

COMMUNICATION NETWORK ARCHITECTURE

This invention relates to a communication network architecture, and in particular to a network architecture that allows the formation of a frame-based network over a connection oriented network in an efficient manner.

In communication networks, and in particular in attempts to evolve towards broadband networks, a very important aspect from a commercial point of view is the coexistence on the same network of both voice and data. This co-existence requirement was the prime motivation behind asynchronous transfer mode (ATM) being the choice broadband Integrated Services Digital Network (B-ISDN). In the past data services have been carried over leased communications circuits, or packet switched radio networks such as X.25. Such data links are circuit-switched in nature and thus are very costly. Voice services are also inherently circuit-switched, however owing to the shared-use nature of Public Switched Telephone Networks (PSTN) the cost to each user is low. Data links hence differ from voice services in the way the circuits are used, and hence result in a different economic model.

In recent years of course the Internet has become more popular. In Internet use data is carried in packets and such packets are routed on a best effort basis traversing a large number of routers along the way to the destination. The Internet thus has no guarantee of delivery of packets. At the lowest network level, the Internet is therefore effectively connectionless.

A wide variety of different forms of communication networks are known or have at least been proposed if not implemented. Simple well-known examples of such prior networks include wireless or cellular communication networks which are generally single connection or virtual circuit forms of networks and are predominantly for voice and for limited data capabilities. Also known is local area network (LAN) emulation over, for example, an asynchronous transfer mode (ATM) network. Such LAN emulation over ATM is however only suitable for a localized private network, limited to one sub-network group. Ad-hoc networks are also known which are packet based networks with little or no dynamic configuration.

9902419-2

27 MAY 1999

In any form of communication network there are a number of desirable objectives. Notably these include reliability and speed of connections and in general terms this means finding ways to limit the amount of traffic on the network, or more precisely to limit the amount of traffic passing through certain key switches and routers
5 that can form a bottleneck.

According to the present invention there is provided a communication network comprising:

- a plurality of user terminals,
- a plurality of local area switches, and
- 10 at least one private network switch,

wherein said private network switch comprises means for allowing groups of user terminals to register as private networks within said communication network.

Preferably the private network switch comprises group registration means for registering a group of user terminals as a private network, and furthermore the private
15 network switch may comprise terminal registration means. In this way an individual user terminal may apply to said terminal registration means to register with an existing private network. Preferably the private network switch comprises authentication means for confirming that a said user terminal is entitled to join a said private network.

In addition to applying to join an existing network an individual user terminal that
20 is a participant in a private network may also apply to the terminal registration means to leave an existing network.

In a preferred embodiment of the invention when a first user terminal that is a member of a private network wishes to communicate a message with a second user terminal that is a member of the private network the communication is via the private
25 network switch. In this embodiment the first user terminal transmits the message with destination address information to the private network switch, and the private network switch sends the message to all members of said private network of which the second user terminal is a member.

An important aspect of the present invention at least in its preferred embodiments
30 is one of traffic management. Preferably therefore if traffic flow between the first and second user terminals via the private network switch exceeds a predetermined level a

direct connection may be established between said first and second users. In this embodiment while the direct connection is being established communication continues via said private network switch.

5 Preferably the direct connection may be established at the request of the second user terminal to the private network switch. The second user terminal may monitor a number of data traffic statistics (for example current instantaneous data flow, average data flow, and duration of data flow over a predetermined threshold) and calculate a determination function from these statistics using weighting functions. If the calculated determination exceeds a predetermined level the direct connection is established.

10 Alternatively the direct connection may be established at the request of the private network switch to the second user terminal. The data traffic statistics monitored by the second user terminal may be supplied to the private network switch which may calculate its own determination function taking into account additionally the total data traffic through the private network switch and the duration for which the second user terminal
15 has not requested a direct connection notwithstanding that a preset level has been exceeded. Preferably means are provided for downgrading the services offered by said private network switch to said second user terminal in the event that said second user terminal refuses said request.

20 An embodiment of the invention will now be described by way of example and with reference to the accompanying drawings, in which:-

Fig.1 is a schematic view of a communication network according to an embodiment of the invention,

Fig.2 is a schematic view of the internal structure of a private network switch,

25 Fig.3 is a schematic view of the internal structure of a signal unit in a private network switch, and

Figs.4 to 7 illustrate the use of a private network for communications between members of a private network.

Referring firstly to Fig.1 there is shown a highly schematic view of a communication network according to an embodiment of the present invention. The
30 network includes a plurality of user terminals 1, a plurality of local area network switches 2, a plurality of wide area network switches 3, a private network switch 4, IP router 5 and

Internet gateway switch 6. Apart from the private network switch 4, the components of the network are conventional and will be briefly described as follows.

Local area network switches 2 form the backbone of the network and connect to user terminals 1 and to other switches forming the network. In an ATM implementation of the present invention local area network switches 2 may comprise a conventional ATM switch. Wide area network switches 3 are adapted to connect a user terminal 1 within the network to another network, for example a network operated by a public network operator. An example of such a wide area switch 3 in an ATM implementation of the invention is a conventional ATM edge-switch. Thus the wide area switches 3 control the connections between user terminals 1 that are members of the network and with other external networks. Generally each wide area network will receive an aggregation of traffic from a number of local area network switches 2.

IP router 5 and Internet gateway switch 6 serve to allow user terminals 1 within the network to communicate with the Internet. Router 5 and gateway switch 6 may take any conventional form.

It will be understood that the connections between the elements forming the network as described above may be in any conventional form provided that they allow end-to-end connections (known as a virtual circuit) to be established between any two user terminals 1 forming part of the network. The precise method of establishing such a virtual circuit will depend on the nature of the network and of the switches 2, 3 and 4 used to implement the network and does not form part of the present invention. However, as an example, if the network is an ATM network the switches 2, 3 and 4 will implement the User-Network-Interface and any other necessary methods (known as "signaling") and protocols as defined by the ATM Forum. Such protocols may, as is well known, be implemented either by hardware or by software or by a combination of the two.

The network comprises at least one private network switch 4 that allows user terminals 1 to form virtual private sub-networks within the overall network as will be described in more detail below. The general structure of the private network switch 4 is shown in Fig.2 and comprises a signal unit 10, switching unit 11 and a port interface unit 12. Signal unit 10 serves to perform the necessary signaling operations to establish a virtual circuit and will be described in more detail below. Switching unit 11 comprises

the necessary hardware and/or software for switching traffic around the network, while port interface unit 12 provides the necessary physical connection to the network.

Fig.3 shows more details of the signal unit 10. Signal unit 10 comprises terminal attachment unit 20, connection unit 21, terminal registration unit 22, group registration unit 23, frame routing unit 24 and switch unit interface 25.

Terminal attachment unit 20 is designed to connect to any user terminal 1 forming part of the network. The particular form of the terminal attachment unit 20 will depend on the nature of the connection-oriented network of which the user terminals 1 are a part, and may be implemented either by software and/or hardware. By way of example, if the network is an ATM network there are both hardware and software methods defined in ILMI 4.0 designed to enable the necessary connections to be made.

Terminal attachment unit 20 interacts with connection unit 21 which sets up a requested virtual circuit, as will be explained in more detail below, by commanding the switching unit 11 via the switch unit interface 25. As with the terminal attachment unit 20 the precise form of the connection unit 21 will depend on the nature of the connection-oriented network.

As described above there is a connection-oriented network comprising a number of user terminals 1 which form part of a larger network interconnected by local area network switches 2, wide area network switches 3 and private network switches 4. Private network switches 4 are, however, provided with further means for establishing frame-based virtual private networks on top of the larger connection-oriented network. To achieve this, a user terminal 1 wishing to form part of a virtual private network will register a request with the terminal registration unit 22 forming part of the signal unit 10 of the private network switch 4. Each user terminal 1 will have a unique address that is included in the address field of the information carrying frames sent by the user terminal 1 and which allows the private network switch to identify different user terminals 1. Terminal registration unit 22 is provided with its own address so that a user terminal 1 can communicate directly with the unit 22. The request from the user terminal 1 will include the identity of the virtual private network in which the user terminal 1 wishes to participate. Group registration unit 23 handles all requests to participate in a virtual private network, to create a virtual private network or for a user terminal 1 to leave a

virtual private network. It will be understood that group registration unit 23 is able to handle a number of different virtual private networks simultaneously. The ability of a user terminal 1 to participate in a given virtual private network may, however, be subject to the condition that the user terminal 1 is authorised to do so and this may be handled by authentication unit 26.

It will also be understood that existing groups can be reconfigured. For example two such groups can be combined to form a single larger group, following which the original two groups would be disbanded.

When a virtual private network has been established, traffic between user terminals 1 forming members of the virtual private network is frame-based and is handled by frame routing unit 27 within the signal unit of the private network switch. A frame will include a header for identification purposes, destination address information, source address information, error checking information and the information that itself is being transmitted. This data will all be presented in a predefined structure. An example of such a frame is that defined in the IEEE802.3 standard. Frame routing unit 27 decides from the destination address information contained in the frame to which virtual private network a received frame should be directed. This may be done with by means of software and/or hardware elements.

Figs.4 to 7 illustrate how members of a virtual private network may communicate with each other. In Figs.4 to 7 a virtual private network is formed of four user terminals 1a,1b,1c and 1d. It will of course be understood that the choice of four terminals in this example is purely for the sake of illustration and there may be any number. It will also be understood that the four terminals 1a-d are a subset of a larger number of user terminals 1 forming a larger connection-oriented network of which terminals 1a-d are still a part and with which terminals 1a-d may continue to communicate in a conventional manner.

As can be seen from Fig.4 virtual circuits are established between each user terminal 1a-d and the private network switch 4, in turn a virtual multicast circuit is established from the private network switch 4 to each user terminal 1a-d forming a given virtual private network. It will be appreciated that each virtual circuit may be comprised of a number of sections interconnected by local area switches 2 as is shown schematically in Fig.4. The virtual circuits and the virtual multicast circuits are established when the

virtual private network is first created and when new participants in the virtual private network are registered.

Fig.5 shows how the frame-based private network may be used when user terminal 1a wishes to communicate with user terminal 1d, both user terminals 1a and 1d being part of the same virtual private network. Data to be sent from user terminal 1a to user terminal 1d is sent from user terminal 1a in the form of data frames including the destination address to the private network switch 4. Upon receipt of the data frames, the private network switch 4 will send the data frames to the appropriate multicast virtual circuit containing the destination address. The data frames will therefore reach all the user terminals 1a-d forming the virtual private network where appropriate software and/or hardware in each user terminal 1a-d will decide whether or not to accept the data frames depending on the destination address. If the destination address is that of terminal 1d, then terminal 1d will of course accept the data frames.

Because the virtual circuits between each user terminal 1a-d and the private network switch 4, and the multicast virtual circuit between the private network switch 4 and the user terminals 1a-d are established on registration of the virtual private network, there is no time requirement to set-up the connection between user terminals 1a and 1d when user terminal 1a wishes to send data traffic to user terminal 1d (and of course this applies to any transmissions between members of the virtual private network).

In this embodiment of the present invention user terminals 1a-d share a responsibility to maintain fair use of traffic capacity. This is done by distributing the monitoring of the traffic flow rate at the receiving end of the data traffic. For example, each user terminal 1a-d has the responsibility to measure and monitor the traffic flow rate and report this rate back to the private network switch 4 on a periodic basis, and also the responsibility and ability to enforce autonomous action to divert traffic away from the private network switch 4 when it exceeds a predetermined limit. This distribution of traffic monitoring and resolution allows the private network switch 4 to be easily scaled. In addition in the present embodiment of the invention the private network switch 4 has the ability to command user terminals to divert traffic away from the private network switch 4 itself. For example, the private network switch 4 may determine that it is overwhelmed with traffic and may command any user terminal 1a-d with known heavy

traffic flow, based on reported traffic flow, to divert traffic away from the private network switch 4. Should a user terminal refuse such a command, means may be provided whereby the private network switch 4 may refuse to handle any further frames originating from that particular user terminal.

5 The decision on when to request a direct connection may be based on a number of factors, such as : (1) the average arrival rate $r1$ of frames coming from the same source, (2) the duration $d2$ of sustained arrival rate above a predetermined threshold, and (3) a peak arrival rate $r2$. These may considered individually or in combination. For example, if used in combination a determination function D may be defined as

$$10 \quad D = w1 \times r1 + w2 \times d2 + w3 \times r2$$

Where $w1$, $w2$ and $w3$ are weighting factors that can be appropriately selected or negotiated during the registration process and/or establishment of a virtual private network. The determination function D (at which point a direct connection is to be established) can also be negotiated during registration.

15 The measured traffic flow statistics $r1$, $d2$ and $r2$ are also reported to the virtual private network switch 4 which may carry out its own determination function Q which may be as follows:

$$20 \quad Q = w4 \times r1 + w5 \times d2 + w6 \times r2 + w7 \times a + w8 \times X$$

Where $w4-8$ are further weighting factors and a is the aggregate load at the switch 4 and x is the time elapsed since D was greater than the level at which that terminal 1d should have requested a direct connection. Weighting factors $w1-3$ are assigned by the switch 4 which therefore can calculate D for itself and will know when it has exceeded the predetermined limit and will order the direct connection to be established if its own determination function Q exceeds a predetermined level taking into account the aggregate loading of switch 4 and the time elapsed since the direct connection should have been established.

30

More generally, it is possible to define any determination function as the summation of a number of measurable traffic flow statistics with appropriate weighting factors that may be either predetermined or negotiated during registration. Threshold levels may be set such that when a level is passed a direct connection is initiated.

5 In Fig.6 there is shown the situation in which user terminal 1d sends a request (the dotted line in the Figure) to the private network switch 4 for a direct connection to user terminal 1a. This request is made by user terminal 1d while still receiving data from terminal 1a via the multicast virtual circuit from the private network switch 4. It is important to note here that the decision to make a direct connection between terminals 1a and 1d is made by terminal 1d itself based upon its own measurements of the traffic flow.
10 It is also important to note that the direct circuit between terminals 1a and 1d is made upon the request of terminal 1d while that terminal continues to receive data from user terminal 1a via the multicast virtual circuit. Thus while the direct circuit is being established, data continues to be transmitted from user terminal 1a to user terminal 1d via
15 the private network switch 4 and the multicast virtual circuit. This means that there is no disruption of the data flow while the direct circuit is being established and that the time for establishing the direct circuit is effectively hidden. Fig.7 shows the situation when a direct circuit has then been established between user terminals 1a and 1d.

One advantage of the architecture of the present invention is that it may be
20 implemented with a wide range of existing communication protocols. For example, the network may be an IP network in which case an address resolution protocol (ARP) is sued to enable the private network switch 4 to map an IP address to the individual MAC address of a given user terminal 1 upon registration of that user terminal 1 as part of a virtual private network. When a user terminal 1 forming part of the virtual private
25 network transmits an IP packet destined for another member of the virtual private network, the private network switch 4 will match the MAC address contained in the data frame and will forward the packet to the appropriate multicast virtual circuit associated with the virtual private network. The destination user terminals 1 on the multicast circuit will pick up and process the IP packet. Upon matching the MAC address, the rest of the
30 user terminals 1 will discard the packet except for the user terminal 1 for which the packet was intended.

If the source user terminal 1 continues to send IP packets to the same destination user terminal 1, the destination user terminal 1 may determine that the flow of data frames is sufficient to justify a dedicated virtual circuit and will therefore initiate a request with the private network switch for a such a dedicated virtual circuit to be
5 established. Once this direct path virtual circuit is established, a route entry will be inserted at the host and will result in all future IP packets for this destination to be directed via the dedicated virtual circuit.

The private network switch 4 may allocate IP addresses as a sub-net. This can be taken from the IP private address in which case the private network switch 4 acts as a
10 masquerading host. However, this would mean that the user terminals 1 participating in a virtual private network would not be "seen" by the larger network. It is therefore preferred to form the private network switch 4 as a point-to-point-transport (PPTP) protocol server as this will allow Internet users to participate as part of the virtual private network.

15 Thus it will be seen that there is provided an architecture that is adapted to support one or more private frame-based networks over a larger connection-oriented network. The architecture may employ any conventional connection-oriented networking techniques, such as ATM and IP systems, and allows users to establish a private network on an ad-hoc basis, with participants joining or leaving as required regardless of any
20 particular physical attachment point. The private network that is thus established is isolated from other users' traffic with provisions for a secure link and a capacity guarantee. One advantage of the present invention, for example, is that members of an established virtual private network are isolated from other users of the larger network and messages between members of the virtual private network are not seen by other user
25 terminals. In addition, however, members of one virtual private network may choose to use a common encryption technique for a further security. To ensure that all members of the larger network can communicate with each other effectively, a common private network including all users may be established.

The architecture is efficient in the sense that a minimum number of messages are
30 exchanged between the network entity and the user terminals, and in that the burden for

providing flow statistics and for deciding whether or not to establish a direct connection is distributed.

5

10

15

20

25

30

CLAIMS

1. A communication network comprising:
a plurality of user terminals,
5 a plurality of local area switches, and
at least one private network switch,
wherein said private network switch comprises means for allowing groups of user terminals to register as private networks within said communication network.
- 10 2. A network as claimed in claim 1 wherein said private network switch comprises group registration means for registering a group of user terminals as a private network.
3. A network as claimed in claim 1 or 2 wherein said private network switch comprises terminal registration means.
- 15 4. A network as claimed in claim 3 wherein an individual user terminal may apply to said terminal registration means to register with an existing private network.
5. A network as claimed in claim 4 wherein said private network switch comprises
20 authentication means for confirming that a said user terminal is entitled to join a said private network.
6. A network as claimed in claim 3 wherein an individual user terminal that is a participant in a said private network may apply to said terminal registration means to
25 leave an existing network.
7. A network as claimed in any preceding claim wherein when a first user terminal that is a member of a said private network wishes to communicate a message with second user terminal that is a member of said private network the communication is via said
30 private network switch.



8. A network as claimed in claim 7 wherein said first user terminal transmits said message with destination address information to said private network switch, and said private network switch sends said message to all members of said private network of which said second user terminal is a member.

5

9. A network as claimed in claim 7 or 8 wherein if traffic flow between said first and second user terminals via said private network switch exceeds a predetermined level a direct connection may be established between said first and second users.

10 10. A network as claimed in claim 9 wherein said while said direct connection is being established communication continues via said private network switch.

11. A network as claimed in claim 9 or 10 wherein said direct connection may be established at the request of said second user terminal to said private network switch.

15

12. A network as claimed in claim 9 or 10 wherein said direct connection may be established at the request of said private network switch to said second user terminal.

13. A network as claimed in claim 12 wherein means are provided for downgrading the services offered by said private network switch to said second user terminal in the event that said second user terminal refuses said request.

20

14. A network as claimed in any preceding claim wherein said network is a connection-oriented network and said private network is a frame-based network.

25

30

