernet header.

Step 176. Strip away Ethernet header.

- 20 Step 178. Put IP packet through firewall rules:

- [N.B. this step is not required if pre-allocated IP addresses are used for the wireless client devices] Is it a DHCP packet (step 180)? If yes – go to step 186, if no – go to step 182.
- 25 - Is it a PPTP packet (step 182)? If yes – got to step 186 (these are encrypted packets).
- Else, throw it away (i.e. intruder packets will get thrown away here) (step 184).

- 30 Step 186. Add in 802.11b header to IP packet, the header will be filled with the source and destination MAC address retrieved in step 144.

Step 188. Transmit packet on wireless interface.

These implementations demonstrate that the intruder can only have access to:

- 5 1. DHCP packets – this is of little use as it only shows the IP addresses that the DHCP server gives out to the client. [That is, they are only visible if pre-allocated IP addresses are not used]
2. PPTP packets – these are encrypted – again, there is little useful that can be derived from the packets.

10 The embodiments described, of a transparent bridging firewall plus VPN connection, will block unauthorized users from accessing the network through the wireless access point. Put another way, an AP is implemented to block all network layer packets except network layer address configuration and discovery (e.g. DHCP) packets and VPN packets. At the same time, users are free to roam
15 transparently from access point to access point and the application will not have to reset during the roaming; for example, file transfers can continue seamlessly while the wireless client is moving from one AP to another AP.

Claims:

1. A method for establishing data access for a wireless device to a wired network resource via a wireless access point, comprising the steps of:
 - 5 establishing a firewall, at or above the data link layer, in said access point to pass only virtual private network data;
 - connecting the wireless device to a server on said wired network via said access point at the data link layer;
 - allocating a network layer address to the wireless device; and
 - 10 establishing a virtual private network connection between the wireless device and the server, via the access point, bridging packets between the wireless device and the server, above the network layer, for data access to a network resource.
- 15 2. The method of claim 1, wherein the step of establishing a firewall further includes passing network addressing configuration data packets, and the step of allocating a network layer address is performed dynamically.
3. The method of claim 2, wherein said virtual private network addressing
20 includes an alias address if said requested resource resides on a common part of the wired network, or one or more separate addresses if said requested resource resides on one or more protected subnets.
4. The method of claim 1, wherein the step of allocating a network layer
25 address is performed by way of a pre-allocated address hard-coded in the wireless device.
5. The method of any one of claims 1 to 4, wherein operation of said firewall performs the steps of: stripping data packet headers, and determining whether the
30 stripped packet is of a data packet type to be passed.
6. The method of claim 5, wherein in the VPN connection, the bridging then adds an appropriate interface header based on the original header destination MAC layer address.

7. A method for providing a wireless device with roaming data access to a wired network resource via wireless access points, the method comprising the steps of:
- 5 establishing a firewall, at or above the data link layer, in said access points to pass only virtual private network data packets;
- connecting the wireless device to a server on the wired network via a said access point at the data link layer;
- 10 allocating a network layer address to the wireless device; and
- establishing a virtual private network connection between the wireless device and the server, above the network layer, via the access point bridging data packets between the wireless device and the server, for data access to a network resource; and
- 15 wherein, upon the wireless device roaming to another access point, the method comprises the further steps of:
- connecting the wireless device to said server via said other access point at the data link layer, the wireless device retaining the currently allocated network layer address and the virtual private network layer connection; and
- 20 continuing data access to a network resource by said virtual private network connection via said other access point.
8. The method of claim 7, wherein the step of establishing a firewall further includes passing network addressing configuration data packets, and the step of
- 25 allocating a network layer address is performed dynamically.
9. The method of claim 8, wherein said virtual private network addressing includes an alias address if said requested resource resides on a common part of the wired network, or one or more separate addresses if said requested resource
- 30 resides on one or more protected subnets.
10. The method of claim 7, wherein the step of allocating a network layer address is performed by way of a pre-allocated address hard-coded in the wireless device.

11. The method of any one of claims 7 to 10, wherein operation of said firewall performs the steps of: stripping data packet headers, and determining whether the stripped packet is of a data packet type to be passed.
- 5 12. The method of claim 11, wherein in the VPN connection, the bridging then adds an appropriate interface header based on the original header destination MAC layer address.
- 10 13. An access point for a wireless communications network supporting roaming, in which wireless devices connect via said access point with a server on a wired network to access a network resource, the access point comprising:
a wireless transceiver for communications with a wireless device;
a wired network interface for communications with a server; and
15 a processor, interfacing between said transceiver and said network interface, and being programmed to connect a wireless device to the wired network at the data link layer by bridging packets between the wireless and wired network, and to implement a firewall which operates to pass only virtual private network data packets existing above the data link layer.
- 20 14. The access point of claim 13, wherein the firewall further passes network addressing configuration data packets if the network layer address is to be assigned dynamically to wireless clients.
- 25 15. The access point of claim 14, wherein said virtual private network addressing includes an alias address if said requested resource resides on a common part of the wired network, or one or more separate addresses if said requested resource resides on one or more protected subnets.
- 30 16. The access point of claim 13, wherein the processor allocates a network layer address as a pre-allocated address.

17. The access point of any one of claims 13 to 16, wherein said firewall strips data packet headers, and determines whether the stripped packet is of a data packet type to be passed.

5 18. The access point of claim 17, wherein in the VPN connection, the bridging then adds an appropriate interface header based on the original header destination MAC layer address.

19. A wireless network in which a wireless device can connect to a server on a
10 wired network to access network resources by one of a plurality of access points, and roam between said access points while maintaining network connection with the server, the network comprising:

a said client device;

a plurality of said access points, each implementing a firewall which
15 operates to pass only virtual private network data packets and network addressing configuration data packets existing above the data link layer; and

a said server supporting a virtual private network and network addressing;
and

wherein said wireless device connects to said server via a said access point
20 at the data link layer, said server allocates a network layer address to the wireless device and establishes a said virtual private network connection between the wireless device and the server above the network layer, via the access point bridging data packets between the wireless device and the server, for data access;
and

25 further wherein, upon the wireless device roaming to another access point, the wireless device connects to said server via said other access point at the data link layer, and retains the currently allocated network layer address and the virtual private network layer connection, and continues data access to a network resource by said virtual private network connection via said other access point.

30

20. The wireless network of claim 19, wherein the firewall further passes network addressing configuration data packets, and allocates a network layer address dynamically.

21. The wireless network of claim 20, wherein said virtual private network addressing includes an alias address if said requested resource resides on a common part of the wired network, or one or more separate addresses if said requested resource resides on one or more protected subnets.

5

22. The wireless network of claim 19, wherein said client device is hard-coded with a pre-allocated network layer address.

23. The wireless network of any one of claims 19 to 22, wherein said firewall
10 strips data packet headers, and determines whether the stripped packet is of a data packet type to be passed.

24. The wireless network of claim 23, wherein in the VPN connection, the
bridging then adds an appropriate interface header based on the original header
15 destination MAC layer address.