IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent of:	Munger *et al.*	
U.S. Patent No.:	6,502,135	Attorney Docket No.: 38868-0004IP1
Issue Date:	Dec. 31, 2002	
Appl. Serial No.:	09/504,783	
Filing Date:	Feb. 15, 2000	
Title:	AGILE NETWORK PROTOCOL FOR SECURE COMMUNICATIONS WITH ASSURED SYSTEM AVAILABILITY	

DECLARATION OF DR. ROCH GUERIN

1. My name is Dr. Roch Guerin. I am the chair of the Computer Science & Engineering department at Washington University in St. Louis. I have been asked to offer technical opinions relating to U.S. Patent No. 6,502,135, and prior art references relating to its subject matter. My current *curriculum vitae* is attached and some highlights follow.

2. I earned my diplôme d'ingénieur (1983) from École nationale supérieure des télécommunications, in Paris, France. Thereafter, I earned my M.S. (1984) and PhD (1986) in electrical engineering from The California Institute of Technology in Pasadena, California.

3. Prior to becoming a professor in engineering, I held various positions at the IBM T.J. Watson Research Center. Specifically, from 1986 to 1990, I was a research staff member within the Communication Department, where I worked to design and evaluate high-speed switches and networks. From 1990 to 1991, I was a research staff member within the IBM High Performance Computing and Communications Department, where I worked to develop and deploy an integrated broadband network. From 1992 to 1997, I was the manager of Broadband Networking within IBM's Security and Networking Systems Department, where I led a group of researchers in the area of design, architecture, and analysis of broadband networks. One of the projects on which I worked, for example, led to U.S. Patent No. 5,673,318, which regards "[a]

method and system for providing data authentication, within a data communication environment, in a manner which is simple, fast, and provably secure," and of which I am a named inventor. *See* U.S. Patent No. 5,673,318, abstract. From 1997 to 1998, I was the manager of Network Control and Services within IBM's Security and Networking Systems Department, where I led a department responsible for networking and distributed applications, including topics such as advance reservations, policy support, including for Resource Reservation Protocol (RSVP), quality of service (QoS) routing , and security, and integrated switch and scheduling designs.

4. I have been a professor of engineering for the past fifteen years. As such, but prior to becoming the chair of the Computer Science & Engineering department at Washington University in St. Louis, I was the Alfred Fitler Moore Professor of Telecommunications Networks (an honorary chair) in the Department of Electrical and Systems Engineering at the University of Pennsylvania. As a professor of engineering, I have taught many courses in networking, including Advanced Networking Protocols (TCOM 502), which addressed, among other things, virtual private networks.

5. I have authored over fifty journal publications, including "On the Feasibility and Efficacy of Protection Routing in IP Networks," which was honored with the IEEE INFOCOM 2010 Best Paper Award. I have been named a Fellow by both the IEEE and ACM, and, from 2009 to 2012, I was the Editor-in-Chief of the IEEE/ACM Transactions on Networking. Furthermore, I am a named inventor on over thirty issued U.S. patents.

6. I am familiar with the content of U.S. Patent No. 6,502,135 (the "'135 patent"). In addition, I have considered the various documents referenced in my declaration as well as additional background materials. I have also reviewed certain sections of the prosecution history of the '135 patent, the prosecution histories of reexamination control numbers 95/001,269,

95/001,679, and 95/001,682; and the claim construction orders from *VirnetX Inc. v. Microsoft Corp.*, Docket No. 6:07CV80 (E.D. Tex.) and *VirnetX Inc. v. Cisco Systems, Inc. et al.*, Docket No. 6:10cv417 (E.D. Tex.).

7. Counsel has informed me that I should consider these materials through the lens of one of ordinary skill in the art related to the '135 patent at the time of the invention, and I have done so during my review of these materials. I believe one of ordinary skill as of February 15, 2000 (the priority date of the '135 patent) would have a Master's degree in computer science or computer engineering, or in a related field such as electrical engineering, as well as about two years of experience in computer networking and in some aspect of security with respect to computer networks. I base this on my own personal experience, including my knowledge of colleagues and others at the time.

8. I have no financial interest in either party or in the outcome of this proceeding. I am being compensated for my work as an expert on an hourly basis. My compensation is not dependent on the outcome of these proceedings or the content of my opinions.

9. My opinions, as explained below, are based on my education, experience, and background in the fields discussed above.

10. This declaration is organized as follows:

I. Brief Overview of the '135 Patent

11. The '135 patent is generally directed to a "agile network protocol for secure communications with assured system availability." Ex. 1001, Title. The '135 patent includes 18 claims, of which claims 1, 10, 13, and 18 are independent.

12. A section of the '135 patent's specification titled "B. Use of a DNS Proxy to Transparently Create Virtual Private Networks" describes "the automatic creation of a virtual private network (VPN) in response to a domain name server look-up function," with reference to FIGS. 25-27. Ex. 1001 at 37:17-21. In the example embodiment, the '135 patent describes that a "specialized DNS server traps DNS requests and, if the request is from a special type of user (e.g., one for which secure communication services are defined), the server does not return the true IP address of the target node, but instead automatically sets up a virtual private network between the target node and the user." Ex. 1001 at 37:63 to 38:2.

13. In the case of standard "DNS requests that are determined to not require secure services (e.g., an unregistered user), the DNS server transparently 'passes through' the request to provide a normal look-up function." Ex. 1001, at 38:6-9. On the other hand, if access to a secure site has been requested, the system described in the '135 patent "determines whether the user has sufficient security privileges to access the site," and, if so, transmits a message requesting that a virtual private network be created between the client and the secure target site. *See* Ex. 1001 at 38:25-33. The '135 patent describes that the various functions of the DNS proxy, DNS server, and gatekeeper can be performed on the same or different machines. *See* Ex. 1001 at 38:53-55; 61-65.

II. Terminology

14. I have been informed that claim terminology must be given the broadest reasonable interpretation during an IPR proceeding. I have been informed that this means the

claims should be interpreted as broadly as their terms reasonably allow, but that such interpretation should not be inconsistent with the patent's specification. I have been informed that this may yield interpretations that are broader than the interpretation applied during a District Court proceeding, such as the pending *VirnetX Inc. v. Microsoft Corp*. litigation

15. I have been informed that it would be useful to provide some guidance in this proceeding with respect to certain terms, and I have been asked to consider the term below and its corresponding construction. In each instance of doing so, I considered the term's context within the claim, use within the specification, and my understanding of how one of ordinary skill in the art would understand the term around the time of the purported invention under the broadest reasonable construction standard.

16. I have considered whether a broadest reasonable interpretation of "virtual private network" would be broad enough to cover "a private network that is configured within a public network." I believe that it would, since, as described below, such an interpretation is not inconsistent with the '135 patent's specification and the understanding one of ordinary skill in the art would ascribe to this term when looking for the broadest reasonable construction.

17. There is not an explicit definition of "virtual private network" in the '135 patent. However, the '135 patent describes that virtual private networks may be established over the Internet, and secured, for example, using public key encryption. *See* Ex. 1001 at 37:37-58. However, the '135 patent also contemplates other methods of establishing security. For example, the '135 patent describes the use of a quasi-random IP hopping scheme to implement a VPN. *See, e.g.*, Ex. 1001 at 23:10-14 ("In a second mode referred to as 'promiscuous per VPN' mode, a small set of fixed hardware addresses are used, with a fixed source/destination hardware address used for all nodes communicating over a virtual private network."). Moreover, claim 6

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.