The Commission's assessment of Microsoft's innovation claims

In the column "Prior Art", the symbol [PA] indicates that the reference is cited as prior art, the symbol [R] means that it is cited as a reference.

The following applies in the column "References":

[July-T, x]	= 8 July Trustee report, page x
[March-T, x]	= 3 March Trustee report (as amending the 22 February Trustee report), page x
[Ecis, x]	= Ecis's comments to Microsoft's Response to the 1 March SO, page x

Protocol		**Technology**	**Description of the technology**	**Date of claim**	**Claimed benefit**	**Reference in Microsoft's filing**	**Assessment**	**Prior Art**	**References**
Active Directory Federation Services	ADFS	Combination of ADFS Technologies	The combination of all the mentioned ADFS technologies.	April 2004	The use of the five individual ADFS innovations in combination is undisclosed and not obvious.	Microsoft's innovation report on "Microsoft Web Browse Federated Sign-on Protocol & Microsoft Web Browser Federated Sign-On Protocol Extensions"	The claimed innovation is the combination of different features belonging to the same protocol. Combining these individual features is an obvious step for a person skilled in the art. NON-INNOVATIVE		[July-T, 4]
Active Directory Federation Services	ADFS	Defining Authentication Communications	ADFS defines communications between a resource identity provider and a web service resource.	April 2004	The protocol delivers maintainability by defining authentication.	Microsoft's innovation report on "Microsoft Web Browse Federated Sign-on Protocol & Microsoft Web Browser Federated Sign-On Protocol Extensions", pages 20 to 21.	The claim concerns resolving problems which are specific to Microsoft's implementation. The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] Anderson, Steve et al: Web Services Trust Language (WS-Trust) (1 May 2004; http://www.ibm.com/developerworks/library/specification/ws-trust/; Microsoft has participated in the development of WS-Trust.) [PA] Bajaj, Siddharth et al: Web Services Federation Language (WS-Federation), Version 1.0 (8 July 2003; http://www.msdn.microsoft.com/ws/2003/07/ws-federation)	[July-T, 4] [March-T, 110]
Active Directory Federation Services	ADFS	SAML Encapsulation of Security IDs in Tokens	ADFS uses SAML to encapsulate security IDs in tokens used to authenticate access to Windows applications. This ensures that only authorized users have access to Windows applications.	April 2004	The protocol delivers security and efficiency by implementing SAML Encapsulation of Security IDs in Tokens.	Microsoft's innovation report on "Microsoft Web Browse Federated Sign-on Protocol & Microsoft Web Browser Federated Sign-On Protocol Extensions", pages 13 to 18.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] OASIS, Security Services Technical Committee: SAML v1.0 Specification Set (5 November 2002 (adoption as an OASIS standard); http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security)	[July-T, 4] [March-T, 110]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Active Directory Federation Services	ADFS	Single Sign-on Capabilities for Web Access	ADFS implements single-sign on capabilities for web access by authenticating a user to a web resource through a third party authentication broker service.	April 2004	The protocol delivers usability via a third-party authentication service.	Microsoft's innovation report on "Microsoft Web Browse Federated Sign-on Protocol & Microsoft Web Browser Federated Sign-On Protocol Extensions", pages 8 to 13.	NON-INNOVATIVE	[PA] U.S. Patent 5,684,950: Method and system for authenticating users to multiple computer servers via a single sign-on (Lockheed Martin Corporation; 4 November 1997 (Filed 23 September 1996 as 08/717,961)) [PA] SecureComputing: SafeWord PremierAccess Authentication Broker (http://www.securecomputing.com/index.cfm?skey=854) [PA] Paschoud, John/McLeish, Simon: Managing Access to Decomate Resources (Logged into Economics: An assessment of the European Digital Library DECOMATE II, Barcelona, Spain; June 2000; http://hdl.handle.net/1988/2806) [PA] Rivest, Ronald A./Lampson, Butler: SDSI - A Simple Distributed Security Infrastructure (15 September 1996; http://people.csail.mit.edu/rivest/sdsi10.html) [PA] Lampson, Butler et al: Authentication in distributed systems: Theory and practice (ACM Transactions on Computer Systems 10(4); 265-310; November 1992; http://portal.acm.org/citation.cfm?id=138874) [R] Leach, Paul J. et al: A Conceptual Authorization Model for Web Services (K. Sparck-Jones and A. Herbert (eds.): Computer Systems: Theory, Technology, and Applications; 137-146; 2004; http://research.microsoft.com/Lampson/71-ConceptualWebAuthZ/71-ConceptualWebAuthZ.pdf)	[July-T, 3] [March-T, 109]
Active Directory Federation Services	ADFS	Use of HTTP Query Strings	ADFS uses query strings in HTTP messages as a way to transmit web access authentication information to a web resource via a client. One common way of transmitting this authentication information is through the use of HTTP Post messages. However, many clients do not support the use of HTTP Post. Data transfer using HTTP is a way to overcome these limitations.	April 2004	The protocol delivers interoperability and adaptability by the innovation of Query Strings in HTTP messages.	Microsoft's innovation report on "Microsoft Web Browse Federated Sign-on Protocol & Microsoft Web Browser Federated Sign-On Protocol Extensions", pages 18 to 20.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] RFC 2965: HTTP State Management Mechanism (October 2000; http://tools.ietf.org/html/rfc2965) [PA] RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1 (June 1999; http://tools.ietf.org/html/rfc2616)	[July-T, 3] [March-T, 110]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Active Directory Federation Services	ADFS	Windows Security Principal Mapping	ADFS uses SAML Security Tokens to transport security information including the identity of the requesting party. In a Windows environment, identities are stored in an Active Directory server as Windows Security Principals. ADFS bridges the gap between Windows Security Principals by mapping the Subject element of a Security Token to a Windows Security Principal and then replacing the AuthIdentity value with Windows Security Principal. This allows a server to quickly access security information in an Active Directory when starting with a Security Token.	April 2004	The protocol delivers efficiency through Windows Security Principal Mapping Innovation.	Microsoft's innovation report on "Microsoft Web Browse Federated Sign-on Protocol & Microsoft Web Browser Federated Sign-On Protocol Extensions", pages 21 to 22.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] NetBSD Programmer's Manual: Name-Service Switch (nsswitch) (22 January 1998; http://netbsd.gw.com/cgi-bin/man-cgi?nsswitch.conf++NetBSD-1.4.3) [PA] Sun Microsystems: Name-Service Switch (nsswitch) (SunOS Manual; December 2005; http://compute.cnr.berkeley.edu/cgi-bin/man-cgi?nsswitch.conf; This is a recent manual reference, but nsswitch has been available since at least 1986 as part of BSD UNIX 4.3.)	[March-T, 111]
Microsoft Content Indexing Services Protocol	CISP	Open Connect Feature	A client has traditionally needed to create a connection with a server in order to issue every query of a content indexing service. Clients often make repeated connections to a server in order to present multiple queries. This consumes more resources and is cumbersome. CISP eliminates this problem through its Open Connect Feature. This feature creates a client-server connection that enables the client to issue multiple queries to the server. As a result, clients can more efficiently query a content indexing server.	July 1996	The Open Connect Feature enhances efficiency by allowing multiple queries to be made serially through a single connection.	Microsoft's Innovation Report: "Content Indexing Service", pages 8 and 9.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[R] Koch, George: Oracle 7 (Osborne/McGraw-Hill, second revised edition; 609; March 1993) [PA] ISO: Information processing systems - Database language - SQL (ISO 9075:1987; http://archive.opengroup.org/public/tech/datam/sql.htm; The linked article provides some background about the chronology of the SQL standards.) [PA] O'Neil, Patrick: Database: Principles, Programming, and Performance (Morgan Kaufmann Publishers, San Francisco, first edition; 1994)	[March-T, 124]
Microsoft Content Indexing Services Protocol	CISP	Oversized Property Value Fetching	If a requested property is too large to fit into a response buffer, then the server flags the property as deferred rather than sending it. By way of a specific message the client requests the deferred property in a series of successive chunks.	July 1996	Oversized Property Value Fetching enhances efficiency by avoiding property value query result delays.	Microsoft's Innovation Report: "Content Indexing Service", pages 9 and 10.	NON-INNOVATIVE	[R] Microsoft: FP97: Using FrontPage Search Engine Instead of Microsoft Index Server (Frontpage 97 was released in 1997.; http://support.microsoft.com/kb/181204/EN-US/) [R] Kahle, Brewster: Wide Area Information Servers Concepts (Thinking Machines, technical report TCM 202; November 1988; http://nti.uji.es/software/Simple/docs/wais-concepts.txt) [PA] Hewlett-Packard: ALLBASE/SQL C Application Programming Guide, fourth edition (Manufacturing Part Number: 36216- 90080; 1992) [PA] ANSI: Information Retrieval Application Service Definition and Protocol Specification (ANSI Z39.50-1995; 1995; http://www.loc.gov/z3950/agency/markup/markup.html) [PA] ANSI: Information Retrieval Application Service Definition and Protocol Specification (ANSI Z39.50-1988; 1988)	[July-T, 11] [March-T, 124]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Microsoft Content Indexing Services Protocol	CISP	Pointer Embedding	Rows are grouped hierarchically. A certain message is used to request rows from a query. Another message replies with the requested rows. A set of pointers is used to identify the point at which data should be retrieved.	July 1996	Pointer Embedding enhances efficiency by reducing the burden on clients to find desired data.	Microsoft's Innovation Report: "Content Indexing Service", pages 11 and 12.	NON-INNOVATIVE	[R] Netscape: Netscape Catalog Server Version 1.0 (http://web.archive.org/web/20030424203159/http://library.n0i.net/netscape/compass/) [PA] ANSI: Information Retrieval Application Service Definition and Protocol Specification (ANSI Z39.50-1995; 1995; http://www.loc.gov/z3950/agency/markup/markup.html) [PA] ANSI: Information Retrieval Application Service Definition and Protocol Specification (ANSI Z39.50-1988; 1988) [R] Kahle, Brewster: Wide Area Information Servers Concepts (Thinking Machines, technical report TCM 202; November 1988; http://nti.uji.es/software/Simple/docs/wais-concepts.txt)	[July-T, 11-12] [March-T, 125]
Microsoft Content Indexing Services Protocol	CISP	Property Rich Queries	In querying a server, a client provides queries containing properties. Content indexing servers support numerous and diverse data types. Such data has typically been retrieved through a flat set of properties whereby complex data has been extracted in an unstructured manner. CISP has solved this problem through property rich queries allowing for a "divide and conquer" approach to data extraction. For example, CISP has defined globally unique property sets of extensible properties for efficiently extracting the desired data. By enhancing queries on the front end, search results have become more powerful.	July 1996	Property Rich Queries enhance usability, efficiency and functionality by efficiently structuring data types.	Microsoft's Innovation Report: "Content Indexing Service", page 8.	The description of the claim is unclear. NON-INNOVATIVE	[PA] O'Neil, Patrick: Database: Principles, Programming, and Performance (Morgan Kaufmann Publishers, San Francisco, first edition; 1994) [PA] Kahle, Brewster: Wide Area Information Servers Concepts (Thinking Machines, technical report TCM 202; November 1988; http://nti.uji.es/software/Simple/docs/wais-concepts.txt)	[March-T, 123]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Microsoft Content Indexing Services Protocol	CISP	Query Results Monitoring and Client Update Notification	Previously, when a client received results from a server based on a query, the server did not track whether there were additional hits later within the scope of the query. Therefore, unless the client ran the same query periodically, the client would be unaware of any updates. CISP solves this problem by having the CISP server track whether there are updates to a query. If the client has indicated it wishes to be notified of such updates, the server will send the updated query results to the client. The client therefore does not need to rerun the same query. This enhances reliability by ensuring that clients automatically learn of updated results.	July 1996	Query Results Monitoring and Client Update Notification improves reliability by alerting clients to updated query results.	Microsoft's Innovation Report: "Content Indexing Service", pages 12 and 13.	NON-INNOVATIVE	[PA] Informant: information.darthmouth.edu (Available before July 1996; http://groups.google.co.uk/group/alt.tv.homicide/browse_thread/thread/28cb88519cae1a54/9a4709ae76ded9df?lnk=st&q=informant. dartmouth.edu&rnum=1&hl=en#9a4709ae76ded9df; The informant was a service that alerted subscribers to new additions to the results of previously run queries.) [PA] Terry, Douglas B. et al: Continuous Queries over Append-Only Databases (Proceedings of the 1992 ACM SIGMOD International Conference on Management of Data, San Diego, CA, USA; 321-330; June 1992) [PA] Urhan, Tolga/Franklin, Michael J./Amsaleg, Laurent: Cost-based Query Scrambling for Initial Delays (Proceedings of ACM SIGMOD; 130-141; 1998; http://citeseer.ist.psu.edu/urhan98costbased.html)	[March-T, 125]
Microsoft Content Indexing Services Protocol	CISP	Remote Querying	A server hosting a content indexing service is remotely accessed by a client. The server is remotely administered by an administrator as well.	July 1996	Remote Querying enhances usability and efficiency by delegating search functions to dedicated servers, freeing up web server resources.	Microsoft's Innovation Report: "Content Indexing Service", pages 7 and 8.	NON-INNOVATIVE	[PA] ANSI: Information Retrieval Application Service Definition and Protocol Specification (ANSI Z39.50-1988; 1988) [PA] Kahle, Brewster: Wide Area Information Servers Concepts (Thinking Machines, technical report TCM 202; November 1988; http://nti.uji.es/software/Simple/docs/wais-concepts.txt)	[July-T, 10] [March-T, 123]
Distributed Component Object Remote Protocols	DCOM	Combination of DCOM Technologies	The combination of all the mentioned DCOM technologies.	May 2006	The combination of DCOM innovations is sustainable over the prior art cited and is useful beyond interoperability.	Microsoft's Innovation Report : "Distributed COM: Protocol Specification"	The claimed innovation is the combination of different features belonging to the same protocol. Combining these individual features is an obvious step for a person skilled in the art. NON-INNOVATIVE		[July-T, 14]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Distributed Component Object Remote Protocols	DCOM	Reclamation of Resources from Terminated Clients	In prior art methods, a server may allocate resources for clients that are no longer available, such as when a network connection is broken, a client crashes, or a client otherwise becomes unresponsive or unreachable. Typically, a client signals the server when it has finished with the associated server state. As such, a server would continue to hold state space for clients that were abnormally disconnected until the server is restarted. A server may encounter many abnormally terminated client connections, thereby wasting significant resources waiting for clients that cannot respond. In DCOM each object exporter has a configurable ping period time value and a minimum number of pings that the object exporter must receive in a set period of time. If the set time expires before the object exporter receives its threshold number of pings, the server reclaims its resources. Objects can also be configured not to require pings. Once the ping timeout is exceeded, the client is deemed dead or unreachable.	May 2006	The protocol promotes efficiency through reclamation of resources allocated for clients which have abnormally terminated.	Microsoft's Innovation Report : "Distributed COM: Protocol Specification", page 35.	NON-INNOVATIVE	[PA] Birrel, A. et al: Distributed Garbage Collection for Network Objects (Digital Equipment Corporation Systems Research Center, technical report 116; December 1993; http://citeseer.ist.psu.edu/birrell93distributed.html) [R] Ravenbrook: The Memory Management Reference Bibliography by Garbage Collection Technique (October 2000; http://www.memorymanagement.org/bib/gc.html; Garbage collection was invented by John McCarthy around 1959 to solve the problems of manual memory management in his Lisp programming language (http://en.wikipedia.org/wiki/Garbage_collection_%28computer_science%29) .)	[July-T, 14] [March-T, 61]
Microsoft Distributed File System	DFSCS	Interlinks and Cascaded Namespaces	Dfs link referral requests are triggered in response to a client receiving a failure code via an SMB message. The client is searching, via a link request, for alternative paths to reach a desired object. When a link is created and a link target is specified, any Universal Naming Convention (UNC) path can be used to name the link, including a path to another namespace. For example, a link target can be any UNC path: a shared folder, a folder underneath a shared folder, or a path to another Dfs namespace. When a client attempts to access a Dfs link on a new server share, it requests a link target referral from the Dfs server. These types of links are often called interlinks, and Distributed File System (Dfs) namespaces that point to other namespaces are referred to as cascaded namespaces.	December 1999	Interlinks and Cascaded Namespaces promote adaptability and fault tolerance by ensuring referral deployment and object accessibility.	Microsoft's Innovation Report: "DFS Referral", pages 23 to 26.	NON-INNOVATIVE	[PA] OpenAFS project: Andrew File System (AFS)/OpenAFS (commercial development by Transarc Corporation starting 1989; http://www.openafs.org/; also see AFS time line at http://www.dementia.org/twiki/bin/view/AFSLore/AncientHistory)	[July-T, 32-33] [March-T, 33]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Microsoft Distributed File System	DFSCS	Referral Management	Referral Management facilitates optimal referral deployment and file accessibility to DFS clients from any location on a distributed system. Referral Management includes DFSCS protocol features such as Target Failover, Target Failback and Set Boundary, Target Priority, referral expiration, and/or referral inconsistency reporting. Target Failover, Target Failback and Set Boundary, and/or Target Priority facilitate continued attempts to locate a DFS target based on accessibility, availability, site-cost, and/or designated priorities. Referral expiration promotes resource and time efficiency in that an associated timeout is designated for every link or root target after which a new referral request is made. Referral inconsistency reporting facilitates accuracy by reporting unsuccessful attempts to contact targets back to the root server that provided the referral.	December 1999	Referral Management promotes processing efficiency, adaptability, fault tolerance and accuracy by facilitating optimal referral deployment and file accessibility.	Microsoft's Innovation Report: "DFS Referral", pages 17 to 23.	INNOVATIVE		[July-T, 31] [March-T, 32]
Microsoft Distributed File System Replication	DFS-R	Chunk Partitioning with Local Maxima	The Chunk Partitioning with Local Maxima feature is applied by both the client and the server to create variably sized chunks the boundaries between which are determined by analyzing data features in the files. A sliding window referred to as a Horizon Window is used to evaluate every byte position in the file as a candidate for a cut-point. This feature identifies file differences with a higher degree of accuracy than other conventional compression techniques, while using less processing and system storage resources.	December 1999	Chunk Partitioning with Local Maxima increases processing efficiency.	Microsoft's Innovation Report: "Remote Differential Compression", pages 7 to 13.	NON-INNOVATIVE	[R] Teodosiu, Dan et al: Optimizing File Replication over Limited-Bandwidth Networks using Remote Differential Compression (MSR-TR-2006-157; November 1996; ftp://ftp.research.microsoft.com/pub/tr/TR-2006-157.pdf; Page 14: "...[Broder 1997] employed similarity techniques from which the one we present is derived.") [PA] Broder, Andrei Z.: On the Resemblance and Containment of Documents (Proceedings of Compression and Complexity of SEQUENCES; 1997; http://citeseer.ist.psu.edu/broder97resemblance.html) [PA] Manber, Udi: Finding Similar Files in a Large File System (Usenix Winter 1994 Technical Conference, San Francisco, CA, USA; 1-10; January 1994; http://citeseer.ist.psu.edu/manber94finding.html)	[July-T, 29-30] [March-T, 8]
Microsoft Distributed File System Replication	DFS-R	Fencing Values	In a multi-master replication system, any server may make unrestricted changes to replicated content in a given replica set. This freedom also presents the issue of potentially conflicting changes. Thus, there must be conflict resolution criteria that define, for every conflict situation, which conflicting change takes precedence over others. Fencing Values allow an overriding conflict policy to be established with respect to a resource.	December 2005	The use of Fencing Values promotes the benefit of data accuracy and adaptability by allowing users to establish a conflict policy.	Microsoft's innovation report: "Microsoft Distributed File System Replication", pages 12 to 17.	NON-INNOVATIVE	[PA] Petersen, Karin et al: Flexible Update Propagation for Weakly Consistent Replication (Proceedings of the 16th ACM Symposium on Operating Systems Principles (SOSP-16), Saint Malo, France; 288-301; October 1997; (http://citeseer.ist.psu.edu/petersen97flexible.html))	[July-T, 26] [March-T, 5]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Microsoft Distributed File System Replication	DFS-R	RDC Protocol When Taken as a Whole	The combination of all the mentioned RDC technologies (Chunk Partitioning with Local Maxima, Recursive Compression, Similarity Detection).	December 2005	Innovative effects are achieved through the combination of the RDC Protocol technologies.	Microsoft's Innovation Report: "Remote Differential Compression"	The claimed innovation is the combination of different features belonging to the same protocol. Combining these individual features is an obvious step for a person skilled in the art. NON-INNOVATIVE		[July-T, 29]
Microsoft Distributed File System Replication	DFS-R	Recursive Compression	After the desired file is chunked in accordance with the Microsoft RDC Chunk partitioning feature, a Signature List is created which can then be fed back into RDC Chunk partitioning to generate a Recursive Signature List. The Recursive Signature List is extremely compact, often reducing the amount of data necessary for transferring the Signature List by an order of magnitude (e.g., from hundreds of kilo-bytes to a few kilobytes). By compressing the original Signature List, network resource utilization is reduced and transfer times are improved. The Microsoft RDC recursive compression technique is functional and highly suitable for very large files or large file systems, where the data bottleneck on network resources can be very significant. Unlike the RSYNC algorithm, where recursion is decidedly not applied in favor of minimizing round-trip times, the recursive compression in Microsoft's RDC is used to decrease transfer times and minimize transfer file size. Moreover, RDC does not require additional cache storage beyond that needed (if any) for the original Signature List.	December 1999	Recursive Compression promotes resource efficiency and adaptability by reducing transfer time with compressed signature files.	Microsoft's Innovation Report: "Remote Differential Compression", pages 13 to 22.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] U.S. Patent 5,486,826: Method and apparatus for iterative compression of digital data (PS Venture 1 LLC; 23 January 1996 (Filed 19 May 1994 as 08/246,014)) [PA] Chien, S./Gratch, J.: Producing Satisfactory Solutions to Scheduling Problems: An Iterative Constraint Relaxation Approach (June 1994; http://hdl.handle.net/2014/33806) [PA] Miyashita, Kazuo: Improving System Performance in Case-Based Iterative Optimization through Knowledge Filtering (Proceedings of the International Joint Conference on Artificial Intelligence; 371-376; 1995; http://citeseer.ist.psu.edu/37779.html) [PA] Fisher, Doug: Iterative Optimization and Simplification of Hierarchical Clusterings (Journal of Artificial Intelligence Research 4; 147-179; http://www.cs.cmu.edu/afs/cs/project/jair/pub/volume4/fisher96a.pdf)	[July-T, 30] [March-T, 9]
Microsoft Distributed File System Replication	DFS-R	Shared Database	DFS-R uses a Shared Database for replicating changes among members of a replica set. The database stores metadata of replicated files, including updates (related to file creations, changes, and deletions) and version chain vectors. It eliminates the need for each member to establish and manage its own database. This eliminates the duplication of resources. Moreover, It reduces replication latency. An upstream member may simply provide the location of information in the shared database to the client. The client can then directly retrieve the necessary information, eliminating the step of having to transfer information through the upstream member.	December 2005	The use of a Shared Database for replication information promotes the benefits of resource and time efficiency.	Microsoft's innovation report: "Microsoft Distributed File System Replication", pages 23 to 25	The claimed innovation is the combination of different features belonging to the same protocol. Combining these individual features is an obvious step for a person skilled in the art. NON-INNOVATIVE		[July-T, 28] [March-T, 7]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Microsoft Distributed File System Replication	DFS-R	Similarity Detection	Similarity Data is generated for a file that is located on one system using a fingerprinting function. The Similarity Data is highly compact and can be stored in the form of metadata that is communicated between the remote device and the local device. The highly compact nature of the Similarity Data is efficient in the use of network resources by conserving bandwidth utilization. The Similarity Data does not create a taxing overhead on file transfers and scales extremely well for large files. The use of Similarity Data also increases the probability of locating an appropriate file match for updating under RDC.	September 2004	Similarity Detection promotes processing efficiency by using minimal metadata to locate similar files with improved accuracy.	Microsoft's Innovation Report: "Remote Differential Compression", pages 23 to 28.	NON-INNOVATIVE	[PA] Broder, Andrei Z.: On the Resemblance and Containment of Documents (Proceedings of Compression and Complexity of SEQUENCES; 1997; http://citeseer.ist.psu.edu/broder97resemblance.html) [PA] Manber, Udi: Finding Similar Files in a Large File System (Usenix Winter 1994 Technical Conference, San Francisco, CA, USA; 1-10; January 1994; http://citeseer.ist.psu.edu/manber94finding.html)	[July-T, 31] [March-T, 10]
Microsoft Distributed File System Replication	DFS-R	Use of Epoch Values	In a multi-master replication system any server may make unrestricted changes to replicated content in a given replica set. One problem that arises in multimaster replication systems is the propagation of stale data. Microsoft's innovative epoch values address this problem. To avoid the replication of stale data, Microsoft developed the Use of Epoch Values to indicate the latest time when a member's version chain vector had been updated. This serves as an indication of the freshness of a member's content with respect to a resource. An epoch value can be compared to the current time, or to an epoch value of a member, to determine whether the information meets a threshold for freshness, or relative freshness. Ensuring that only fresh information is replicated provides significant benefits of data accuracy to a user. Alternative technologies do not provide for comparing values of version chain vectors to determine the freshness of data on a member, prior to replicating information between members of a replica set.	December 2005	The Use of Epoch Values promotes the benefit of data accuracy by preventing the replication of state content.	Microsoft's innovation report: "Microsoft Distributed File System Replication", pages 18 to 23.	NON-INNOVATIVE	[PA] Merrells, John/Reed, Ed/Srinivasan, Uppili: LDAP Replication Architecure Draft (IETF draft; section 4.4; August 1998; http://www.imc.org/ietf-ldup/mail-archive/msg00138.html) [PA] Petersen, Karin et al: Bayou: Replicated Database Services for World-wide Applications (Proceedings of the 7th SIGOPS European Workshop, Connemara, Ireland; 275-280; September 1996; http://citeseer.ist.psu.edu/petersen96bayou.html)	[July-T, 27] [March-T, 6]
Microsoft Distributed File System Replication	DFS-R	Version Chain Vectors	The Version Chain Vectors associate version sequence numbers with unique object/resource identifiers. As one example, changes may be made to a replica by creating a new directory, and creating new files within the directory. Version chain vectors give clients the ability to recognize that replicating the new files correctly depends on first replicating the new directory under which the files will be organized. This innovation avoids errors that may result from replicating changes out of order, such as new files before a new directory.	December 2005	The use of Version Chain Vectors promotes the benefit of data accuracy by allowing a client to recognize dependant updates.	Microsoft's innovation report: "Microsoft Distributed File System Replication", pages 7 to 12.	NON-INNOVATIVE	[PA] U.S. Patent 5,765,171: Maintaining consistency of database replicas (Lucent Technologies; 9 June 1998 (Filed 29 December 1995 as 08/580,954)) [PA] Petersen, Karin et al: Bayou: Replicated Database Services for World-wide Applications (Proceedings of the 7th SIGOPS European Workshop, Connemara, Ireland; 275-280; September 1996; http://citeseer.ist.psu.edu/petersen96bayou.html)	[July-T, 25-26] [March-T, 4]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Net Logon Remote Protocol	DIGEST	General Pass-Through Authentication	Net Logon's generic pass-through allows multiple authentication protocols (e.g. NTLM, Kerberos) to communicate with a domain controller using Net Logon's secure channel. Any authentication data can utilize Net Logon's secure channel for passing secure data to a domain controller. As a benefit, workstations and servers can forego the overhead associated with providing their own secure channel to the domain controller. Prior authentication protocols were limited to using channels that were allowed by their transportation packages and these channels were often unsecured. Net Logon provides the flexibility to work in combination with other protocols. For instance, a new authentication protocol can rely on the secure channel provided by Net Logon.	December 1999	Generic Pass-Through Authentication delivers network functionality through improved interoperability.	Microsoft's Innovation Report: "Net Logon Remote", pages 99 to 11.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] Pfleeger, C. P.: Security in Computing, second edition (Prentice Hall, Upper Saddle River, NJ, USA; 1996; page 412)	
Net Logon Remote Protocol	DIGEST	Service Discovery	Within a network, there are typically a number of servers that work together to provide services to the clients or workstations. These servers are often referred to as Domain Controllers (DCs). Although a DC can provide multiple services, it was not always clear to the client which server provides which services. This is important since the client requesting or needing a particular service must interact with the right server. Prior to this version of Net Logon, to find and use a particular DC service, a client painstakingly polled the DCs in the network to determine service capability. This method was an inefficient means for a client to try to locate a service and even more so if a previously discovered service stopped, requiring subsequent rounds of querying. Net Logon solved this problem by implementing a service-locating query. A client can request a service of any DC in the form of a query and the appropriate DC providing that service will reply. As a further benefit, a service discovery request can include a site name to locate the closest DC providing the service.	December 1999	Net Logon delivers network efficiency through faster Service Discovery.	Microsoft's Innovation Report: "Net Logon Remote", pages 6 to 9.	NON-INNOVATIVE	[PA] Cisco: Appletalk Specification (1984; www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1909.htm)	

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Distributed Link Tracking Remote Protocol	DLTP	Backup-Driven File Link Deactivation	A shell shortcut is a binary file containing information about an object whereby a user or application can quickly access the object without knowing its current name or location. Due to a backup or restore operation, an object may be restored to a new location, creating duplicate objects. The shell shortcut could then be referencing the incorrect object. The Distributed Link Tracking Protocol overcomes this problem by deactivating file movement updates during backup and restore operations. As a result, an original copy of the object is maintained in a proper file location.	December 1999	Backup-Driven File Link Deactivation maintains file link security and efficiency.	Microsoft's Innovation Report: "Distributed Link Tracking Workstation, Distributed Link Tracking Central Manager, and Distributed Link Tracking Central Store", pages 25 to 27.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[R] N.N.: Backing up a Unix(-like) system (http://www.halfgaar.net/backing-up-unix)	[July-T, 36] [March-T, 116]
Distributed Link Tracking Remote Protocol	DLTP	Domain Relative Tracking	Locating moved files has been a persistent problem for computers. Techniques for linking to files have often been thwarted by renaming of files, directories or machines. Users have avoided moving files when helpful out of fear that the files will not be found when needed. By uniquely identifying a file within a domain, Microsoft's domain-relative tracking delivers robustness in file link integrity.	December 1999	Domain Relative Tracking promotes file link integrity.	Microsoft's Innovation Report: "Distributed Link Tracking Workstation, Distributed Link Tracking Central Manager, and Distributed Link Tracking Central Store", pages 13 to 16.	INNOVATIVE		[March-T, 113]
Distributed Link Tracking Remote Protocol	DLTP	File Location Tracking Machine	Many systems have relied upon file names and other basic metadata to locate files. These strategies often fail when files are moved within a volume, across volumes or across machines. Microsoft's file location tracking search machine fills that file link integrity gap by tracking the previous and current locations of file.	December 1999	File Location Tracking Machine promotes file link integrity.	Microsoft's Innovation Report: "Distributed Link Tracking Workstation, Distributed Link Tracking Central Manager, and Distributed Link Tracking Central Store", pages 16 to 21.	INNOVATIVE		[March-T, 113-114]
Distributed Link Tracking Remote Protocol	DLTP	Previous Link Move Notification	A move notification for a file must specify the previous location of the file. Similarly, a notification to a DLT Central Manager server that a file has moved refers to files with respect to their volume. The parameters within a notification include rgdroidBirth (previous file location), rgdroidNew (current or new location) and rgobjidCurrent (file identifier). Each parameter is defined in terms of the associated volume. A DLT Central Manager client sends a search request to find a file's current location. The parameter request include droidBirth (file identifier) and droidLast (last known location of the file).	December 1999	Previous Link Move Notification enhances security for file tracking.	Microsoft's Innovation Report: "Distributed Link Tracking Workstation, Distributed Link Tracking Central Manager, and Distributed Link Tracking Central Store", pages 21 to 23.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] Bell Telephone Laboratories: UNIX Programmer's Manual, Seventh Edition, Volume 1 (124; January 1979; http://cm.bell-labs.com/7thEdMan/v7vol1.pdf; (mv command))	[July-T, 35] [March-T, 114-115]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Directory Replication Service Remote Protocol	DRS	Automated Topology Modeling	A network of servers requires a topology to manage communication between the several servers. The topology organizes the servers in sites and organizes the sites into an ordered structure. This topology must be generated for the network. Old techniques of topology generation required the manual creation of the topology by a network administrator. The manual generation of the topology was often less efficient and potentially more error-prone. DRS addresses these shortcomings by providing an automated topology modeling. An administrator can enter data, such as costs of connections, and then the Knowledge Consistency Checker (KCC) automatically generates the topology model. This automated modeling enables an administrator to give very specific directions to the KCC regarding a specific topology design, while at the same time allowing the KCC to generate the topology and related objects and data without intervention by the administrator. For example, an administrator could create a link, and the KCC will respond to this creation by augmenting the link, if necessary, with information or attributes to create a new topology.	December 1999	Automated Topology Modelling promotes processing efficiency by using the least-costly communication path between servers.	Microsoft's Innovation Report: "Directory Replication Service Remote Protocol", pages 21 to 23.	NON-INNOVATIVE	[PA] Wang, Randolph Y./Anderson, Thomas E.: xFS: A Wide Area Mass Storage File System (Fourth Workshop on Workstation Operating Systems; 71-78; October 1993; http://citeseer.ist.psu.edu/161339.html) [PA] Guy, Richard G.: Ficus: A Very Large Scale Reliable Distributed File System (PhD thesis, University of California, Los Angeles (UCLA technical report CSD-910018); June 1991; http://citeseer.ist.psu.edu/guy91ficu.html)	
Directory Replication Service Remote Protocol	DRS	Behavior Versioning	Software updates help remove bugs and improve the function of the software. Server software can be updated periodically by administrators. Each site might have different versions of software operating because the updates do not occur simultaneously. Old techniques of update administration would prevent functionality between servers executing different software versions. Thus, all servers would need to execute the same software to collaborate. The network running different versions of a software on different servers does not necessarily operate properly until all software updates are completed. DRS addresses these shortcomings by the use of a behaviour vector approach to enable global network upgrading of versions. The behavior vector supports a "feature list", as opposed to a "hierarchy" approach. The sequential hierarchy describes each set of features that the version of software being executed may use. Each server supports up to a certain version level.	December 1999	Behavior Versioning promotes changeability by allowing different versions of software on different servers to function together.	Microsoft's Innovation Report: "Directory Replication Service Remote Protocol", pages 103 to 105.	NON-INNOVATIVE	[PA] U.S. Patent 5,832,275: System for dynamically replacing operating software which provides distributed directory service after verifying that versions of new software and the operating software are compatible (3 November 1998 (Filed 4 June 1997 as 08/871,569)) [PA] Intel: Intel Architecture Software Developer's Manual Volume 1: Basic Architecture (section 10; 1997) [PA] ISO/IEC: X.519: ISO/IEC 9594-5: The Directory: Protocol specifications (http://archive.dante.net/np/ds/osi/9594-5-X.519.A4.ps; The use of protocol versioning to control the behaviors of directory instances in a topology is defined in the section 7.5 of the standard.)	[July-T, 42] [March-T, 27] [ECIS, 33]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Directory Replication Service Remote Protocol	DRS	Combination of Automated Topology Modification Technologies	The combination of all the mentioned Automated Topology Modification technologies.	December 1999	Combination of Automated Topology Modification Technologies Achieves Innovative Automated Topology Modification and Management.	Microsoft's Innovation Report: "Directory Replication Service Remote Protocol"	The claimed innovation is the combination of different features belonging to the same protocol. Combining these individual features is an obvious step for a person skilled in the art. NON-INNOVATIVE		[July-T, 39]
Directory Replication Service Remote Protocol	DRS	Combination of Information Disclosure Technologies	The technologies combined to effect Microsoft's innovation in improved Information Disclosure are: (1) automated domain controller location process; and (2) global catalog querying of distributed data.	December 1999	A combination of technologies creates the innovative systems and methods of the DRSR Protocol for promoting functionality, resource efficiency, adaptability, and usability for innovative Information Disclosure in a multimaster database where multiple servers replicate and provide one or more resources.	Microsoft's Innovation Report: "Directory Replication Service Remote Protocol"	The claimed innovation is the combination of different features belonging to the same protocol. Combining these individual features is an obvious step for a person skilled in the art. NON-INNOVATIVE		[July-T, 43]
Directory Replication Service Remote Protocol	DRS	Combination of Optimizing Replication Technologies	The combination of all the mentioned Optimizing Replication Modification technologies.	December 1999	The Combination of the individual Optimizing Replication Technologies to achieve the overall innovation of optimized replication is innovative.	Microsoft's Innovation Report: "Directory Replication Service Remote Protocol"	The claimed innovation is the combination of different features belonging to the same protocol. Combining these individual features is an obvious step for a person skilled in the art. NON-INNOVATIVE		[July-T, 40-41]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Directory Replication Service Remote Protocol	DRS	Global Catalog Search	Locating information in a distributed directory requires searching each server for the information. Each server is addressed and then asked for the required information. The searching process can become time-consuming if the network is large and distributed over several distant locations. Old techniques would query each server. It was difficult to obtain accurate search results when searching took place across domains/partitions. In addition, completing more difficult searches, such as recursive group expansion searches across domains, could lead to continually expanding searches and were not possible in previous systems. Microsoft's Global Catalog addresses these shortcomings by the use of the Global Catalog which allows a single-point search for information that resides across domains. The GC creates a unified view of all naming contexts in a distributed partitioned directory to enable efficient distributed querying. Microsoft's Global Catalog provides a single source for searches that eliminates the single-server searches that a user would have had to complete and that would use excessive network bandwidth.	December 1999	Global Catalog Search promotes changeability by allowing querying of distributed data.	Microsoft's Innovation Report: "Directory Replication Service Remote Protocol", pages 115 to 116.	NON-INNOVATIVE	[PA] Gopal, Burra/Manber, Udi: Integrating content-based access mechanisms with hierarchical file systems (Operating Systems Design and Implementation, Proceedings of the third symposium on Operating systems design and implementation, New Orleans, Louisiana, USA; 265-278; 1999; http://portal.acm.org/citation.cfm?id=296806.296838) [PA] Manber, Udi: GLIMPSE: A Tool to Search Through Entire File Systems (Proceedings of the USENIX Winter 1994 Technical Conference, San Fransisco, CA, USA; 23-32; January 1994; http://citeseer.ist.psu.edu/manber94glimpse.html) [PA] Novell: Novell Directory Services (1993) [PA] Lotus: Global Address Book of Lotus Notes Release 4.0 (January 1996; http://www.ibm.com/developerworks/lotus/library/ls-NDHistory/) [PA] U.S. Patent 5,551,027: Multi-tiered indexing method for partitioned data (IBM; 27 August 1996 (Filed 11 September 1995 as 08/526,723))	[July-T, 43] [March-T, 29] [ECIS, 34]
Directory Replication Service Remote Protocol	DRS	KCC Monitoring for Automated Topology Management - ISTG latency monitoring	DRS provides a Knowledge Consistency Checker (KCC) that constructs a circular path of all the intra-site servers in a ring fashion, such that even if one node breaks, the domain controllers on each side of the broken node may still connect and thus allow for continual replication. The KCC thus allows for "routing around" domain controllers from which replication cannot be accomplished. The KCC also detects and routes around failed domain controllers acting as Intersite bridgehead servers. The KCC conducts both intrasite and intersite monitoring for failed servers which could cause breaks in convergence.	December 1999	The protocol provides for Automated Topology Management through monitoring of latency of the Intersite Topology Generator (ISTG), by configuring and adjusting the connections between servers, or domain controllers, and enabling automatic replication throughout the network.	Microsoft's Innovation Report: "Directory Replication Service Remote Protocol", page 49	NON-INNOVATIVE	[PA] Paxson, Vern: End-to-End Routing Behavior in the Internet (IEEE/ACM Transactions on Networking 5(5); 601-615; October 1997; http://citeseer.ist.psu.edu/3573.html) [PA] RFC 1771: A Border Gateway Protocol 4 (BGP-4) (March 1995; http://tools.ietf.org/html/rfc1771) [PA] Walker, Bruce/Popek, Gerald et al: The LOCUS Distributed Operating System (Proceedings of the 9th ACM Symposium on Operating Systems Principles; 49-70; October 1983)	[July-T, 38-39] [March-T, 20]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Directory Replication Service Remote Protocol	DRS	Managing the Addition, Removal and Rejoining of Partitions	Different data may require different partitions, or naming contexts (NC). Adding or changing data may require the addition or modification of partitions. Through the Global Catalog (GC), the DRS protocol provides for the automatic addition and removal of NC replicas for domain NCs identified by objects in the Partitions container of the config NC. The config NC also contains a set of objects - one for each DC - which grows or shrinks as new DCs are added to or removed from the forest.	December 1999	This technology provides the benefits of changeability and reliability by automatically adjusting the addition and removal of Naming Contexts and Domain Controllers in the network.	Microsoft's Innovation Report: "Directory Replication Service Remote Protocol", pages 51 to 54.	NON-INNOVATIVE	[PA] Liskov, Barbara et al: Replication in the Harp File System (Proceedings of 13th ACM Symposium on Operating Systems Principles; 226-238; October 1991; http://citeseer.ist.psu.edu/liskov91replication.html) [PA] International Telegraph and Telephone Consultative Committee (CCITT): Recommendation X.501 (chap. 10 "The Administrative Authority Model"; 1993) [PA] RFC 1034: Domain names - concepts and facilities (November 1987)	[July-T, 39] [March-T, 22] [ECIS, 28]
Directory Replication Service Remote Protocol	DRS	Replication Convergence Despite Server Failure	DRS provides for convergence of replication even where multiple domain controllers are involved and where there is a potential, in a global-scale multi-master replication environment, for at least one server to be off-line or to otherwise replicate in a non-optimal state. Replication convergence requires both connectivity between servers and an agreement between servers as to the correct version of the replica. Thus, a server failure that breaks the connectivity of the network servers precludes the possibility of convergence. Prior global-scale replication systems could experience interruptions and "breaks" in convergence if a server failed. As a result, errors and duplicate replications, among other problems, were inherent defects in such environments.	December 1999	Replication Convergence Despite Server Failure promotes fault tolerance, time and resource efficiency, changeability and stability by not allowing a failed server to cause a "break" in convergence.	Microsoft's Innovation Report: "Directory Replication Service Remote Protocol", pages 45 to 48.	NON-INNOVATIVE	[PA] Walker, Bruce/Popek, Gerald et al: The LOCUS Distributed Operating System (Proceedings of the 9th ACM Symposium on Operating Systems Principles; 49-70; October 1983) [PA] Siegel, Alexander/Birman, Kenneth P./Marzullo, Keith: Deceit: A Flexible Distributed File System (Cornell University, Ithaca, NY, USA, technical report TR89-1042; 1989; http://portal.acm.org/citation.cfm?id=866411)	[July-T, 38-39] [March-T, 19]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Directory Replication Service Remote Protocol	DRS	Replication Latency	AD provides a multi-master database where several servers share the contents of the database. The data on the servers is often replicated where several replications may occur and some replications may be pending. However, one or more servers may become latent through failure or other processes. Replications will continue to be sent to the server that became latent, but the server will not be able to update. When the server is ready to be updated, one or more old replications will need to be identified and sent to the server. DRS ensures that only replications missed during the period of latency are sent to servers that are no longer latent by giving each server a vector table that includes state information about other servers in the system. If a server is latent or fails, the server is found via monitoring the vector table so that users can be notified. The replica partner vector table includes data fields for storing an update sequence number and timestamp information that identifies the time of the last update and/or the time of the last successful replication attempt for each replica server.	December 1999	Replication Latency promotes improved stability and resource efficiency by ensuring that only changes occurring during latency are sent to a recovered server.	Microsoft's Innovation Report: "Directory Replication Service Remote Protocol", pages 88 to 96.	NON-INNOVATIVE	[PA] Merrells, John/Reed, Ed/Srinivasan, Uppili: LDAP Replication Architecure Draft (IETF draft; section 4.4; August 1998; http://www.imc.org/ietf-ldup/mail-archive/msg00138.html)	[July-T, 40-41] [March-T, 25]
Directory Replication Service Remote Protocol	DRS	Simultaneous Domain Rename	When a forest requires a domain rename, each server in the forest must make the name change. Old techniques would attempt to propagate the rename one server at a time. However, the rename could be propagated through a majority of the system and then get backed out due to a single server failure. DRS addresses the rename failure shortcoming by use of a script language built for renaming and restructuring. A tool is used to create the script that describes the enterprise rename, and the generated script is then replicated throughout the system. Methods allow the servers to prepare and run the script. By running the methods, the domain controllers are able to understand the script, accept it, and execute it. A triggering mechanism then allows for simultaneous execution of the name change across all of the domain controllers. The replication of the script before the execution of the rename provides enough time to complete replication regardless of possible server failures. Then, upon the trigger, all servers are renamed without the problem of the rename being backed out.	March 2003	Simultaneous Domain Rename promotes stability by coordinating domain renames of forests that ensure adoption across the forest.	Microsoft's Innovation Report: "Directory Replication Service Remote Protocol", pages 35 to 38.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] Gray, Jim: Notes on Data Base Operating Systems (Lecture Notes In Computer Science, vol 60: Operating Systems, An Advanced Course; 393 - 481; 1978; Microsoft has implemented the two phase commit protocol described in section 5.8.3.3 20 years after it was first described.)	[July-T, 38-39] [March-T, 17]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Directory Replication Service Remote Protocol	DRS	Use of GUID Identification	DRS allows for simultaneous forest rename without requiring a ground-up re-install of the name change. Prior systems presented numerous problems associated with the propagation of a name change. For example, without simultaneous renaming amongst domain controllers, a rename propagated through a large part of the system failed when a server identified by a name could not be contacted during the rename because the name was changed or inaccurate. The DRS protocol solves the problems associated with servers identified with names by using the innovative identification of servers by a globally unique identifier (GUID). By identifying servers by GUID instead of by name, the servers can still be contacted even during a rename.	December 1999	The protocol allows efficient renaming through the Use of GUID Identification.	Microsoft's Innovation Report: "Directory Replication Service Remote Protocol", pages 50 to 51.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] Kong, Mike et al: Network computing system reference manual (Prentice-Hall, Upper Saddle River, NJ, USA; 1990; Network computing system was Apollo Computer's implementation of the Networkig Computing Architecture (NCA).) [PA] Transarc Corporation: Distributed File System (DFS) (http://en.wikipedia.org/wiki/DCE_Distributed_File_System; Transarc was founded in 1989 and commercially developed the Andrew File System (AFS) and the Distributed File System (DFS aka DCE/DFS). Transarc was bought by IBM in 1998 and became the IBM Pittsburgh Lab in 1999.) [PA] Stokes, Ellen/Good, Gordon: The LDUP Replication Update Protocol (22 October 1999; http://www3.ietf.org/proceedings/99nov/I-D/draft-ietf-ldup-protocol-00.txt)	[March-T, 21] [ECIS, 27]
ExtendedError Remote Protocol Extensions	EERR	Building Error Reports using a Rich Extended Error Schema	Microsoft's EERP Provides for Encoding of Error Records in a Structured Schema for Use by a Human Reader, where the Error Records are Extensible.	August 2001	Building Error Reports Using a Rich Extended Error Schema is innovative and advantageous over alternatives.	Microsoft's Innovation Report: "ExtendedError Remote"	NON-INNOVATIVE		[July-T, 44-45]
ExtendedError Remote Protocol Extensions	EERR	Encoding of Error Records in a Structured Schema for Use by a Human Reader	An error message often results in a cascade of error messages throughout a computer network. In complex computer networks, this can lead to countless error messages. A software agent, trying to identify and fix the error, is placed in the unenviable position of seeking the root error through a large number of symptomatic and less important error messages. This leads to time-consuming and inefficient trouble shooting. Microsoft addressed this problem by designing a scheme that maintains the error records in a linked list. The linked list permits a software agent to quickly trace an error message to the root.	August 2001	Encoding of Error Records in a Structured Schema for Use by a Human Reader promotes efficiency and reliability by enabling faster and more accurate troubleshooting.	Microsoft's Innovation Report: "ExtendedError Remote", pages 6 to 8.	NON-INNOVATIVE	[PA] IBM: OS/400 API Error Reporting (Introduced in 1998; http://publib.boulder.ibm.com/iseries/v5r1/ic2924/index.htm?info/apis/error.htm)	[July-T, 46-47] [March-T, 39]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
ExtendedError Remote Protocol Extensions	EERR	Encoding of Error Records in a Structured Schema for Use by a Human Reader, which Includes an Error Linked List	In complex computer systems, an error encountered on one network node often has to be transmitted to another network node. Depending on the complexity of the computer network, the information relating to the error might prove insufficient causing a software agent to pursue countless symptoms before finding the cause. EERR addresses this problem by creating a scheme for encoding extended errors (hereinafter "schema") that compiles information a software agent needs to perform proficient and effective troubleshooting. For example, information identifying the computer on which an error occurred may be important to troubleshooting, and is provided with the schema.	August 2001	Error Report Building through a schema providing a linked error list promotes efficiency and reliability through the compilation and capture of information about errors allowing to identify root causes of network problems.	Microsoft's Innovation Report: "ExtendedError Remote", pages 8 to 9.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE		[July-T, 47-48] [March-T, 40]
Encrypted File System Remote Protocol	EFS	Administrative Control of Encryption	EFS allows administrators to control encryption and decryption of client files on servers.	December 1999	Administrative Control of Encryption improves security through deployment of encryption policies.	Microsoft's Innovation Report "Encrypting File System Remote", on pages 7 to 11.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] GNU project: The GNU privacy guard (20 December 1997; http://www.gnupg.org/; http://www.gnupg.org/(en)/download/release_notes.html) [PA] Cooper, Mendel: Advanced Bash-Scripting Guide. An in-depth exploration of the art of shell scripting (24 June 2007; http://tldp.org/LDP/abs/html; http://personal.riverusers.com/~thegrendel/Change.log; (The guide describes functionality that was available with release of the different Bash versions starting from 1987 and thus long before the first version of the guide itself was released on 14 June 2000.)) [PA] Blaze, Matt: A Cryptographic File System for Unix (Proceedings of the 1st ACM Conference on Computer and Communications Security; 9-16; November 1993; http://citeseer.ist.psu.edu/blaze93cryptographic.html)	[July-T, 50] [March-T, 141]
Encrypted File System Remote Protocol	EFS	Customized User Encryption Permissions	EFS allows the user to define access for a particular encrypted file or group of files by adding or deleting those individuals that the user wishes to allow access to the encrypted file(s).	December 1999	Customized User Encryption Permissions enhance transparency and usability of encrypted files while maintaining security through user control of access to the encrypted files.	Microsoft's Innovation Report "Encrypting File System Remote", on pages 7 to 11.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] NSA: NSA Security-Enhanced Linux (22 December 2000; http://www.nsa.gov/selinux/) [PA] Sun Microsystems: Java (Java 2 (SDK 1.2) was announced on 8 December 1998; http://java.sun.com) [PA] Hewlett-Packard: Accessing Files Programmers Guide (Manufacturing Part Number: 32650-90885; March 2000; This manual is about the HP 3000 machine which went through several development stages between 1971 and today.) [R] Tanenbaum, Andrew S.: Operating Systems: Design and Implementation (Prentice Hall, Upper Saddle River, NJ, USA; 1987)	[July-T, 49] [March-T, 140]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Encrypted File System Remote Protocol	EFS	Data Recovery Agent	The protocol utilizes data recovery agents that are added to metadata associated with each encrypted file. The data recovery agents include a recovery key that is used to recover the encrypted data should the user lose the original key used to encrypt the file. In addition, the recovery key can be used by an enterprise to access the enterprise's encrypted files regardless of whether the personnel that encrypted the files are unavailable or uncooperative. It therefore addresses the issue of recovery of files when the keys used to encrypt the files have been lost or are otherwise unavailable.	December 1999	Use of Data Recovery Agent transparently improves usability and security through automatic association of the recovery agent with an encrypted file.	Microsoft's Innovation Report "Encrypting File System Remote", on pages 7 to 11.	NON-INNOVATIVE	[PA] SowSoft: Big Crocodile Password Manager (http://www.sowsoft.com/bigcroc.htm) [PA] WhiteCanyon Software: MySecurityVault PRO (http://www.whitecanyon.com/password-backup.php) [PA] Brostoff, Sacha: Improving Password System Effectiveness (PhD thesis, University College London; September 2004) [PA] U.S. Patent 6,842,523: Encryption apparatus, cryptographic communication system, key recovery system and storage medium (Kabushiki Kaisha Toshiba; 11 January 2005 (Filed 24 November 1999 as 09/448,470))	[July-T, 49] [March-T, 140]
Encrypted File System Remote Protocol	EFS	Remote Key Update and Cache Flush	EFS allows users and administrators to remotely access and update information related to the encryption of files. The user can access information about the keys used to encrypt the file, update the keys associated with the file to grant or deny access to other individuals, and obtain information about whether the user can encrypt or decrypt the file. It also allows the user to remotely flush the logical cache on the server that holds all of the sensitive information, such as key information, required to perform operations for the user. Previous technology that lacked this innovation was less secure and less usable because a remote user concerned about a breach of security with respect to his or her encryption information did not have a readily available means of changing or flushing such information to prevent misuse.	December 1999	Remote Key Update and Cache Flush enhance usability and security through allowing users to remove, change or delete sensitive user encryption information.	Microsoft's Innovation Report "Encrypting File System Remote", on pages 7 to 11.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] VanBuer, Darrel: Re: Stanford breakin, RISKS-3.62 DIGEST (E-mail; 24 September 1986, 09:35:37 PDT; http://catless.ncl.ac.uk/Risks/3.67.html) [PA] Hewlett-Packard: Getting Started as an MPE/iX Programmer Programmer's Guide (June 1992; http://docs.hp.com/cgi-bin/doc3k/B3265090421.12013/1)	[July-T, 50-51] [March-T, 142]
Encrypted File System Remote Protocol	EFS	Two Factor Authentication Using Smart Card Security technology	It facilitates two factor authentication by leveraging smart card technology.	December 1999	Remote Two Factor Authentication Using Smart Card Security Technology enhances security through enabling remote use of smart cards.	Microsoft's Innovation Report "Encrypting File System Remote", on pages 7 to 11.	The description of the claim is unclear. NON-INNOVATIVE	[PA] Blaze, Matt: Key Management in an Encrypting File System (Proceedings of the 1994 USENIX Summer Technical Conference, Boston, MA, USA; 27-35; June 1994; http://citeseer.ist.psu.edu/blaze94key.html)	[July-T, 51] [March-T, 142]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Eventlog Remote Protocol	ELOG	Consolidation of Event Log Query and Subscription Functionality	Event logs allow applications or the operating system to store information that may be of interest to administrators. The information is organized in events. These event data may be queried based upon various criteria relating to event characteristics. ELOG consolidates event log query and subscription functionality within a protocol. Event data is exposed to the user via this protocol. Queries may be issued through the protocol to filter event data so that only desired event records are returned. If a user desires to continuously apply a given filter, ELRP allows clients to set up a subscription that allows clients to receive data on events asynchronously via the ELRP, or as the event data is received, to minimize delay in being notified of the events. Using ELRP, an administrator can manage subscriptions for event monitoring and query rules with a single protocol instead of individually maintaining an arbitrarily large number of client agents.	July 2005	Consolidation of Event Log Query and Subscription Functionality into a protocol delivers adaptability through streamlined management of clients.	Microsoft's Innovation Report "Windows Eventlog remote", pages 7 to 20	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] W3C: XML Path Language (XPath), Version 1.0 (W3C Working Draft; 9 July 1999; http://www.w3.org/1999/07/WD-xpath-19990709) [PA] Cisco Systems: XML Interface to Syslog Messages (17 March 2003; http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080154000.html) [PA] Log4J project: Log4J (15 October 1999; http://logging.apache.org/log4j/docs/index.html; http://logging.apache.org/log4j/docs/HISTORY) [PA] Zhang, Qizhou: Design and Initial Implementation of Diagnostic and Error Reporting System of SMA (SMA Technical MEMO 132; 1 February 1999; http://sma-www.harvard.edu/private/memos/132.pdf)	[July-T, 52] [March-T, 36]
Eventlog Remote Protocol	ELOG	Potential Event Type Reporting	Event logs allow applications or the operating system to store information that may be of interest to administrators. Events may be queried based upon various criteria relating to event characteristics such as event type. Knowledge of possible event types that may be reported is important for writing such a query. However, without knowledge of every publisher on the system and their possible event types, it has often been difficult or impossible for a user to write an optimal query relating to events generated by that publisher or across a variety of publishers on a system. ELOG addresses these needs by reporting all possible event types that a publisher may generate. ELRP thus exposes the full power of the query infrastructure to users, who can in turn write optimized queries to get the most out of available event information.	July 2005	Potential Event Type Reporting delivers operability by allowing clients to know all possible event types that publishers can generate and to write optimized queries to get the most out of available system information.	Microsoft's Innovation Report "Windows Eventlog remote", pages 21 to 28	NON-INNOVATIVE	[PA] Graham, Steve et al: Web Services Notification (WS-Notification), Version 1.0 (1 March 2004; http://www.ibm.com/developerworks/library/specification/ws-notification/) [PA] WebMethods: WebMethods B2B Integration Server (pre 2000; http://www.webmethods.com/Products/B2B) [PA] Sun Microsystems: JavaSpaces Specification (Sun Microsystems Inc, technical report; March 1998; http://citeseer.ist.psu.edu/microsystems98javaspaces.html)	[July-T, 52] [March-T, 37]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
File Replication Service Protocol	FRS	Aging Cache	Files on the servers are often open and closed again. Some files that are opened may include changes that need to be replicated. To replicate changes, the changes need to be discovered as those changes are made. The FRS protocol provides for an aging cache called the file IDtable. Each server in a replica set stores a file IDtable for the files of the replica. When a file is opened and then closed on the local server, the local server must determine if changes have been made to the file and whether those changes need to be replicated. The replica members compute an MD5 hash of the data in the closed file, but does not include the file attributes. The local server then compares the computed MD5 hash to an MD5 hash in the file IDtable. If the hashes are the same, then the file has not been changed and need not be replicated. However, if the hashes are different, the changes may be replicated.	August 1998	Aging Cache delivers resource efficiency by minimizing the amount of data that is replicated	Microsoft's Innovation Report "File Replication Service", on pages 49 to 50.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] Heckel, Paul: A technique for isolating differences between files (Communications of the ACM 21(4); 264-268; 1978; http://doi.acm.org/10.1145/359460.359467)	[March-T, 52]
File Replication Service Protocol	FRS	Combination of Customized Replication Scheduling Technologies	The Combination of Customized Replication Scheduling Technologies in FRS.	August 1998	FRS Customized Replication Scheduling involves several technologies that work together to provide a flexible system for replicating in a multi-master replication environment. Microsoft's combination of scheduling technologies included in a multi-master replication environment is novel and non-obvious.	Microsoft's Innovation Report "File Replication Service"	The claimed innovation is the combination of different features belonging to the same protocol. Combining these individual features is an obvious step for a person skilled in the art. NON-INNOVATIVE		[July-T, 17]
File Replication Service Protocol	FRS	Combination of Customized Replication Technologies	The Combination of Customized Replication Technologies in FRS.	August 1998	FRS Customized Replication involves several technologies that work together to make the replication of data more flexible. This combination of replication technologies is novel and non-obvious in light of the prior art.	Microsoft's Innovation Report "File Replication Service"	The claimed innovation is the combination of different features belonging to the same protocol. Combining these individual features is an obvious step for a person skilled in the art. NON-INNOVATIVE		[July-T, 18-19]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
File Replication Service Protocol	FRS	Combination of FRS Technologies	The combination of all the mentioned FRS technologies, in particular: There are three components whose combination is claimed to create innovation: 1. Patented event-based multi-master replication combined with collision avoidance provides reliable master servers. 2. Customized replication scheduling optimizes timing of replication events in multi-master replication 3. Applying replication pre-processing enhances the efficiency of event based multi-master replication by avoiding unnecessary replications that are wasteful of network resources	August 1998	FRS Technologies Identified by Microsoft Operate Together in Combination to Provide a Highly Innovative Multi-Master Replication Framework that Limits Data Corruption and Optimizes Network and Processing Resources.	Microsoft's Innovation Report "File Replication Service"	The claimed innovation is the combination of different features belonging to the same protocol. Combining these individual features is an obvious step for a person skilled in the art. NON-INNOVATIVE		[July-T, 16]
File Replication Service Protocol	FRS	Combination of Multiple Pre-Processing Technologies	The combination of Multiple Pre-Processing Techniques in FRS.	August 1998	FRS pre-processing involves several techniques that work together to eliminate the replication of unnecessary changes. This combination of pre-processing technology is novel and non-obvious in light of the prior art.	Microsoft's Innovation Report "File Replication Service"	The claimed innovation is the combination of different features belonging to the same protocol. Combining these individual features is an obvious step for a person skilled in the art. NON-INNOVATIVE		[July-T, 18]
File Replication Service Protocol	FRS	Conflict Detection and Resolution	The FRS protocol provides for conflict detection and resolution in multi-master replicating of files and folders. Replicating files with multiple servers poses the potential problem that two or more users will create files with the same file name on different replica set members and the identically-named files will then collide with each other as the files are replicated to other members. The FRS protocol resolves mutually conflicting updates in multi-master file replication environments. This resolution is accomplished by comparing event times, file version numbers, file sizes, file globally unique identifiers (fileGUIDs), and/or other variables.	August 1998	Conflict Detection and Resolution (collision management) promotes reliability and data accuracy by applying certain comparison rules.	Microsoft's Innovation Report "File Replication Service", on pages 17 to 19.	NON-INNOVATIVE	[PA] Weider, Chris/Strassner, John/Huston, Bob: LDAP Multi-Master Replication Protocol (IETF draft; November 1997; http://www1.tools.ietf.org/html/draft-ietf-asid-ldap-mult-mast-rep-02.txt)	[July-T, 16] [March-T, 43]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
File Replication Service Protocol	FRS	Customized Polling	The FRS protocol replicates files according to a replication topology. To ensure that the files are properly replicated, the topology needs to be accurate. Otherwise, required replications to added members may not occur or unneeded replications will be attempted to replica members that have been deleted. Thus, topology changes must be discovered on a continuing and periodic basis. The FRS protocol provides for searching of replica topology changes by polling. The polling in the FRS protocol can occur at two times, i.e., a short interval and a long interval. The short time interval is based on the Short DS Polling Interval Timer, and the long time interval is based on the Long DS Polling Interval Timer. The interval for polling in the FRS protocol adjusts to the number of changes being made. If no changes are made to the topology during eight consecutive short polling intervals, the polling interval is automatically changed to the long interval to eliminate unnecessary polling.	August 1998	Customized Polling delivers resource efficiency by minimizing the amount of data that is replicated.	Microsoft's Innovation Report "File Replication Service", on pages 51 to 52.	NON-INNOVATIVE	[PA] RFC 1305: Network Time Protocol (Version 3). Specification, Implementation and Analysis (March 1992; http://tools.ietf.org/html/rfc1305) [PA] Popek, Gerald J. et al: LOCUS: A network transparent, high reliability distributed system (Proceedings of the Eigth Symposium on Operating Systems Principles, Pacific Grove, CA, USA; 169-177; December 1981; http://portal.acm.org/citation.cfm?id=806605)	[July-T, 20] [March-T, 53] [ECIS, 42]
File Replication Service Protocol	FRS	Customized Replication Scheduling	Data changes on files within the file system require replication. Replication requires that any server having a replica copies any changes to the replica. The changes to the data may be more routine and can be replicated according to a schedule. The replica may dictate the schedule, and each replica may require a different schedule. The FRS protocol provides for a selectable replication schedule. To execute a replication on a schedule, FRS allows for setting the times that the replication should occur.	August 1998	Customized Replication Scheduling delivers adaptability by adjusting when replications are accomplished based on the system and data needs.	Microsoft's Innovation Report "File Replication Service", on pages 59 to 60.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] Bell Telephone Laboratories: UNIX Programmer's Manual, Seventh Edition, Volume 1 (399; January 1979; http://cm.bell-labs.com/7thEdMan/v7vol1.pdf; interactive tar backup (179), cron driven tar backup (399 + 179)) [PA] IBM: OS/360 (1966; http://en.wikipedia.org/wiki/OS_360)	[March-T, 55-56]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
File Replication Service Protocol	FRS	Deterministic Compression	Replications of data can include several files with large amounts of data. As the number of replications and the number of files replicated increase, the load on the network to transfer the data increases. The FRS protocol provides for deterministic compression by determining if a server can compress the file data in the staging file and by compressing the file data before sending the staging file to a replica partner. During a join of a replica partner, the partner acknowledges whether the server can compress data. If the server can compress data, the file data in the staging file object sent between replicating partners is compressed. The staging file header includes a flag, the compression flag, to represent that the file data is compressed and an identifier, the compression GUID, for the compression algorithm used for compression. Upon receiving the staging file, the receiving server extracts the compressed data.	August 1998	Deterministic Compression delivers resource efficiency by minimizing the amount of data that is replicated	Microsoft's Innovation Report "File Replication Service", on pages 53 to 55.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] Katz, Phil: PKZIP (1989; http://en.wikipedia.org/wiki/PKZIP; (Deterministic compression))	[March-T, 54]
File Replication Service Protocol	FRS	File Staging	Before replications occur, a user may make several changes to a document. The changes may occur over an extended period of time. While changes are still being made, previous changes could be replicated. The FRS protocol provides for file staging. When changes are made on a local server, a local change order for the change is created at the local server and the local server creates a staging file. The staging file is a backup copy of the changed file that encapsulates the file's data and attributes. Upon receiving the change order, a replica partner can request the staging file that includes the change. The replica partners request the staging file for replicating the changes. This staging file is sent, and the change(s) is (are) replicated, regardless of whether something is being done to the original file that would prevent access to the changes, such as additional editing. Partners can replicate the changes without waiting to access the original file by replicating the staging file. In addition, the staging file may be compressed without interrupting further editing on the original file.	August 1998	File Staging delivers resource efficiency by minimizing the amount of data that is replicated.	Microsoft's Innovation Report "File Replication Service", on pages 46 to 49.	INNOVATIVE		[July-T, 20] [March-T, 51]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
File Replication Service Protocol	FRS	MoveIn and MoveOut Flags	The FRS protocol provides systems and methods for replicating files or data in a distributed file database. When a change to a group of files is made, such as a move of an entire folder directory, all changes to the files need to replicate. The file changes are communicated between servers in one or more change orders. If each file change in a large folder move uses a separate change order, numerous change orders are generated. Microsoft's MoveIn or MoveOut flag eliminates or, at least, reduces the number of change orders created and transmitted during a large folder move. The flags are set on a single change order to represent a change to a set of files, such that a single similar change to the files can be replicated to all files without a change order for each file.	August 1998	MoveIn and MoveOut Flags deliver resource efficiency by minimizing the number of change orders that are needed to replicate large file moves.	Microsoft's Innovation Report "File Replication Service", on pages 62 to 63.	The description of the claim is unclear. NON-INNOVATIVE	[PA] Guy, Richard G.: Ficus: A Very Large Scale Reliable Distributed File System (PhD thesis, University of California, Los Angeles (UCLA technical report CSD-910018); June 1991; http://citeseer.ist.psu.edu/guy91ficu.html)	[July-T, 21] [March-T, 57] [ECIS, 42]
File Replication Service Protocol	FRS	SYSVOL Replication with the Active Directory Topology	The enterprise system volume (SYSVOL) contains a domain's public files. As such, SYSVOL is intimately connected to the configuration of the domain and likewise the domain's topology. The FRS protocol provides an innovative method for using the domain topology created in Active Directory to replicate SYSVOL files among domain controllers. Thus, the replication of the SYSVOL files uses a specific topology, namely the Active Directory topology.	August 1998	Use of SYSVOL Replication with the Active Directory Topology promotes adaptability.	Microsoft's Innovation Report "File Replication Service", on pages 30 to 31.	NON-INNOVATIVE	[PA] Carter, Robert L./Crovella, Mark E.: Server Selection using Dynamic Path Characterization in Wide-Area Networks (Proceedings of the IEEE Infocom '97; 1014-1021; November 1990; http://citeseer.ist.psu.edu/carter96server.html) [R] Popek, Gerald J.: Replication in Ficus Distributed File Systems (IEEE Computer Society Technical Committee on Operating Systems and Application Environments Newsletter 4(3); 24-29; November 1990; http://citeseer.ist.psu.edu/popek90replication.html) [R] Heidemann, J.S. et al: Primarily Disconnected Operation: Experiences with Ficus (The 2nd International Workshop on Management of Replicated Data; November 1992; http://citeseer.ist.psu.edu/heidemann92primarily.html)	[July-T, 17-18] [March-T, 46]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
File Replication Service Protocol	FRS	Use of DFS Replication by Custom Topology	The FRS protocol provides for the use of a topology tailored to the Directory File System (DFS) to replicate distributed file system data. The DFS contains files used by users on the system. DFS replication uses a topology tailored to DFS. DFS is different from SYSVOL and may not be able to, or should not, employ the Active Directory topology. The FRS protocol provides an innovative method for using a customized topology for FRS that is created and is different from the topology used for SYSVOL.	August 1998	Use of DFS Replication by Custom Topology promotes adaptability.	Microsoft's Innovation Report "File Replication Service", on pages 32 to 34.	NON-INNOVATIVE	[PA] Carter, Robert L./Crovella, Mark E.: Server Selection using Dynamic Path Characterization in Wide-Area Networks (Proceedings of the IEEE Infocom '97; 1014-1021; November 1990; http://citeseer.ist.psu.edu/carter96server.html) [R] Popek, Gerald J.: Replication in Ficus Distributed File Systems (IEEE Computer Society Technical Committee on Operating Systems and Application Environments Newsletter 4(3); 24-29; November 1990; http://citeseer.ist.psu.edu/popek90replication.html) [R] Heidemann, J.S. et al: Primarily Disconnected Operation: Experiences with Ficus (The 2nd International Workshop on Management of Replicated Data; November 1992; http://citeseer.ist.psu.edu/heidemann92primarily.html)	[July-T, 18] [March-T, 47]
File Replication Service Protocol	FRS	Use of GUIDs	Files may be identified by file-name-independent globally unique identifiers. Similarly, directories may be identified by directory-name-independent GUIDs. Prior methods of using filenames or directory names created potential problems in replicating files or directories because, among other problems, changes in a file's full pathname would typically require special handling in replicating given that it was the file or directory itself which had changed and a host of identification problems could result. Further, replicating a change in file or directory name would typically require replicating the file's or directory's contents as well. Microsoft's FRS protocol addresses these shortcomings by identifying files by filename-independent GUIDs (file GUIDs). With file GUIDs, file name changes and file content changes can be tracked independently of each other. Further, with file GUIDs, FRS can replicate a change in file name only without replicating the file's contents, and changes in a file's full pathname do not necessitate special handling.	August 1998	Use of GUIDs promotes resource efficiency and data accuracy by enabling the accurate tracking of a file or folder among multiple servers.	Microsoft's Innovation Report "File Replication Service", on pages 20 to 21.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] U.S. Patent 5,052,040: Multiple user stored data cryptographic labeling system and method (Micronyx, Inc.; 24 September 1991 (Filed 25 May 1990 as 07/529,107); The patent describes among other things cryptographically labelling a data file.) [PA] Tanenbaum, Andrew S.: Distributed Operating Systems (Prentice Hall, Upper Saddle River, NJ, USA; 1995)	[July-T, 16] [March-T, 44]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
File Replication Service Protocol	FRS	Using the Version Sequence Number (VSN) to Indicate File Version	The FRS protocol provides systems and methods for replicating files or data in a distributed file database. When a change to a file is made, the file change must be replicated to other copies of the file that may be stored in other computers. The file changes are communicated between servers in one or more replication cycles. Before file changes are replicated, FRS pre-processes the files to determine changes that need to replicate. The pre-processing involves several innovative technologies that eliminate the replication of unnecessary changes. Microsoft's replication pre-processing innovation eliminates or, at least, reduces transmission between servers that occur before or during replication.	August 1998	Using the VSN to Indicate File Version delivers resource efficiency by minimizing the amount of data that is replicated.	Microsoft's Innovation Report "File Replication Service", on pages 36 to 42.	NON-INNOVATIVE	[PA] Terry, D. B. et al: Session Guarantees for Weakly Consistent Replicated Data (Proceedings of the IEEE Conference on Parallel and Distributed Information Systems (PDIS); 140-149; September 1994) [PA] Kumar, Puneet: Mitigating the Effects of Optimistic Replication in a Distributed File System (PhD thesis, Carnegie Mellon University; December 1994; http://citeseer.ist.psu.edu/kumar94mitigating.html)	[July-T, 18-19] [March-T, 48] [ECIS, 41]
File Replication Service Protocol	FRS	Version Vector Join	The servers, or members, which replicate certain data, may change. Servers may be added to replicas such that those new members replicate changes to the replica. The FRS protocol provides for the joining of new members. When joining a replica, the new member must replicate changed data in the replica. With Version Vector Join the FRS protocol determines which changes a replica member will need to make upon becoming a partner with other replica members. The new member of the replica set establishes a version vector object, which includes a globally unique identifier and version sequence number of each member of the replica set. The version vector object is sent to the upstream partner in the replica set. Upon examining the version vector object, the upstream partner can determine which changes to send to the new downstream partner. The upstream partner sends one or more change orders to the downstream partner. The newly joined member need only replicate files from the upstream partner, which reduces the amount of information communicated amongst members of the replica set.	August 1998	Version Vector Join delivers resource efficiency by minimizing the amount of data that is replicated.	Microsoft's Innovation Report "File Replication Service", on pages 42 to 43.	NON-INNOVATIVE	[PA] Petersen, Karin et al: Bayou: Replicated Database Services for World-wide Applications (Proceedings of the 7th SIGOPS European Workshop, Connemara, Ireland; 275-280; September 1996; http://citeseer.ist.psu.edu/petersen96bayou.html) [PA] Saito, Yasushi: Unilateral Version Vector Pruning Using Loosely Synchronized Clocks (Hewlett-Packard Labs, Storage Systems Department, technical report; 5 March 2002; http://citeseer.ist.psu.edu/541468.html) [PA] Satyanarayanan, Mahadev: Coda: A Higly Available File System for a Distributed Workstation Environment (IEEE Transactions on Computers, 39(4); 447-459; 1990; http://citeseer.ist.psu.edu/satyanarayanan90coda.html)	[July-T, 19] [March-T, 49] [ECIS, 41]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
File Replication Service Protocol	FRS	Version Vector Rejoin	The FRS protocol provides for a version vector rejoin, in which FRS establishes what changes a replica member that stopped running FRS will need to make upon rejoining the replica set. The rejoining member of the replica sends its last updated vector object, which includes a globally unique identifier and version sequence number for each previously established member of the replica set, to its previously established upstream partner. Upon examining the version vector object, the upstream partner can determine which changes to send to the rejoining partner. The changes are sent as change orders. The rejoining member receives and inspects the change orders to determine which changes to apply based on local changes. The rejoining member need only replicate files from the upstream partner and not every partner in the replica set, which reduces the amount of information communicated amongst members of the replica set. After this rejoin, the version vector is maintained to determine which changes have been made.	August 1998	Version Vector Rejoin delivers resource efficiency by minimizing the amount of data that is replicated.	Microsoft's Innovation Report "File Replication Service", on pages 44 to 45.	NON-INNOVATIVE	[PA] Petersen, Karin et al: Bayou: Replicated Database Services for World-wide Applications (Proceedings of the 7th SIGOPS European Workshop, Connemara, Ireland; 275-280; September 1996; http://citeseer.ist.psu.edu/petersen96bayou.html)	[July-T, 19] [March-T, 50]
Health Certificate Enrollment Protocol	HCEP	Evaluation of a Client's Health Against Multiple Networks' Health Policies	The server determines the network(s) for which the client's state of health complies and issues a health certificate permitting access to each. The client can then use its health certificate to access the network access server(s) for which its health has been determined compliant. This creates the ability for one health registration authority to validate a client's health against several networks' health policies.	July 2005	The ability of a client to send its statement of health to a server capable of Evaluating the Client's Health Against Multiple Networks' Health Policies promotes extensibility and efficiency.	Microsoft's Innovation Report: "Health Certificate Enrollment Protocol", pages 11 to 16.	NON-INNOVATIVE	[PA] Trusted Computing Group (TCG): TCG Trusted Network Connect TNC Architecture for Interoperability, Specification Version 1.0, Revision 4 (3 May 2005 (Revision 1 was dated 11 February 2005); https://www.trustedcomputinggroup.org/groups/network/TNC_Architecture_v1_0_r4.pdf)	[July-T, 53] [March-T, 137]
Health Certificate Enrollment Protocol	HCEP	Out-of-Band Health Certification	HCEP enables a client to obtain its own reusable health certificate from an out-of-band server that verifies that the client's health complies with a particular network's health policy. Prior to contacting the network that the client seeks to access, the client sends a request for a health certificate, along with its statement of health, to an out-of-band server. The out-of-band server compares the client's statement of health against a health policy. If the client complies with the health policy, the out-of-band server sends a response, including a health certificate, indicating the client's compliance. The client may then use the certificate to access the network through any network access server - avoiding the need for independent health evaluations at each server.	July 2005	Out-of-Band Health Certification promotes processing efficiency by enabling a client to obtain it sown reusable health certificate from an out-of-band server.	Microsoft's Innovation Report: "Health Certificate Enrollment Protocol", pages 6 to 10	NON-INNOVATIVE	[PA] Trusted Computing Group (TCG): TCG Trusted Network Connect TNC Architecture for Interoperability, Specification Version 1.0, Revision 4 (3 May 2005 (Revision 1 was dated 11 February 2005); https://www.trustedcomputinggroup.org/groups/network/TNC_Architecture_v1_0_r4.pdf)	[July-T, 53] [March-T, 136]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Health Certificate Enrollment Protocol	HCEP	SoHR Messages Identifying and Categorizing Health-Related Policy Failures	A server uses HCEP to manage the health of its networked resources. A network administrator is able to implement health policies that require client(s) to satisfy certain threshold health requirements prior to gaining full access, such as activation of firewall(s), antivirus software, and/or anti-spy software. Prior to the SoHR protocol, servers gathered health information about their clients through connection management and running local scripts. These systems resulted in a client being deemed either compliant or non-compliant, with no details regarding a non-compliant client's failures. This prevented networks from permitting limited access to those clients with only minor health failures.	July 2005	The technology SoHR Messages Identifying and Categorizing Health-Related Policy Failures promotes network accessibility by providing information that may permit network access to clients that are not fully compliant with health policies.	Microsoft's Innovation Report: "Network Access Protection Statement of Health Protocol", on pages 6 to 12.	NON-INNOVATIVE	[PA] Trusted Computing Group (TCG): TCG Trusted Network Connect TNC Architecture for Interoperability, Specification Version 1.0, Revision 4 (3 May 2005 (Revision 1 was dated 11 February 2005); https://www.trustedcomputinggroup.org/groups/network/TNC_Architecture_v1_0_r4.pdf)	[July-T, 54] [March-T, 138]
Health Certificate Enrollment Protocol	HCEP	SoHR Messages Providing Remediation Guidance	HCEP uses SoHR messages to promote client support through directed client remediation. After receiving the client's SoHR message and determining the client is noncompliant according to network policies, HCEP provides a means for the health server to not only inform the client of its failure, but also include direction as to how to remediate the failure. This enables non-compliant clients to quickly become aware of their precise failures and gain knowledge regarding how to fix them.	July 2005	SoHR Messages Providing Remediation Guidance promotes clients reliability and compliance with health policies through informing the client how to remedy failures to meet health policies.	Microsoft's Innovation Report: "Network Access Protection Statement of Health Protocol", on pages 12 to 16.	NON-INNOVATIVE	[PA] Trusted Computing Group (TCG): TCG Trusted Network Connect TNC Architecture for Interoperability, Specification Version 1.0, Revision 4 (3 May 2005 (Revision 1 was dated 11 February 2005); https://www.trustedcomputinggroup.org/groups/network/TNC_Architecture_v1_0_r4.pdf)	[July-T, 55] [March-T, 139]
ICertPassage Remote Protocol	ICERTP	Certificate Revocation List Publishing	The CRL publishing handler provides the ability of the ICertAdminD protocol to create and publish new certificate revocation lists. The certificate revocation list is a list of certificate serial numbers which have been revoked and are no longer valid. One part of the certificate authority process determines the public key certificate revocation information. The CRL publishing handler enables the creation and publishing of new certificate revocation lists. This innovation first shipped with ICertAdminD2 in Windows XP Professional.	December 1999	Certificate Revocation List (CRL) Publishing promotes usability by providing control of the CRL.	Microsoft's innovation report: "certificate services remote administration", pages 15 to 16.	NON-INNOVATIVE	[R] RFC 3280: Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile (April 2002; http://tools.ietf.org/html/rfc3280) [R] RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile (January 1999; http://tools.ietf.org/html/rfc2459) [PA] Netscape: ICRLPublisher::publish method (http://www.redhat.com/docs/manuals/cert-system/sdk/7.1/javadocs/framework/public/com/netscape/certsrv/publish/ICRLPublisher.html)	[July-T, 57-58] [March-T, 86]
ICertPassage Remote Protocol	ICERTP	Combination of ICERTP Technologies	The Combination of all the mentioned ICERTP Technologies.	December 1999	The Combination of all the ICERTP Technologies provides yet another level of innovation beyond any of these innovations standing alone.	Microsoft's innovation report: "certificate services remote administration"	The claimed innovation is the combination of different features belonging to the same protocol. Combining these individual features is an obvious step for a person skilled in the art. NON-INNOVATIVE		[July-T, 58]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
ICertPassage Remote Protocol	ICERTP	Importing and Converting Certificates	The import and convert handlers in the ICertAdminD protocol assist in transitions from older, perhaps obsolete certificate authorities to a new certificate authority. The innovation prevents burdening customers of the certificate authority when transitioning from an old to a new certificate authority. This is accomplished by transferring all the old certificates to the new certificate authority so that new certificates do not have to be issued for each customer or end user.	December 1999	Importing and Converting Certificates Into a Certificate Authority promotes efficiency for the end user by allowing old certificates to be transferred into a new certificate authority.	Microsoft's innovation report: "certificate services remote administration", pages 7 to 9.	NON-INNOVATIVE	[R] Sun Microsystems: keytool - Key and Certificate Management Tool (2001; http://web.archive.org/web/20030202134922/java.sun.com/products/jdk/1.2/docs/tooldocs/win32/keytool.html) [PA] Oaks, Scott: Java Security (O'Reilly; May 1998; Sun Java Keytool)	[July-T, 56] [March-T, 83]
ICertPassage Remote Protocol	ICERTP	Interface-Based Row Deletion in a Certificate Authority Database	An interface utilizing the ICertAdminD protocol provides a system administrator with the ability to delete obsolete rows without requiring specialized knowledge regarding the database structure or corresponding query language. The row deletion feature is an additional function used to remove expired certificates, or pending or failed requests from the database.	December 1999	Interface-Based Row Deletion promotes usability in the interface by not requiring knowledge of the database query language.	Microsoft's innovation report: "certificate services remote administration", pages 14 to 15.	NON-INNOVATIVE	[PA] Digital Equipment Corporation: RSX-11M/M-PLUS RMS-11 User's Guide (section 7.2.2; This reference relates to version 4.2 of RSX-11 from 1983.; http://www.computer.museum.uq.edu.au/RSX/AA-L669A-TC%20RSX-11M%20&%20M-PLUS%20RMS-11%20User's%20Guide.pdf)	[July-T, 57] [March-T, 85]
ICertPassage Remote Protocol	ICERTP	Key Archival and Recovery	A Key Recovery Agent (KRA) is a registration authority that can obtain a Key Recovery Certificate (or Key Archival Certificate) for the purposes of key archival, escrow or recovery.	December 1999	Key Archival and Recovery promotes reliability and security by creating an archive of keys in preparation for a system failure.	Microsoft's innovation report: "certificate services remote administration", pages 9 to 11.	NON-INNOVATIVE	[PA] RedHat: Netscape Certificate Management System (Chapter 3: Handling Certificate Requests; http://www.redhat.com/docs/manuals/cert-system/agent/request.htm) [PA] RFC 2527: Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework (March 1999; http://www.ietf.org/rfc/rfc2527.txt) [PA] Oaks, Scott: Java Security (O'Reilly; May 1998; Sun Java Keytool)	[July-T, 56] [March-T, 84]
ICertPassage Remote Protocol	ICERTP	Officer Designation	The officer designation innovation of the ICertAdminD protocol fulfills government requirements for certificate authorities. The officer designation is a list of administrator defined rights or access control lists (ACLs). ACLs define the capability of a given principal to configure or administer a certificate authority. Thus, officer designation promotes efficiency (compliance) by fulfilling U.S. Government requirements, and also provides an increased level of granularity in security by offering four distinctive roles in the security model: administrator, operator, officer, and auditor.	December 1999	Officer Designation promotes security by offering four distinctive roles in the security model.	Microsoft's innovation report: "certificate services remote administration", pages 12 to 13.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE		[July-T, 57] [March-T, 84]
Internet Protocol Security Protocol Extensions	IPSEC	Authentication Using CGA		July 2005		Microsoft's Innovation Report: "Internet Key Exchange Protocol Extensions", page 12.	NON-INNOVATIVE	[PA] Laganier, J./Montenegro, G.: Using IKE with IPv6 Cryptographically Generated Address (24 February 2003; http://tools.ietf.org/html/draft-laganier-ike-ipv6-cga-00)	[July-T, 59] [March-T, 145]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Internet Protocol Security Protocol Extensions	IPSEC	Combination of IPSEC Technologies	The combination of all the mentioned IPSEC technologies.	July 2005	The combination of innovations in AuthIP together provides a substantial advance in the security, efficiency, reliability and usability of IP Security.	Microsoft's Innovation Report: "Internet Key Exchange Protocol Extensions"	The claimed innovation is the combination of different features belonging to the same protocol. Combining these individual features is an obvious step for a person skilled in the art. NON-INNOVATIVE		[July-T, 8]
Internet Protocol Security Protocol Extensions	IPSEC	Efficient Denial of Service Attack Resistance	Responding to request for authentication is the responsibility of a responder. However, if the responder receives more requests than it can process it may deny legitimate requests for authentication or crash. AuthIP, as well as IKE and other protocols use Denial of Service (DoS) cookies to verify the identity of an initiator; however, this may not be sufficient. Prior art, such as IKE, still process a Diffie-Hellman exchange prior to determining whether a message should be discarded. As a result, a great deal of processing time may be expended to determine if there is an DoS attack designed to cause the responder to spend processor and other resources.	November 2006	Efficient Denial of Service Attack Resistance delivers processor efficiency through postponement of Diffie-Hellman calculations.	Microsoft's Innovation Report: "Authenticated IP", pages 12 to 13.	INNOVATIVE		[March-T, 152]
Internet Protocol Security Protocol Extensions	IPSEC	Fallback Authentication	While some protocols require a complete restart upon a failed authentication, even if the failure is due to an incompatible authentication method, AuthIP allows authentication to continue. As a result, authentication is more likely to be successful and authentication restarts less likely. Traffic and messaging resources are not wasted retrying single authentication messages with only one chance of being accepted by the responder. An exchange that fails due to incompatible authentication methods wastes time and resources if the initiator is only able to guess at a new authentication method and try the exchange again. With AuthIP initiators that can authenticate with a variety of authentication methods can suggest those methods up front. Responders then select an acceptable method and continue the exchange.	November 2006	Fallback Authentication delivers connection efficiency through suggestion of alternate authentication methods.	Microsoft's Innovation Report: "Authenticated IP", pages 13 to 14.	NON-INNOVATIVE		[July-T, 7] [March-T, 153]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Internet Protocol Security Protocol Extensions	IPSEC	Initiator-Indifferent User Authentication	IKE provides for machine authentication, but not user authentication. Some methods have been developed to incorporate user authentication into IKE using other known protocols such as Kerberos. However, these methods require that a new IKE main mode be conduced in conjunction with each user authentication. Compatibility issues also exist when some protocols are combined with IKE. For example, when the initiator sends a request to the responder in clear text, meaning not according to a security protocol, and the responder requires secure communication, the responder initiates an IKE negotiation. When this occurs, the responder effectively becomes the initiator and the initiator effectively becomes the responder thereby subverting the roles of the initiator and the responder. Protocols, such as Kerberos, are sensitive to the direction of the negotiation and can fail when the roles of initiator and responder are subverted.	November 2006	Initiator-Indifferent User Authentication delivers connection efficiency through authentication connection preservation.	Microsoft's Innovation Report: "Authenticated IP", pages 10 to 12.	The claimed innovation is not described in the Technical Documentation. NON-INNOVATIVE		[July-T, 6] [March-T, 152]
Internet Protocol Security Protocol Extensions	IPSEC	Negotiation Discovery	In a complex network environment, computers with different security capabilities may be present and need to communicate with each other. In order to ensure security, the security capability of the computers attempting to communicate with one another must be determined. If either computer lacks sufficient security capability, the computers communicate in clear text. Otherwise, secure communication can be established between them. With alternative prior art technology, determination of security capability is carried out before communication takes place, either in clear text or by a secure link. Such sequential steps slow negotiations, adversely affecting performance of the network. With negotiation discovery, whether a remote computer is IPsec-capable can be determined at the same time communication is carried out between the remote computer and the host. The host communicates in clear text and starts an IKE negotiation with a remote computer simultaneously. If the remote computer is determined to be IPsec-capable, the computers switch to secured communication; if not, the communication stays in clear text.	July 2005	Negotiation Discovery promotes efficiency and flexibility by simultaneously conducting clear text and IKE negotiations.	Microsoft's Innovation Report: "Internet Key Exchange Protocol Extensions", page 12.	NON-INNOVATIVE		[July-T, 60] [March-T, 145]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Internet Protocol Security Protocol Extensions	IPSEC	One-Way Authentication Enforcement	Not all parties need to have mutual authentication. If a first computer trusts a second computer then the trust relationship is controlled by the first computer. Once a secure connection is established the parties may converse on a secure channel established with oneway authentication. The secure channel is initially established by the trusting party which establishes the one-way security association. If the keys used in that security association fail, only the trusting party can cause a re-keying. AuthIP innovation in one-way authentication enforcement delivers security by preserving the re-keying role of the trusting party. The trusted party cannot re-key the security associations and usurp the role of the trusting part.	November 2006	One-Way Authentication Enforcement delivers security through preserving the re-keying rights.	Microsoft's Innovation Report: "Authenticated IP", pages 14 to 15.	NON-INNOVATIVE	[PA] RFC 4478: Repeated Authentication in Internet Key Exchange (IKEv2) Protocol (April 2006 (first draft 13 May 2004); http://tools.ietf.org/html/rfc4478)	[July-T, 7-8] [March-T, 153-154]
Internet Protocol Security Protocol Extensions	IPSEC	Secure Communication Channel Negotiation	Two machines, an initiator and responder, use AuthIP to authenticate machines and establish a secure channel. The secure channel can then be available for the secure exchange of data or for the authentication of one or more users on either or both machines. The exchange begins when the initiator sends a message to initiate a secure mode with the responder. The responder and initiator then engage in an exchange of messages to authenticate at least one of the machines.The first and second phases of the exchange of messages between the initiator and responder are the main mode and the quick mode. The main mode is used to perform oneway or mutual machine authentication and to provide a secure channel for conducting the quick mode and optional user mode. The quick mode is used to derive and refresh keys used with Internet Protocol Security protocols such as the encapsulating security protocol and the authentication header protocol. In the prior protocols the main mode ran to completion before the quick mode started. AuthIP improves the exchange by providing for the overlap of the main mode and quick mode.	November 2006	Negotiating a secure communication channel delivers connection efficiency through overlapping main mode and quick mode portions of a channel negotiation.	Microsoft's Innovation Report: "Authenticated IP", pages 7 to 10.	INNOVATIVE		[March-T, 151]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
IPv4 over IEEE 1394 Protocol Extensions	IPV4	Encapsulation of STP Packets in IPo1394 Extensions	To ensure reliable operation of a bridged network environment, bridges, under the IEEE802.1D standard, detect and prevent loops. Loops can impair reliability and efficiency by causing packets of data to be sent and received by the same device, unnecessarily increasing network traffic, wasting resources, and increasing the risk of erroneous processing of such data. Bridges employ the Spanning Tree algorithm and Protocol (STP) to diagnostically detect looping, so that the bridge can make adjustments to prevent it during the regular forwarding of packets. Part of the STP algorithm requires the bridge to send out STP frames for propagation through the network nodes attached to the bridge ports. However, standard IPo1394 does not support recognizing and forwarding STP frames - rendering the bridge incapable of using STP to ensure that loopback conditions do not exist. Prior to development of Microsoft's innovation, no solution existed for detecting loops in a bridged environment linking an IEEE 1394 bus to other networks that support STP, such as Ethernet networks.	June 2000	Encapsulating STP Packets in Standard IPo1394 Packets promotes interoperability by allowing IPo1394 networks to support the spanning tree algorithm used in bridges that connect networks.	Microsoft's Innovation Report: "IPv4 over IEEE 1394 (IPo1394) Extensions", on pages 6 to 9.	NON-INNOVATIVE	[R] Perlman, Radia: Interconnections: Bridges and Routers (Addison-Wesley Publishing Company, Reading, Mass.; 54, 73; 1992) [PA] U.S. Patent 6,747,979: Method and apparatus for bridging between networks (Hewlett-Packard; 8 June 2004 (Filed 27 October 1999 as 09/427,705))	[July-T, 61-62]
Local Security Authority (Domain Policy) Remote Protocol	LSA-D	Combination of LSA-D Technologies	The Combination of all LSA-D Technologies.	July 1993	The combination of the innovations in LSA-Domain described above and its other features provide an innovative interface to Remote Procedure Call (RPC) that promotes the benefits of granularity of control, scalability, and efficiency.	Microsoft's Innovation Report: "Local Security Authority (Domain Policy) Remote"	The claimed innovation is the combination of different features belonging to the same protocol. Combining these individual features is an obvious step for a person skilled in the art. NON-INNOVATIVE		[July-T, 66]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Local Security Authority (Domain Policy) Remote Protocol	LSA-D	Policy Management Across Security Boundaries via LSA-Domain	LSA-Domain allows security policy to be managed between machines in a single domain, then between different domains that shared the same schema ("forests"), and then further across forests that did not share the same schema ("cross-forest trusts"). More specifically, LSA-Domain can be used by administrators to set policy across these security boundaries, including cross-forest trusts and enabling cross-realm authentication. The security boundaries are defined by objects in the LSA-Domain data model. LSA-Domain objects are the foundation structure that enable dynamic capabilities of the LSA-Domain security architecture. The trusted object methods are described below. The use of trusted domain objects increases scalability of the security architecture as the administrative boundary grows because a network administrator can associate multiple security boundaries with a single user. This ability makes the maintenance of a security architecture easier because there is no duplication of accounts.	March 2003	LSA-Domain provides scalability through the management of Policy Management Across Security Boundaries via LSA-Domain.	Microsoft's Innovation Report: "Local Security Authority (Domain Policy) Remote", on pages 11 to 17.	NON-INNOVATIVE	[PA] Reiter, Michael K./Stubblebine, Stuart G.: Path Independence for Authentication in Large-Scale Systems (AT&T Technical Report TR.96.8.1; 21 August 1996; http://citeseer.ist.psu.edu/reiter96path.html) [PA] Pato, Joseph N.: Hierarchical Trust Relationships for Inter-Cell Authentication (OSF DCE SIG Request for Comments 7.0; July 1992; http://www.opengroup.org/tech/rfc/mirror-rfc/rfc7.0.ps) [PA] U.S. Patent 5,544,322: System and method for policy-based inter-realm authentication within a distributed processing system (IBM; 6 August 1996 (Filed 9 May 1994 as 08/239,669))	[July-T, 65] [March-T, 135]
Local Security Authority (Domain Policy) Remote Protocol	LSA-D	Security Management Applications Accessing a Security Model Via LSA-Domain to LSA	LSA-Domain comprises methods of communication, policy setting, and account creation. LSA-Domain uses a message syntax to create a uniform method of communication. In order to create a uniform and secure method of gaining access to policies, LSA-Domain grants an open handle to the Policy Object, provided the caller is able to authenticate successfully. The LSA-Domain protocol provides a uniform method of account creation.	July 1993	Security Management Applications Accessing a Security Model Via LSA-Domain to LSA provides the benefit of improved efficiency due to decreased application development cost, faster development times, and stronger security.	Microsoft's Innovation Report: "Local Security Authority (Domain Policy) Remote", on pages 18 to 24.	NON-INNOVATIVE	[PA] Satyanarayanan, Mahadev: Integrating Security in a Large Distributed System (ACM Transactions on Computer Systems 7(3); 247-280; August 1989; http://portal.acm.org/citation.cfm?id=65002)	[July-T, 66] [March-T, 135]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Local Security Authority (Domain Policy) Remote Protocol	LSA-D	Setting Security Policy on a "Per-Object-Per-Security-Principal" Basis	Microsoft's LSA-Domain sets policies on a per-object-per-security-principal basis. Queries may be made to retrieve and adjust the security policies that are in effect on the target computer and map privileges to Security Principals. The queries can only be made after proper authentication, thus protecting the security policy data store.	July 1993	Setting Security Policy on a "Per-Object-Per-Security-Principal" Basis Via LSA-Domain delivers the benefit of granularity of control.	Microsoft's Innovation Report: "Local Security Authority (Domain Policy) Remote", on pages 7 to 11.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] IBM: Resource Access Control Facility (RACF) (http://www-03.ibm.com/servers/eserver/zseries/zos/racf/) [PA] Hewlett-Packard: Accessing Files Programmers Guide (Manufacturing Part Number: 32650-90885; March 2000; This manual is about the HP 3000 machine which went through several development stages between 1971 and today.) [R] U.S. Department of Defense: Trusted Computer System Evaluation Criteria (15 August 1983; http://www-cse.ucsd.edu/~bsy/sec/CSC-STD-001-83.txt; The fact that the the U.S. Department of Defense could specify what it considered to be "...a uniform set of basic requirements..." shows the extent to which the requirements were not considered novel or innovative in 1983.)	[July-T, 64] [March-T, 134-135]
Local Security Authority Translation Protocol	LSA-T	Capturing SID History	LSA-Translation implements a capturing SID history functionality via the sidHistory attribute. The sidHistory attribute provides the basis for privileges and policies being discovered automatically. This is accomplished by capturing SIDs for security principals in the sidHistory attribute.	July 1993	Capturing SID History delivers efficiency through time, accuracy and resource savings by automatically creating new SIDs from captured SID history.	Microsoft's Innovation Report: "Local Security Authority Translation Protocol", on pages 6 to 9.	The description of the claim is unclear. The claimed innovation is not described in the Technical Documentation. NON-INNOVATIVE		[July-T, 67] [March-T, 133]
Microsoft Distributed File System (Server to Server)	MS-DFSS	Referral Management	The distributed file system provides a superstructure for "tying" together portions of the distributed system having heterogeneous file systems and heterogeneous network operating systems. It provides name resolution services to the file systems and the network operating system, but the distributed file system is transparent to the file systems and the network operating system. Maintaining security among such a variety of systems can be problematic. There is a need to support heterogeneous systems without problematic security issues. MS-DFSS addresses this need by allowing security policy independence among the domains. The distributed file system partitions the distributed system into administrative domains which may each implement separate administrative and security policies. Each domain is self-contained such that it may operate independently of other domains. The distributed system runs a network operating system in a first domain that implements a security policy. The domain implements a security policy that differs from the first security policy and is independent of the distributed file system.	April 2006	Referral Management promotes processing efficiency, adaptability, fault tolerance and accuracy by facilitating optimal referral deployment and file accessibility.	Microsoft's Innovation Report: "Microsoft Distributed File System Server-to-Server", on pages 35 to 41.	NON-INNOVATIVE	[PA] Cluster File Systems, Inc.: Lustre file system (http://www.lustre.org; Production versions since 2003.) [PA] Pai, Vivek S. et al: Locality-Aware Request Distribution in Cluster-based Network Servers (Proceedings of the 8th ACM Conference on Architectural Support for Programming Languages and Operating Systems, San Jose, CA, USA; 205-216; October 1998)	[July-T, 23] [March-T, 148]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Microsoft Distributed File System (Server to Server)	MS-DFSS	Target Sorting	A referral response typically includes a list of targets corresponding to servers and/or shares having the requested file. In some cases, the referral response may have the targets identified listed in a random order or by site-cost. A problem with this randomness is the fact that the first available target may be located on the other side of the world. Thus, the cost of communicating with this first-available target may be relatively high. In some cases, all future referrals and requests are also routed to that target for continuity unless the user of the client computer specifically requests a new referral. Referral management involves organizing and sorting targets received in a referral response to promote efficient deployment and accessibility. Furthermore, referral management may include an indication of bounded sets each including a grouping of targets. An indication of the beginning of a bounded set is made by providing a demarcation value associated with, for instance, a timeout setting associated with the first target after which a new referral must be requested.	April 2006	Target Sorting delivers efficiency, adaptability and reliability through optimal target organization and load sharing.	Microsoft's Innovation Report: "Microsoft Distributed File System Server-to-Server", on pages 41 to 42.	NON-INNOVATIVE	[PA] Cluster File Systems, Inc.: Lustre file system (http://www.lustre.org; Production versions since 2003.) [PA] Carter, Robert L./Crovella, Mark E.: Server Selection using Dynamic Path Characterization in Wide-Area Networks (Proceedings of the IEEE Infocom '97; 1014-1021; November 1990; http://citeseer.ist.psu.edu/carter96server.html)	[July-T, 23] [March-T, 148]
Microsoft Protected Extensible Authentication Protocol Extensions	MS-PEAP	Assessing the State of Health of a Client Computer Device	Factors such as the version of anti-virus protection, the state of operating system security level updates and the level of firewall software are important factors to be learned in making this determination. MS-PEAP facilitates this exchange of information between the server and client. A given TLV may be used to signal that an information packet carries a statement of health payload. For example, a specific TLV type can be assigned to each desired health parameter. The client returns the value of the health parameter in the TLV value field. For example, one TLV type can be assigned for the version of anti-virus program. Another can be assigned for the level of operating system security updates. A third type can be assigned for the version of firewall software.	August 2002	The protocol delivers adaptability in accessing the state of health of a client computing device.	Microsoft's innovation report: "Microsoft Protected Extensible Authentication Protocol version 0", on pages 6 to 14	NON-INNOVATIVE		[July-T, 79-80] [March-T, 118]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Microsoft Protected Extensible Authentication Protocol Extensions	MS-PEAP	TLS Tunnneling and TLV Identification	MS-PEAP provides a secure channel for the authentication of users and computer devices on a computer network.It provides a two-part conversation where the server authenticates to the client and the client authenticates to the server. In the first part, the Transport Layer Security protocol is used to establish a secure communication tunnel. In the second part, a protocol such as the Extensible Authentication Protocol (EAP) can be used to negotiate a specific protocol for authenticating the user to allow access to the network. MS-PEAP extends the capability of the EAP exchange by, in part, providing a name/value pair or TLV (representing type, length and value) portion within each message sent during the authentication process. The TLVs contained within MS-PEAP messages provide a framework for identifying the particular data being transmitted and therefore promote adaptability and more accurate communication between the user computing device and the authentication server computing device.	August 2002	The protocol delivers security through TLS Tunneling and adaptability through TLV Identification.	Microsoft's innovation report: "Microsoft Protected Extensible Authentication Protocol version 0", on pages 15 to 18.	The description of the claim is unclear. NON-INNOVATIVE		[July-T, 79] [March-T, 118]
Messenger Service Remote Protocol	MSRS	Message Differentiation	Numerous users often concurrently use a terminal server. Each user has its own terminal that is connected to the server over a common broadcast channel. Differentiating messages among the users has been a real dilemma especially when the users have different operating systems. As a result, server messages have been multicast to each user regardless of whether the user has a need to know of each message. MSRSP's message differentiation addresses this concern by enabling messages to be differentiated despite the shared server and single broadcast channel. For example, on a terminal server computer hosting concurrent user sessions, each user might request that the server listen for messages on his or her behalf and deliver the messages to his or her console. This avoids the need for multicast messages and the inconvenience to users from receiving unnecessary messages. By ensuring that each concurrent user only receives his or her messages, the protocol promotes efficiency in allocation of computer resources and management of terminal servers and enhances productivity for concurrent users.	July 1993	Message Differentiation promotes efficiency and productivity in computer resources by differentiating server messages over a common broadcast channel.	Microsoft's innovation report: "Messenger Service Remote and Send Protocol", on pages 6 to 8.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] Tanenbaum, Andrew S.: Operating Systems: Design and Implementation (Prentice Hall, Upper Saddle River, NJ, USA; section 2.2.8; 1987; The use of message passing mechanisms was sufficiently common that Tanenbaum finds it sufficient to comment "that the list while not endless is long".)	[July-T, 71] [March-T, 62]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Security Account Manager Remote Protocol	MS-SAMR	Account Aggregation and Privilege Delegation	MS-SAMR enables administrators to access the capabilities of an object oriented security model. In particular, one security object can inherit privileges from another security object. An administrator can then assign privileges to a group associated with the security object and members automatically gain privileges simply by becoming group members. In addition, administrative privileges can be delegated to sub-level administrators as well.	July 1993	MS-SAMR delivers efficient management of Network Access through Account Aggregation and Privilege Delegation.	Microsoft's innovation report: "SAM Client to Server", on pages 7 to 11.	NON-INNOVATIVE	[PA] Satyanarayanan, Mahadev: Integrating Security in a Large Distributed System (ACM Transactions on Computer Systems 7(3); 247-280; August 1989; http://portal.acm.org/citation.cfm?id=65002)	[July-T, 68] [March-T, 96]
Security Account Manager Remote Protocol	MS-SAMR	Automatic Account Resets	It is known to use a security feature whereby a user is locked out from their account after a number of failed login attempts. While this may prevent some malicious actors from accessing an account, it also enables a malicious actor to intentionally enter wrong passwords to cause the account to be locked and thereby deny access to a legitimate user. MS-SAMR provides an innovative solution to this problem by allowing an account to be automatically reset after an automatic lockout. The "LockoutDuration" allows administrators to set a reset delay period. An account that has been automatically locked out will be automatically reset after the delay period lapses.	July 1993	Automatic Account Resets deliver network availability and usability through resetting accounts following an automatic lockout.	Microsoft's innovation report: "SAM Client to Server", on pages 15 to 17.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] Tanenbaum, Andrew S.: Modern Operating Systems (Prentice Hall, Upper Saddle River, NJ, USA; 195; 1992)	[March-T, 97]
Security Account Manager Remote Protocol	MS-SAMR	Combination of MS-SAMR Technologies	The Combination of all the MS-SAMR Technologies.	July 1993	Together, the innovations set forth above significantly decrease demands upon administrators dealing with account and password information.	Microsoft's innovation report: "SAM Client to Server"	The claimed innovation is the combination of different features belonging to the same protocol. Combining these individual features is an obvious step for a person skilled in the art. NON-INNOVATIVE		[July-T, 70]
Security Account Manager Remote Protocol	MS-SAMR	Fast Retrieval of Account Names Based on Partially Entered Account Names	The MS-SAMR method SamrGetDisplayEnumerationIndex2 takes an index containing an account name or portion of an account name and returns a sorted list of accounts.	July 1993	Fast Retrieval of Account Names Based on Partially Entered Account Names delivers network administration efficiency and usability.	Microsoft's innovation report: "SAM Client to Server", on pages 17 to 19.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] ISO: Information processing systems - Database language - SQL (ISO 9075:1987; http://archive.opengroup.org/public/tech/datam/sql.htm; The linked article provides some background about the chronology of the SQL standards.)	[March-T, 97]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Security Account Manager Remote Protocol	MS-SAMR	Fine-Grained Control over Password Policy	MS-SAMR allows policies to be fine-grained to allow for more precise and varying policies at the enterprise-wide level on down to individual users. These policies include: Whether to require a password, per user, or skip the minimum password length check, Minimum Password age - once set, the password cannot be changed for a period of time, Minimum Password Length, Password Complexity Check, Password History Check, LogonHours Restrictions, per user (client can only logon during certain hours), Workstations Restrictions, per user (client can only logon to certain workstations), Don't expire password, per user (skip the maximum password age check), Maximum Password age, Account Expires, per user - account is not usable after a certain period of time, Smartcard logon only - account can logon only using a smart card.	July 1993	The Fine-Grained Control Over Password Policy feature delivers network security and manageability through selectable password policy details.	Microsoft's innovation report: "SAM Client to Server", on pages 11 to 14.	NON-INNOVATIVE	[PA] Spafford, Eugene H./Weeber, Stephen A.: User Authentication and Related Topics: An Annotated Bibliography (Purdue technical report CSD-TR-91-086; http://homes.cerias.purdue.edu/~spaf/tech-reps/9186.pdf; Microsoft has taken a subset of the features described in papers referenced by Spafford and implemented them in MS-SAMR. See in particular the references [20], [55] and [147] cited therein.)	[July-T, 68-69] [March-T, 96]
Security Account Manager Remote Protocol	MS-SAMR	Local Password Recovery	Local recovery password can be set for safe-mode recovery of a domain controller.	July 1993	Local Password Recovery and availability through setting the local recovery password of a domain controller enable a failed domain controller to be promptly restarted while remaining secured.	Microsoft's innovation report: "SAM Client to Server", on pages 14 to 15.	The claim concerns resolving problems which are specific to Microsoft's implementation. NON-INNOVATIVE	[R] U.S. Department of Defense: Trusted Computer System Evaluation Criteria (3.3.3.1.5 on trusted recovery; December 1985; http://www.iwar.org.uk/comsec/resources/standards/rainbow/5200.28-STD.html)	[July-T, 69] [March-T, 96]
Security Account Manager Remote Protocol (Server to Server)	MSSAMS	Expedited User Password Updates	With MS-SAMS, certain password changes (such as password update or account terminations) on low-level DCs (e.g., DC-1, DC-3) are immediately sent (i.e., "pushed") to the PDC. The change is then cascaded down each branch to each DC. As a result, password changes are quickly propagated throughout the network. It ensures usability through network homogeneity and network security by quickly denying terminated accounts access to any part of the network through prompt password updates and quickly enabling access to new users. It delivers network security and usability by minimizing the delay between password updates and system-wide implementation of those updates.	unclear, probably between 1993-2003	Expedited, system wide, User Password Updates provide improved security and usability through enabling prompt communication of changes in password status throughout a network.	Microsoft's innovation report: "Security Account Manager Remote protocol (server-to-server)", on pages 6 to 8.	The description of the claim is unclear. NON-INNOVATIVE	[PA] U.S. Patent 5,611,048: Remote password administration for a computer network among a plurality of nodes sending a password update message to all nodes and updating on authorized nodes (IBM; 11 June 1997 (Filed 9 May 1994 as 08/240,291); Depending on the actual claim date, this patent may be appropriate prior art.)	[July-T, 72] [March-T, 95]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Net Logon Remote Protocol (Server to Server)	NLOGON	Generic Pass-Through Authentication	Authentication data using the Net Logon secure channel causes a package, which is a blob, to pass from one (source) Net Logon component to another (destination) Net Logon component. The destination Net Logon component then routes the package to the component associated with the particular authentication protocol.	December 1999	Generic Pass-Through Authentication delivers network functionality through improved interoperability.	Microsoft's innovation report "Net Logon remote", on pages 9 to 11.	NON-INNOVATIVE	[PA] The Open Group: DCE 1.1: Remote Procedure Call (Catalog number C706; section 4.2.9.5; August 1997; http://www.opengroup.org/public/pubs/catalog/c706.htm) [PA] Ylonen, Tatu/Kivinen, T./Saarinen, M.: SSH Protocol Architecture (IETF Draft; 7 November 1997; http://tools.ietf.org/id/draft-ietf-secsh-architecture-01.txt) [PA] Ylonen, Tatu: The SSH (Secure Shell) Remote Login Protocol (15 November 1995; https://datatracker.ietf.org/drafts/draft-ylonen-ssh-protocol/)	[July-T, 74-75] [March-T, 100]
Net Logon Remote Protocol (Server to Server)	NLOGON	Service Discovery	Net Logon's generic pass-through allows multiple authentication protocols (e.g. NTLM, Kerberos) to communicate with a domain controller using Net Logon's secure channel. Any authentication data can utilize Net Logon's secure channel for passing secure data to a domain controller.	December 1999	The protocol delivers network efficiency through faster Service Discovery.	Microsoft's innovation report "Net Logon remote", on pages 6 to 9.	NON-INNOVATIVE	[PA] U.S. Patent 5,758,077: Service-centric monitoring system and method for monitoring of distributed services in a computing network (Hewlett-Packard Company; 26 May 1998 (Filed 2 August 1996 as 08/691,994)) [PA] The Open Group: DCE 1.1: Directory Services (Catalog number C705; August 1997; http://www.opengroup.org/pubs/catalog/c705.htm) [PA] Goland, Yaron Y. et al: Simple Service Discovery Protocol/1.0 (IETF Draft; 21 June 1999; http://tools.ietf.org/html/draft-cai-ssdp-v1-02) [PA] Cisco: Appletalk Specification (1984; www.cisco.com/univercd/cc/td/doc/cisintwk/itg_v1/tr1909.htm)	[July-T, 73-74] [March-T, 99]
Microsoft RADIUS Attributes for Network Access Protection	RADIUS	Vendor-Specific Attributes	RADIUS provides Authentication, Authorization, and Accounting (AAA) of end systems in scenarios such as wireless networking, dial-up networking, and virtual private networking.	December 1999	Microsoft's Vendor-Specific Attributes promote extensibility, efficiency and security by enabling transport of Client Health Information from a client to a RADIUS server over the RADIUS protocol so that the RADIUS server can tailor access to network resources.	Microsoft's Innovation Report: "Microsoft Vendor Specific RADIUS Attributes", pages 6 to 10.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE		[July-T, 81] [March-T, 94]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Remote Certificate Mapping Protocol	RCMP	Customized Mapping	A server uses RCMP to authenticate user's via X.509 certificates. A user submits a request for authentication to the server, based on a certificate. The server authenticates the user by matching the certificate with corresponding information in the user's account. The server uses attributes in the client's request for authentication to map the certificate to a security principal account for the user, such as an Active Directory account. In some environments, there is a need to support multiple certificate mapping schemes. Microsoft's RCMP addresses this need by allowing for customization of the selection of attributes used for mapping. An administrator can select between multiple attributes in an authentication request message for mapping the user's certificate to the user's account data in Active Directory. Microsoft's innovation delivers the ability to tailor mapping criteria to the specific needs of an organization.	December 1999	Customized Mapping delivers adaptability through administrator definable certificate mapping criteria.	Microsoft's innovation report: "Remote certificate mapping", pages 6 to 9.	NON-INNOVATIVE	[PA] US-Patent 6,088,805: Systems, methods and computer program products for authenticating client requests with client certificate information (IBM; 11 July 2000 (Filed 13 February 1998 as 09/023,863)) [PA] IBM: IBM WebSphereTM Application Server, Version 4.0.x (http://publib.boulder.ibm.com/infocenter/wasinfo/v4r0/index.jsp?topic=/com.ibm.websphere.v4.doc/wasa_content/050505.html; section 5.5.5: Mapping certificates to users for client authentication and authorization)	[July-T, 82] [March-T, 79]
Active Data Tablegram Protocol, includes RDS Transport Protocol	RDST	Byte Order Designation	Microsoft's RDST Protocol defines the byte-ordering of the row data in the result sets. Some systems use little-endian byte order, while others use big-endian byte order. Prior systems would encounter problems arising from the use of byte order in data different from the byte order used by the system. The tablegram header defines the byte-order of the result set, thereby increasing compatibility with different computer architectures using different byte order schemes.	August 1997	Byte Order Designation enhances interoperability through the definition of the byte order in the header of the tablegram.	Microsoft's Innovation Report: "Remote Data Services Transport", on pages 14 to 15.	NON-INNOVATIVE	[PA] TIS Committee: Tool Interface Standard (TIS) Portable Formats Specification, version 1.1 (October 1993; http://refspecs.freestandards.org/elf/TIS1.1.pdf) [PA] Cohen, Danny: On Holy Wars and a Plea for Peace (IEN137; 1 April 1980; http://www.ietf.org/rfc/ien/ien137.txt)	[July-T, 86] [March-T, 120]
Active Data Tablegram Protocol, includes RDS Transport Protocol	RDST	Hierarchical Data Representation	Microsoft's RDST Protocol presents related data in a hierarchical format. In this manner, it is unnecessary for the user to manage the relationships between data in parent and child result sets. Instead, the relationships between data are managed automatically, thereby enhancing usability and promoting data integrity. For example, if data related to sales is changed in one result set including sales data, this change is reflected in another result set including data related to the company that made the sales.	August 1997	Hierarchical data representation enhances usability and data integrity through automated management of related data.	Microsoft's Innovation Report: "Remote Data Services Transport", on pages 23 to 26.	NON-INNOVATIVE	[PA] Koch, George: Oracle 7 (Osborne/McGraw-Hill, second revised edition; 609; March 1993) [PA] ISO: Information Technology - Database Language SQL (ISO 9075:1992; July 1992; http://www.contrib.andrew.cmu.edu/~shadow/sql/sql1992.txt) [PA] Melton, Jim/Simon, Alan R.: Understanding the new SQL: A Complete Guide (Morgan Kaufmann Publishers; March 1993; page 403)	[July-T, 87] [March-T, 122]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Active Data Tablegram Protocol, includes RDS Transport Protocol	RDST	Relational Data Compression	Microsoft's RDST Protocol densely encodes the result sets that are transported between the server and client. Any row in the tablegram that contains no data is omitted from the result set, thereby decreasing the size of the result set and increasing processing efficiency. Prior systems did not compress the data in this manner. This innovation permits efficient use of the advantageous table approach to data sets.	August 1997	Relational Data Compression enhances processing efficiency through dense encoding of result sets.	Microsoft's Innovation Report: "Remote Data Services Transport", on pages 22 to 23.	NON-INNOVATIVE		[July-T, 87] [March-T, 121]
Active Data Tablegram Protocol, includes RDS Transport Protocol	RDST	Result Set Caching	Microsoft's RDST Protocol facilitates the caching of the results of a query on the client and allows transporting only the changes back to the server. Only data that is changed by the client is sent back to the server. In this manner, the amount of data that is communicated between the client and server is minimized, thereby enhancing efficiency.	August 1997	Result Set Caching enhances processing efficiency through storage of results on the client and transmission of only modified data to the server.	Microsoft's Innovation Report: "Remote Data Services Transport", on pages 9 to 11.	NON-INNOVATIVE	[PA] Keller, Arthur M./Basu, Julie: A Predicate-based Caching Scheme for Client-Server Database Architectures (VLDB Journal: Very Large Data Bases 5(1); 35-47; January 1996; http://citeseer.ist.psu.edu/231038.html) [PA] Franklin, Michael J./Carey, Michael J./Livny, Miron: Local Disk Caching for Client-Server Database Systems (Proceedings of the Nineteenth International Conference on Very Large Databases, Dublin, Ireland; 641-654; August 1993; http://citeseer.ist.psu.edu/franklin93local.html) [PA] Hennessy, John L./Patterson, David A: Computer Architecture: A Quantitative Approach, second edition (Morgan Kaufmann Publishers, San Francisco, CA; 1996; http://www.ercb.com/brief/brief.0042.html)	[July-T, 85] [March-T, 119]
Active Data Tablegram Protocol, includes RDS Transport Protocol	RDST	Result Set Packet Overloading	Microsoft's RDST Protocol transports multiple result sets in a single tablegram. In this manner, parent and child tables are transported in the same result set. In prior systems, each set of results was transported separately, increasing processing and network traffic overhead. Result set packet overloading reduces the overhead associated with transmission of multiple result sets, thereby enhancing efficiency.	August 1997	Result Set Packet Overloading enhances processing efficiency through transmission of multiple result sets in a single Tablegram.	Microsoft's Innovation Report: "Remote Data Services Transport", on pages 11 to 13.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE		[July-T, 85] [March-T, 120]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Active Data Tablegram Protocol, includes RDS Transport Protocol	RDST	User-Defined Option Packet	Microsoft's RDST Protocol facilitates extended properties that can be set for a result set by the client or server. For example, a vendor can reserve a 16-byte value for a property set, GUIDPropertySet. When this value is used, the PropertyID and PropertyValue fields can have meanings defined by the vendor. Thus, the vendor's implementation of the RDST Protocol can transmit extended properties. The extended properties are either understood by the receiving party of the result set, or the receiving party can simply ignore the extended properties. The extended properties thereby enhance the extensibility of the tabular datastream format.	August 1997	User-Defined Option Packet enhances extensibility through extended properties that can be associated with a results set.	Microsoft's Innovation Report: "Remote Data Services Transport", on pages 15 to 22.	NON-INNOVATIVE	[PA] U.S. Patent 5,632,015: Computer program product to efficiently process diverse result sets returned by a stored procedure (IBM; 20 May 1997 (Filed 7 June 1995 as 08/474,111)) [PA] Sperberg-McQueen, C. M.: From the W3C SGML ERB to the SGML WG and from the W3C XML ERB to the XML SIG (9 October 1996; http://www.w3.org/XML/9712-reports.html#ID1)	[July-T, 86] [March-T, 121]
RPC over HTTP Protocol	RHTTP	Carrying RPC on an HTTP Transport	HTTP is a nearly ubiquitous transport protocol, because it is the protocol used by the World Wide Web. Today, HTTP traffic constitutes the vast majority of all traffic carried on the Internet. In many settings, the only transport available for carrying out communication between a client and a server is HTTP. For example, most ordinary computer users primarily communicate with servers on the Internet via their web browsers, meaning HTTP is a required transport for carrying on communication with such users. The state of affairs existing prior to Microsoft's RPC over HTTP Protocol was that RPC could not be conducted with such users. Microsoft's RPC over HTTP Protocol specifies a way in which encoded RPC PDUs may be inserted into the message body of HTTP requests and responses.	July 1996 (Trustee doubts this based on information provided by Microsoft at (http://msdn2.microsoft.com/En-US/library/aa378698.aspx which points to October 1998)	Carrying RPC on an HTTP Transport promotes flexibility and compatibility by transporting encoded RPC in the body of HTTP requests and responses.	Microsoft's Innovation Report: "RPC over HTTP", on pages 7 to 11.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE		[July-T, 88] [March-T, 104]
RPC over HTTP Protocol	RHTTP	Establishing Virtual In and Out Channels	Microsoft's virtual in and out channels permit RPC function calls to execute when they require more data than can be carried on in a single HTTP request, or when they generate a response that requires more data than can be carried on a single HTTP request. Such an ability promotes usability and reliability by preventing the client from malfunctioning in the event of such an RPC call, and effectively enabling the use of HTTP to communicate RPC, with all the benefits that result from this option.	March 2003	Establishing Virtual In and Out Channels promotes usability and reliability by layering an infinite request/response data stream on a finite transport.	Microsoft's Innovation Report: "RPC over HTTP", on pages 17 to 25.	INNOVATIVE		[July-T, 89] [March-T, 105]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
RPC over HTTP Protocol	RHTTP	Selection of Separate Inbound and Outbound Proxies	When RPC is conducted via HTTP, the HTTP requests and responses are communicated through one or more proxies. Proxies typically execute firewall software, i.e., software that examines incoming packets, and elects not to pass them on to the remainder of the network if the packet violates one or more of a set of chosen rules. In some instances, the firewall software may block an HTTP packet carrying RPC BLOBs (Binary Large Objects). To address this issue, RHTTP Protocol permits selection of a particular proxy for forwarding of RPC PDUs to the server, the "inbound proxy." To address the reverse issue regarding an outgoing packet, RHTTP permits selection of another proxy for forwarding of HTTP responses to the client. The ability to select inbound and outbound proxies permit RPC to adapt to the network environment, and to avoid proxies implementing uncooperative firewalls. Therefore, RPC is able to function in a relatively wider range of network environments.	March 2003	Selection of Separate Inbound and Outbound Proxies promotes adaptability by permitting a troublesome firewall to be circumvented.	Microsoft's Innovation Report: "RPC over HTTP", on pages 12 to 16.	NON-INNOVATIVE	[PA] Xu, Jun/Singhal, Mukesh: Logical Firewalls: A Mechanism for Security in Future Networking Environments (1996; http://citeseer.ist.psu.edu/363105.html) [PA] Black, Uyless: Computer Networks: Protocols, Standards and Interfaces, second edition (Prentice Hall; 1993) [PA] RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1 (June 1999; http://tools.ietf.org/html/rfc2616)	[July-T, 89] [March-T, 104]
Microsoft Secure RPC Protocols	RPC	64-Bit Network Data Representation	When a client and server communicate with one another via RPC, they exchange sets of information known as RPC PDUs. Data within an RPC PDU is represented in a predetermined manner known as a transfer syntax. Most data types, including arrays and pointers, for example, are 32-bit data types. As computer systems have advanced, some systems have moved to a 64-bit platform. Hence, their pointers are 64 bits in length. Per C706, there is no way to represent a 64-bit pointer, because it must be mapped into a 32-bit space. Thus, NDR as specified in C706 is inadequate for a 64-bit platform. To solve the aforementioned problem, Microsoft has specified a 64-bit representation of data types, referred to as 64-bit network data representation (64-bit NDR). For example, according to Microsoft's 64-bit NDR, an array is expressed via a syntax employing a 64-bit maximum count, meaning that an array may have twice as many elements as were possible per NDR as specified in C706. Further, all pointers are specified as being 64 bit in length. Thus, Microsoft's 64-bit NDR is compatible with a 64-bit platform.	March 2003	64-bit Network Data Representation delivers adaptability by permitting various data types, including pointers, to be represented as 64-bit quantities.	Microsoft's Innovation Report: "Remote Procedure Call Protocol Extensions", on pages 13 to 16.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[R] SCO: Developer Specs (http://www.sco.com/developers/devspecs ; Use of 64-bit is simply an obvious logical extension of 32-bits in the same way that 32-bits is an obvious extension of 16-bits.)	

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Microsoft Secure RPC Protocols	RPC	Asynchronous RPC	Multiple RPC calls can be communicated in a single RPC session. However, a first RPC call must be completed prior to communication of a subsequent RPC call, i.e., the client must receive a response indicating that its RPC call was completed or canceled, or must receive a fault response in response to the RPC call. If, in the context of a single RPC session, a client communicates an RPC call prior to the server completing its action vis-à-vis a previous RPC call, the server aborts its action on the previous RPC call. Microsoft's RPC Protocol Extensions provides for asynchronous communication of RPC calls in a single RPC session. In other words, a client may communicate an RPC call to a server without having to wait for a previous RPC call to be completed, and may do so in the context of the RPC session used in connection with the previous RPC call. This advancement means that a new RPC session does not need to be established for each RPC call that is communicated prior to completion of a previous RPC call.	December 1999	Asynchronous RPC delivers efficiency and reliability by permitting asynchronous RPC Calls to be communicated along a single connection.	Microsoft's Innovation Report: "Remote Procedure Call Protocol Extensions", on pages 20 to 21.	NON-INNOVATIVE	[PA] The Open Group: Protocols for Interworking: XNFS, Version 3W (Document Number C702; 1998; http://www.opengroup.org/onlinepubs/9629799/) [PA] Ananda, A. L./Tay, B. H./Koh, E. K.: A survey of asynchronous remote procedure calls (National University of Singapore, Department of Information Systems and Computer Science, technical report TRB7/91; 97; 1991)	
Microsoft Secure RPC Protocols	RPC	Bind-Time Feature Negotiation	For a remote procedure call to successfully execute, a relationship must be established that associates a particular procedure call residing in a client with corresponding manager code residing on the server ("binding"). During the binding process, a client may check to ensure that the version of the interface to which it is to bind is compatible. Thus, at the time of binding, a client is aware of only the version number of the interface of the manager to which it is binding. According to Microsoft's RPC, during the binding operation, the client and server may exchange bitmasks. Each bit in the bitmask corresponds to a particular feature. If a given bit in a bitmask is set, then the corresponding feature is supported by the client or server sending the bitmask. If, on the other hand, a given bit in a bitmask is cleared, then the corresponding feature is not supported by the client or server sending the bitmask. By virtue of the foregoing scheme, the client and server can be made aware of features supported by one another at the time at which binding is occurring, reducing the burden on the network.	March 2003	Bind-Time Feature Negotiation delivers efficiency by communicating supported features on a feature-by-feature basis at the time of binding between a Client and a Server.	Microsoft's Innovation Report: "Remote Procedure Call Protocol Extensions", on pages 11 to 13.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] Millard, Peter/Saint-Andre, Peter/Paterson, Ian: XEP-0020: Feature Negotiation (February 2002; http://www.xmpp.org/extensions/xep-0020.html; This document defines an XMPP protocol extension that enables two entities to mutually negotiate feature options. The first version of the XMPP protocol has a copyright of 1999.)	

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Microsoft Secure RPC Protocols	RPC	Callback Methods	A connection between a client and a server must be established to provide for the initial invocation of a desired server operation, and the connection must be held open until the server responds. The rigid client/server scheme presents certain liabilities. For example, the server may occasionally require an extended period of time to respond to the client's RPC call, as is the case when the invoked operation is computationally intense. Microsoft's RPC Protocol Extensions allow for a client to present one or more of its methods as being invocable by the server. Such a method is referred to as a "callback method." The import of the foregoing is that a client may make an RPC call that invokes a client operation, and the server may respond by initiating the invoked process and closing the connection between the client and server. Upon completion of the invoked operation, the server may re-establish a connection with the client, and may invoke a callback method that is designed to receive the RPC response via the newly established connection.	July 1993	Callback Methods deliver efficiency and scalability by permitting a server to invoke a client callback method.	Microsoft's Innovation Report: "Remote Procedure Call Protocol Extensions", on pages 22 to 24.	NON-INNOVATIVE	[PA] Myers, Brad A.: Separating Application Code From Toolkits: Eliminating The Spaghetti Of Call-Backs (Symposium on User Interface Software and Technology, Proceedings of the 4th annual ACM symposium on User interface software and technology; 211-220; 1991) [PA] Apple: Pascal to C: Procedure Parameters (Apple, technical note PT31; February 1990; http://developer.apple.com/technotes/pt/pt_31.html) [PA] Heller, Dan: Motif Programming Manual (January 2001) [PA] Object Management Group: CORBA 1.0 (October 1991; http://www.omg.org/gettingstarted/history_of_corba.htm; included Call backs and RPC calls)	
Microsoft Secure RPC Protocols	RPC	Header Signing	When a client and server communicate with one another via RPC, they exchange sets of information known as RPC protocol data units, or RPC PDUs, which are encoded as binary large objects. To ensure that an RPC PDU is not tampered with as it traverses the network between the client and the server, the RPC PDU may be presented to a security service. When a PDU is provided to a security provider for digital signing, the digital signature is formed based upon a digest of the PDU contents. In prior systems, the PDU contents provided to the security provider excluded the PDU header. Thus, the information in the PDU header was not taken into account during the creation of the digital signature. This meant that a PDU header could be altered without detection. In RHTTP, information from the PDU header is copied into a portion of the PDU body called the verification trailer. By virtue of inclusion in the PDU body, the header information is included in the set of information provided to the security service, and therefore to the hash function.	March 2003	Header Signing delivers enhanced security by including PDU Header data in a verification trailer.	Microsoft's Innovation Report: "Remote Procedure Call Protocol Extensions", on pages 7 to 10.	NON-INNOVATIVE	[PA] Pruneda, Andrea: Developing a License Provider service for Windows Media Encoder (November 2002; http://msdn2.microsoft.com/en-us/library/ms867146.aspx) [PA] Blom, Rolf et al: The Secure Real Time Transport Protocol (July 2001; http://tools.ietf.org/html/draft-ietf-avt-srtp-01)	

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Microsoft Secure RPC Protocols	RPC	Security Context Multiplexing	For each new association or "connection" between a client and a server, a new security context is to be created. A security context is a set of information used for completion of the specified security governing the communication between the client and server vis-à-vis a given connection. The rule of one security context is established per connection. If it does not allow for more than one security context to be opened for a given connection, the intermediate server may eventually run out of connections (because it must continually open new connections for each new security context). Microsoft's security context multiplexing technology addresses this issue by permitting more than one security context to be applied to a given channel. The effect of this is that the intermediate server is less apt to exhaust its ability to open new connections, and is therefore better able to reliably offer service to its various clients.	March 2003	Security Context Multiplexing delivers reliability by permitting multiple security contexts to be applied to a single connection.	Microsoft's Innovation Report: "Remote Procedure Call Protocol Extensions", on pages 16 to 20.	NON-INNOVATIVE	[PA] BEA Systems: Load Balancing in BEA Tuxedo CORBA Applications (7 October 2002; http://whitepapers.techrepublic.com.com/ whitepaper.aspx?docid=42326) [PA] RFC 3080: The Blocks Extensible Exchange Protocol Core (March 2001; http://tools.ietf.org/html/rfc3080)	
Remote Procedure Call Protocol Extensions	RPCEXT	64-Bit Network Data Representation	When a client and server communicate with one another via RPC, they exchange sets of information known as RPC PDUs. Data within an RPC PDU is represented in a predetermined manner known as a transfer syntax. Data within an RPC PDU is represented in accord with network data representation (NDR). Per NDR, most data types, including arrays and pointers, for example, are 32-bit data types. Other types of pointers are specified by NDR, and the referent identifiers of those other pointer types are also always 32 bits. As computer systems have advanced, some systems have moved to a 64-bit platform. Hence, their pointers are 64 bits in length. There is no way to represent a 64-bit pointer, because it must be mapped into a 32-bit space. Microsoft has specified a 64-bit representation of data types, referred to as 64-bit network data representation. For example, according to Microsoft's 64-bit NDR, an array is expressed via a syntax employing a 64-bit maximum count. Further, all pointers are specified as being 64 bits in length. Thus, Microsoft's 64-bit NDR is compatible with a 64-bit platform.	March 2003	64-Bit Network Data Representation delivers adaptability by permitting various data types, including pointers, to be represented as 64-Bit quantities.	Microsoft's Innovation Report: "Remote Procedure Call Protocol Extensions", on pages 13 to 16.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[R] SCO: Developer Specs (http://www.sco.com/developers/devspecs ; Use of 64-bit is simply an obvious logical extension of 32-bits in the same way that 32-bits is an obvious extension of 16-bits.)	[July-T, 93] [March-T, 128]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Remote Procedure Call Protocol Extensions	RPCEXT	Asynchronous RPC	Multiple RPC calls can be communicated in a single RPC session. However, a first RPC call must be completed prior to communication of a subsequent RPC call. If, in the context of a single RPC session, a client communicates an RPC call prior to the server completing its action vis-à-vis a previous RPC call, the server aborts its action on the previous RPC call. With prior technology, a new RPC session must be established for each RPC call that is to be initiated prior to the completion of a previous RPC call. RPCEXT provides for asynchronous communication of RPC calls in a single RPC session. In other words, a client may communicate an RPC call to a server without having to wait for a previous RPC call to be completed, and may do so in the context of the RPC session used in connection with the previous RPC call. A new RPC session does not need to be established for each RPC call that is communicated prior to completion of a previous RPC call.	December 1999	Asynchronous RPC delivers efficiency and reliability by permitting asynchronous RPC Calls to be communicated along a single connection.	Microsoft's Innovation Report: "Remote Procedure Call Protocol Extensions", on pages 20 to 21.	NON-INNOVATIVE	[PA] The Open Group: Protocols for Interworking: XNFS, Version 3W (Document Number C702; 1998; http://www.opengroup.org/onlinepubs/9629799/) [PA] Ananda, A. L./Tay, B. H./Koh, E. K.: A survey of asynchronous remote procedure calls (National University of Singapore, Department of Information Systems and Computer Science, technical report TRB7/91; 97; 1991)	[July-T, 94] [March-T, 128]
Remote Procedure Call Protocol Extensions	RPCEXT	Bind-Time Feature Negotiation	For a remote procedure call to successfully execute, a relationship must be established that associates a particular procedure call residing in a client with corresponding manager code residing on the server. This association is referred to as a "binding." According to Microsoft's RPC Protocol Extensions, during the binding operation, the client and server may exchange bitmasks. Each bit in the bitmask corresponds to a particular feature. If a given bit in a bitmask is set, then the corresponding feature is supported by the client or server sending the bitmask. If, on the other hand, a given bit in a bitmask is cleared, then the corresponding feature is not supported by the client or server sending the bitmask. By virtue of the foregoing scheme, the client and server can be made aware of features supported by one another at the time at which binding is occurring, reducing the burden on the network.	March 2003	Bind-Time Feature Negotiation delivers efficiency by communicating supported features on a feature-by-feature basis at the time of binding between a Client and a Server.	Microsoft's Innovation Report: "Remote Procedure Call Protocol Extensions", on pages 11 to 13.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] Millard, Peter/Saint-Andre, Peter/Paterson, Ian: XEP-0020: Feature Negotiation (February 2002; http://www.xmpp.org/extensions/xep-0020.html; This document defines an XMPP protocol extension that enables two entities to mutually negotiate feature options. The first version of the XMPP protocol has a copyright of 1999.)	[July-T, 93] [March-T, 127]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Remote Procedure Call Protocol Extensions	RPCEXT	Callback Methods	A connection between a client and server must be established to provide for the initial invocation of a desired server operation, and the connection must be held open until server responds. The rigid client/server scheme imposed presents certain liabilities. For example, occasionally, the server may require an extended period of time to respond to the client's RPC call. Microsoft's RPCEXT allows for a client to present one or more of its methods as being invocable by the server. The import of the foregoing is that a client may make an RPC call that invokes a client operation, and the server may respond by initiating the invoked process and closing the connection between the client and server. Upon completion of the invoked operation, the server may re-establish a connection with the client, and may invoke a callback method that is designed to receive the RPC response via the newly established connection. The effect of the foregoing is to eliminate the need to hold open connections during lengthy intervening periods between an RPC call and an RPC response.	July 1993	Callback Methods deliver efficiency and scalability by permitting a server to invoke a client callback method.	Microsoft's Innovation Report: "Remote Procedure Call Protocol Extensions", on pages 22 to 24.	NON-INNOVATIVE	[PA] Myers, Brad A.: Separating Application Code From Toolkits: Eliminating The Spaghetti Of Call-Backs (Symposium on User Interface Software and Technology, Proceedings of the 4th annual ACM symposium on User interface software and technology; 211-220; 1991) [PA] Apple: Pascal to C: Procedure Parameters (Apple, technical note PT31; February 1990; http://developer.apple.com/technotes/pt/pt_31.html) [PA] Heller, Dan: Motif Programming Manual (January 2001) [PA] Object Management Group: CORBA 1.0 (October 1991; http://www.omg.org/gettingstarted/history_of_corba.htm; included Call backs and RPC calls)	[July-T, 95] [March-T, 129]
Remote Procedure Call Protocol Extensions	RPCEXT	Header Signing	When a client and server communicate with one another via RPC as defined in The Open Group, they exchange sets of information known as RPC protocol data units, or RPC PDUs, which are encoded as binary large objects (BLOBs). To ensure that an RPC PDU is not tampered with as it traverses the network between the client and the server, the RPC PDU may be presented to a security service. The security service is a unit of software that may perform security functions, such as encrypting the PDUs, digitally signing the PDUs, etc. When a PDU is provided to a security provider for digital signing, the digital signature is formed based upon a digest of the PDU contents. In Microsoft's Remote Procedure Call Protocol Extensions using RPC Header Signing, information from the PDU header is copied into a portion of the PDU body called the verification trailer. By virtue of inclusion in the PDU body, the header information is included in the set of information provided to the security service, and therefore to the hash function.	March 2003	Header Signing delivers enhanced security by including PDU Header data in a verification trailer.	Microsoft's Innovation Report: "Remote Procedure Call Protocol Extensions", on pages 7 to 10.	NON-INNOVATIVE	[PA] Pruneda, Andrea: Developing a License Provider service for Windows Media Encoder (November 2002; http://msdn2.microsoft.com/en-us/library/ms867146.aspx) [PA] Blom, Rolf et al: The Secure Real Time Transport Protocol (July 2001; http://tools.ietf.org/html/draft-ietf-avt-srtp-01)	[July-T, 92] [March-T, 127]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Remote Procedure Call Protocol Extensions	RPCEXT	Security Context Multiplexing	For each new association or "connection" between a client and a server, a new security context is to be created. A security context is a set of information used for completion of the specified security governing the communication between the client and server vis-à-vis a given connection. The rule of one security context is established per connection. If it does not allow for more than one security context to be opened for a given connection, the intermediate server may eventually run out of connections (because it must continually open new connections for each new security context). Microsoft's security context multiplexing technology addresses this issue by permitting more than one security context to be applied to a given channel. The effect of this is that the intermediate server is less apt to exhaust its ability to open new connections, and is therefore better able to reliably offer service to its various clients.	March 2003	Security Context Multiplexing delivers reliability by permitting multiple security contexts to be applied to a single connection.	Microsoft's Innovation Report: "Remote Procedure Call Protocol Extensions", on pages 16 to 20.	NON-INNOVATIVE	[PA] BEA Systems: Load Balancing in BEA Tuxedo CORBA Applications (7 October 2002; http://whitepapers.techrepublic.com.com/whitepaper.aspx?docid=42326) [PA] RFC 3080: The Blocks Extensible Exchange Protocol Core (March 2001; http://tools.ietf.org/html/rfc3080)	[July-T, 94] [March-T, 128]
Remote Procedure Call Location Services Protocol	RPCLS	Location Service Query Forwarding	Microsoft's RPC-LS extends the Name Service Interface specification defined in the Distributed Computing Environment (DCE) standard RPC protocol to provide RPC location service functionality in a directory service environment. RPC Location Services provides an automated, dynamic method for assigning multiple RPC endpoints at runtime to a server process, and for the server process to efficiently inform a requesting client of these endpoints. By implementing RPC location services in a directory service like Active Directory (AD), RPC-LS makes use of a number of features of AD that would otherwise not be available in a remote environment.	December 1999	RPC-LS Service Query Forwarding delivers extensibility by providing support for computers with and without AD.	Microsoft's Innovation Report: "Remote Procedure Call Location Services Extensions", on pages 6 to 10.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE		[July-T, 91] [March-T, 126]
Removable Storage Manager Remote Protocol	RSM	Innovative Control Libraries	Microsoft's RSM Remote Protocol standardizes the libraries that are used to control the devices associated with the RSM Remote Protocol, such as robotic changers, media libraries and tape drives. In this manner, the user can control the devices through a consistent interface facilitated by the RSM Remote Protocol, thereby increasing the efficiency for the user. For example, the libraries used to control one device, such as a tape drive, are consistent with the libraries used to control a different device, such as a robotic changer. The user can therefore utilize the libraries to efficiently control multiple devices.	December 1999	Innovative Control Libraries enhance usability through standardizing control of different storage devices.	Microsoft's Innovation Report: "Removable Storage Manager Remote", on pages 10 to 11.	NON-INNOVATIVE	[PA] Apple: MAC O/S X Mass Storage Driver Stack (introduced with Mac OS/X formal release in March 2001; http://developer.apple.com/documentation/DeviceDrivers/Conceptual/MassStorage/02_Overview/chapter_2_section_4.html#//apple_ref/doc/uid/TP30000734-BJGCIFBA)	[July-T, 97]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Removable Storage Manager Remote Protocol	RSM	System Service Level Implementation	The RSM Remote Protocol is a set of a distributed component object model interfaces for applications to manage robotic changers, media libraries and tape drives. The RSM Remote Protocol deals with detailed low-level operating system and storage concepts. Specifically, the RSM Remote Protocol provides a mechanism for the remote configuration and management of removable storage devices. The Protocol allows multiple applications to manage removable media within a single-server system and share local robotic media libraries, tape drives, and disk drives. The protocol also enables clients to obtain notifications of changes to these storage objects.	December 1999	System Service Level Implementation enhances interoperability through management of devices at the driver level.	Microsoft's Innovation Report: "Removable Storage Manager Remote", on pages 6 to 10.	NON-INNOVATIVE	[PA] U.S. Patent 5,983,283: Storage manager independent configuration interface translator and method (Sun Microsystems; 9 November 1999 (Filed 15 April 1996 as 08/632,217)) [PA] ANSI: Information technology - Small Computer System Interface - 2 (SCSI) (ANSI X3T9.2 Project 375D, Revision 10, Working Draft; 7 September 1993; http://t10.org/ftp/t10/drafts/s2/s2-r10l.pdf) [PA] Goland, Yaron Y. et al: Simple Service Discovery Protocol/1.0 (IETF Draft; 21 June 1999; http://tools.ietf.org/html/draft-cai-ssdp-v1-02) [PA] USB Implementers Forum: USB specification (USB 1.0 released in January 1996; http://www.usb.org; http://en.wikipedia.org/wiki/USB)	[July-T, 96] [March-T, 63]
Service For Users	S4U	Constrained Delegation	When a user requests authentication in order to access a service on a server, the server relies on a trusted source, such as a Kerberos domain controller, for authenticating the user. However, some clients may not have information or processes to request authentication. Under prior authentication protocols, the client could delegate the authentication to the server, but in order for the server to have rights to obtain tickets for the user, the server had to obtain a ticket granting ticket (TGT) from the trusted source. An undesirable consequence of this approach is that the server could obtain tickets to many other services and delegate the TGT to other servers. To overcome this, S4U permits the server to request an authentication ticket on behalf of the user instead of the server.	March 2003	Constrained Delegation delivers security and interoperability through limited delegation of authentication credentials.	Microsoft's Innovation Report: "Kerberos Protocol Extensions: Service For User (S4U) and Constrained Delegation", on pages 6 to 11.	NON-INNOVATIVE	[PA] Condell, Matthew N.: A Security Model for the Information Mesh (MIT/LCS/TR-691; June 1996) [PA] Erdos, Marlena E./Pato, Joseph N.: Extending the OSF DCE Authorization System to Support Practical Delegation (Proceedings of the PSRG Workshop on Network and Distributed System Security; 93-100; February 1993) [PA] Pato, Joseph N.: Extending the OSF DCE Authorization System to Support Practical Delegation (SF DCE SIG, RFC 3.0; June 1992; http://www.opengroup.org/tech/rfc/mirror-rfc/rfc3.0.txt)	[July-T, 98] [March-T, 146]
Service For Users	S4U	Protocol Transition	Protocol transition allows a user to have access to the service on the server without first authenticating with Kerberos. Protocol Transition delivers adaptability by allowing access to users who have authenticated with a means other than Kerberos. S4U permits the server to then seek a Kerberos authentication on behalf of the user for use with services that may require it.	March 2003	Protocol Transition delivers adaptability.	Microsoft's Innovation Report: "Kerberos Protocol Extensions: Service For User (S4U) and Constrained Delegation", on pages 11 to 17.	NON-INNOVATIVE	[PA] SURFnet: The innovative authentication system (A-Select) (implementation before March 2003; http://a-select.surfnet.nl/aselect_overview.html)	[July-T, 98] [March-T, 146]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Shadow Copy Network Access Protocol	SCNA	Extended File Information	The SMB protocol provides for a server to return extended information, such as the maximal access rights of a user to a file or share in response to a request. This extended information allows a client to implement additional functionality, such as caching of share information. Prior to Microsoft's innovation, CIFS did not provide for a server to send a client this extended information.	December 1999	Extended File Information benefits users by reducing the number of requests a client makes to a server and servicing requests locally.	Microsoft's Innovation Report: "Microsoft Server Message Block (SMB) Protocol and Extensions", on pages 28 to 32.	NON-INNOVATIVE		[July-T, 101] [March-T, 103]
Shadow Copy Network Access Protocol	SCNA	Message Signing	The SMB protocol provides for a server to return extended information, such as the maximal access rights of a user to a file or share in response to request. This extended information allows a client to implement additional functionality, such as caching of share information. Prior to Microsoft's innovation, CIFS did not provide for a server to send a client this extended information.	December 1999	Message Signing promotes the benefit of security by guaranteeing response and request message integrity.	Microsoft's Innovation Report: "Microsoft Server Message Block (SMB) Protocol and Extensions", on pages 8 to 12.	NON-INNOVATIVE	[PA] *Hobbit*: CIFS: Common Insecurities Fail Scrutiny (Avian Research; January 1997; http://web.textfiles.com/hacking/cifs.txt) [PA] Rubin, Frank: Message Authentication Using Quadratic Residues (Cryptologia XIX(4); October 1995; http://www.mastersoftware.biz/crypt002.htm) [PA] National Institute of Standards and Technology: Computer Data Authentication (Federal Information Processing Standards (FIPS) Publication 113; 30 May 1985; http://www.itl.nist.gov/fipspubs/fip113.htm) [PA] ISO/IEC: Banking - Approved Algorithms for Message Authentication - Part 1: Data Encryption Algorithm (DEA) (ISO/IEC 8731:1987; 1987) [PA] ANSI: Financial Institution Message Authentication (Wholesale) (ANSI X9.9:1986, American Bankers Association; 15 August 1986) [PA] RFC 1321: The MD5 Message-Digest Algorithm (April 1992; http://tools.ietf.org/html/rfc1321) [R] Schneier, Bruce: Applied Cryptography: Protocols, Algorithms, and Source Code in C (Wiley; 31 January 1996)	[July-T, 99-100] [March-T, 101]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Shadow Copy Network Access Protocol	SCNA	Retrieving Prior Versions of Files	The SMB protocol allows a client to view a list of prior versions of a file that a client can use to recover one of the versions. Using the SMB protocol, a client sends a request for snapshots (i.e., prior versions of volumes which may contain prior versions of a file) to a server. In response to the request, a server obtains a list of snapshots, including timestamps, and returns the data to the client, which the client can use to access prior versions of files. Often, it is difficult to recover a version of a file that has been lost by a user. The file may have been lost by accidental deletion, by being overwritten with a different version, or a system error that results in the loss of a file. With Microsoft's innovation of enumerating and accessing previous versions of a file, a user can request a list of previous versions of the file and select the version it wants to recover.	March 2003	Retrieving Prior Versions of Files provides users with the benefit of data redundancy.	Microsoft's Innovation Report: "Microsoft Server Message Block (SMB) Protocol and Extensions", on pages 12 to 17.	NON-INNOVATIVE	[PA] ECMA: Universal Disk Format (UDF) file system (30 August 1996, Revision 1.02; http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-167.pdf; UDF is an implementation of ISO/IEC 13346 (also known as ECMA-167).) [PA] Digital Equipment Corporation: RSX-11 and VMS operating systems (http://www.computer.museum.uq.edu.au/RSX-11%20Manuals.html; This is a collection of historic manuals of these operating systems.) [PA] Digital Equipment Corporation: TOPS-20 operating system (1969; http://en.wikipedia.org/wiki/TOPS-20; Also see "Origins and Development of TOPS-20" at http://www.linique.com/dlm/tenex/hbook.html.) [PA] Tichy, Walter F.: RCS - A System for Version Control (Software - Practice & Experience 15(7); 637-654; July 1985; http://www.cs.purdue.edu/homes/trinkle/RCS/rcs.ps) [PA] Network Appliance Corporation: WAFL file system (Network Appliance Corporate, technical report 3002; 1994; http://www.netapp.com/library/tr/3002.pdf) [PA] Bell Labs: Plan 9 default Fossil File System (Manual page; 2002; http://plan9.bell-labs.com/magic/man2html/4/fossil) [PA] Dehaese, Gratien: (ISO 9660; ISO 9660 was first standardised in 1988.; http://users.pandora.be/it3.consultants.bvba/handouts/ISO9960.html)	[July-T, 100] [March-T, 101]
SMB2	SMB2	Command Compounding	SMB2 promotes processing efficiency by allowing multiple commands to be contained within a single SMB2 packet, i.e. command compounding. Command compounding promotes processing efficiency by allowing a client to send a number of requests together in a single packet avoiding the need to have to send each command in a separate packet.	July 2005	Command Compounding promotes processing efficiency by allowing a client to send numerous commands in a single request.	Microsoft's Innovation Report: "Server Message Block 2,0 Protocol Specification", on pages 14 to 19	NON-INNOVATIVE	[PA] Leach, Paul J./Naik, Dilip C.: A Common Internet File System (CIFS/1.0) Protocol (IETF draft; 19 December 1997; http://tools.ietf.org/html/draft-leach-cifs-v1-spec-01) [PA] RFC 3530: Network File System (NFS) version 4 Protocol (April 2003)	[July-T, 102-103] [March-T, 12]
SMB2	SMB2	Establishing Durable Opens	SMB2 allows a client to request a durable open to a file or directory. The durable open allows a client who is temporarily disconnected to reestablish the previous connection to a server without the need to negotiate a new session and connection with a client. A client merely sends a command to connect to a share, and the connection with the server is reestablished.	July 2005	Establishing Durable Opens promotes processing efficiency by allowing a client to reconnect without establishing a new connection.	Microsoft's Innovation Report: "Server Message Block 2,0 Protocol Specification", on pages 19 to 20.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] U.S. Patent 6,349,350: System, method, and program for handling failed connections in an input/output (I/O) system (IBM; 19 February 2002 (Filed 4 May 1999 as 09/304,736); United States Patent 6349350, Issued on February 19, 2002,) [PA] RFC 3748: Extensible Authentication Protocol (EAP) (June 2004; http://tools.ietf.org/html/rfc3748; See "Fast Connect", part of this RFC.)	[July-T, 103] [March-T, 13]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
SMB2	SMB2	Sequence Numbering	The use of sequence numbers protects the server against denial of service attacks made by malicious users. A server grants the client a certain number of credits, and the client consumes a credit for sending each command to the server. Each credit corresponds to a sequence number, which is included in each command sent to the server. A server can thus control the amount of resources consumed by a client by issuing more or less credits. Denial of service attacks occur when a malicious user attempts to send an inordinate number of requests/commands for processing by a server. The large number of commands overwhelms the server by consuming all of the server's available resources. This results in the server being unable to process requests from legitimate users. The use of sequence numbering in SMB2 provides an elegant mechanism for protecting a server from denial of service attacks by allowing a server to control the number of requests that a single client can have processed.	July 2005	Sequence Numbering provides robust security against denial of service attacks by controlling the number of requests a client can issue.	Microsoft's Innovation Report: "Server Message Block 2,0 Protocol Specification", on pages 7 to 14.	NON-INNOVATIVE	[PA] RFC 2402: IP Authentication Header (November 1998; http://tools.ietf.org/html/rfc2402)	[July-T, 102] [March-T, 11]
Passport Protocol	SSI	Authentication Server Redirection	Within a realm of computers (i.e., clients, partner servers, and Passport authentication servers), a client is required to present login credentials to an authentication server in order to obtain access to restricted partner servers. If a client sends a login-request to a busy (or incorrect) authentication server within the realm, that server may redirect the client to a more appropriate authentication server (where the client repeats the login-request at the new server). In this instance, the SSI 1.4 (Passport) protocol redirects a client to a proper authentication server. That is, if a first authentication server is busy (or is not the correct server for a particular client or partner server), the client's attempt to access the partner server might fail, even though the client has proper credentials for that server. Thus, the ability of the first authentication server to redirect the client to a second authentication server within the realm provides fault tolerance and recoverability in the case of an error during the authentication process.	August 2001	Redirecting Client Login-Requests promotes reliability and efficiency by distributing the load between authentication servers.	Microsoft's Innovation Report: "Passport Server Side Include (SSI) 1,4", on pages 8 to 10.	NON-INNOVATIVE	[PA] Lioy, A./Maino, F.: Providing X.509-based user access control to web servers (Proceedings of the IFIP/SEC'98, 14th International Information Security Conference, Vienna/Budapest; 1998; http://citeseer.ist.psu.edu/505660.html) [PA] RFC 2617: HTTP Authentication: Basic and Digest Access Authentication (June 1999; http://tools.ietf.org/html/rfc2617) [PA] Katz, Eric Dean/Butler, Michelle/McGrath, Robert: A Scalable HTTP Server: The NCSA Prototype (Computer Networks and ISDN Systems; 155-164; May 1994; http://citeseer.ist.psu.edu/katz94scalable.html) [R] Gábor, Gombás: Evaluation of Distributed Authentication, Authorization and Directory Services (2001; http://www.caesar.elte.hu/eltenet/projects/demogrid/demogrid-report-1/dg-rep-1-sec-eval.pdf; This is not prior art in itself but provides references to older papers.)	[July-T, 106] [March-T, 155]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Passport Protocol	SSI	Co-Branding	A client that undergoes the "Passport" authentication process is typically redirected from a "partner" Web site (i.e., the site to which the client is attempting to gain access) to an authentication server within the Passport realm. This redirection is necessary to allow the client to present login credentials to the authentication server (and thereby obtain the necessary tickets in order to access the restricted partner server). Because the authentication server typically sends messages that are displayed by the client (i.e., in a browser), the user may be confused and concerned by the sudden redirection. Thus, the authentication server dialogs may included "co-branded" information from the organization that operates the partner server, so that the user understands the connection between the authentication prompts and the original "partner" server. The co-branding information is sent to the client within designated fields of a "server challenge" message that is sent from the authentication server to the client during the login process.	August 2001	Co-Branding Authentication Server dialogs with "Partner Information" promotes usability by reassuring the user that the authentication process was requested by the partner server.	Microsoft's Innovation Report: "Passport Server Side Include (SSI) 1,4", on pages 10 to 12.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] U.S. Patent 6,601,761: Method and system for co-branding an electronic payment platform such as an electronic wallet (Citibank, N.A.; 5 August 2003 (Filed 15 September 1999 as 09/396,242)) [PA] WorldPay: WorldPay (founded in 1993; http://www.worldpay.com/about_us/index.php?page=history)	[July-T, 107] [March-T, 155]
Passport Protocol	SSI	Local Authentication	Local authentication enables participating Web servers to automatically use a client's local system-based authentication mechanism, provided that the server and the client are properly configured (i.e., are aware of the SSI 1.4 protocol). In particular, using a client's local system-based authentication mechanism (i.e., SSI 1.4) promotes efficiency since user credentials may be locally cached, thereby relieving the user from the requirement of manually entering username and password information each time the client contacts an SSI 1.4 authentication server.	August 2001	Using a Local Authentication mechanism promotes efficiency by allowing updated clients to obtain authentication credentials locally.	Microsoft's Innovation Report: "Passport Server Side Include (SSI) 1,4", on pages 6 to 8.	NON-INNOVATIVE	[PA] Rivest, Ronald A./Lampson, Butler: SDSI - A Simple Distributed Security Infrastructure (15 September 1996; http://people.csail.mit.edu/rivest/sdsi10.html) [PA] Lioy, A./Maino, F.: Providing X.509-based user access control to web servers (Proceedings of the IFIP/SEC'98, 14th International Information Security Conference, Vienna/Budapest; 1998; http://citeseer.ist.psu.edu/505660.html) [PA] RFC 2617: HTTP Authentication: Basic and Digest Access Authentication (June 1999; http://tools.ietf.org/html/rfc2617) [PA] RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1 (June 1999; http://tools.ietf.org/html/rfc2616) [PA] Lampson, Butler et al: Authentication in distributed systems: Theory and practice (ACM Transactions on Computer Systems 10(4); 265-310; November 1992; http://portal.acm.org/citation.cfm?id=138874) [PA] Leach, Paul J. et al: A Conceptual Authorization Model for Web Services (K. Sparck-Jones and A. Herbert (eds.): Computer Systems: Theory, Technology, and Applications; 137-146; 2004; http://research.microsoft.com/Lampson/71-ConceptualWebAuthZ/71-ConceptualWebAuthZ.pdf)	[July-T, 105-106] [March-T, 154]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Task Scheduler	TSCH	Account Per Job	The Account Per Job feature of Task Scheduler allows a set of jobs to be run, with each job in an account set by the user who schedules the job. For example, a system administrator can schedule a job to be run on the account of a client with lesser security privileges. Thus, each job can be scheduled to run with only the minimum privilege level needed to run that job, thereby enhancing system security. Alternative prior art approaches run scheduled jobs as the user scheduling them, e.g., in the example above, as the system administrator, leaving unattended jobs running with high security privileges. The Account Per Job feature offers even more security than the Scheduling Executables to Run on a Preset Account feature discussed above. Whereas the Scheduling Executables to Run on a Preset Account feature uses a single account for running all jobs, Account Per Job allows each individual job to run with its own separate account.	December 1999	Account Per Job enhances security by avoiding running jobs with unnecessary security privileges.	Microsoft's Innovation Report: "Task Scheduler", on pages 17 to 19.	NON-INNOVATIVE	[PA] Tomasello Software, LLC: WinCron Technical reference, Version 4.3 (2006; http://www.wincron.com/pages/WCTechnicalReference.pdf) [PA] IBM: IBM LoadLeveler: User's Guide (IBM Publication number ST00-9696; October 1994; see also IBM LoadLeveler for AIX 5L: Using and Administering http://www.ncsa.uiuc.edu/UserInfo/Resources/Hardware/IBMp690/IBM/usr/lpp/LoadL/html/am2ugmst02.html#ToC)	[July-T, 109] [March-T, 92]
Task Scheduler	TSCH	Condition-Based Task Execution	The Condition-Based Task Execution feature of Task Scheduler adds more refined control on whether a task can run. Events trigger when a task should execute. Upon being triggered, conditions detect if the task can or should in fact run at that time. Condition-Based Task. Execution detects the presence or absence of a set of conditions prescribed by the administrator for a particular task and permits the task to run only if the conditions are met. For example, it may be desirable to prevent a task from running on a laptop computer if the remaining battery power, network connectivity or idle state of the computer is not suitable for running the task.	December 1999	Condition-Based Task Execution enhances maintainability by adding more refined control on when a task can run.	Microsoft's Innovation Report: "Task Scheduler", on pages 10 to 11.	The description of the claim is unclear. NON-INNOVATIVE		[July-T, 109] [March-T, 90]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Task Scheduler	TSCH	Group-Dependent Security Settings	For a task scheduled for a group of users, the Group-Dependent Security Settings feature of Task Scheduler allows the administrator to specify a subgroup of users the logging on of which will trigger the task. For example, a domain may include users A-Z and it may be desirable to run the task in a particular account (for example, user A) within the group. The administrator has the ability under the Group-Based Security Settings to specify the user or users upon whose logging on the task will run. Thus, each job can be scheduled to run with only the privilege level appropriate for individual users, thereby enhancing system security. Alternative prior art approaches run scheduled jobs as the user scheduling them, leaving unattended jobs running with high security privileges.	July 2005	Group-Dependent Security Settings enhance security by avoiding running jobs with unnecessary security privileges.	Microsoft's Innovation Report: "Task Scheduler", on pages 20 to 21.	The description of the claim is unclear. NON-INNOVATIVE	[PA] Apple: Automator (29 April 2005; http://www.automator.us/; released as a part of MAC O/S 10.4)	[July-T, 110] [March-T, 93]
Task Scheduler	TSCH	Job Interactive Option	The Job Interactive Option feature of Task Scheduler allows a job scheduler to choose whether to run a job in interactive mode, thereby enabling an operator to intervene in the running of jobs as necessary. This allows the administrator to delegate some of the administrator's duties, where appropriate, thereby utilizing human resources more efficiently. In prior task scheduling, tasks that required user interaction could not be delegated by the scheduling user and thus scheduled jobs could only be run in the background. In combination with Scheduling Executables to Run on a Preset Account, the operator's intervention can be confined to the level of privilege appropriate to the operator. System security is therefore not compromised.	July 1993 (Date of claim unclear)	Job Interactive Option enhances efficiency by allowing delegation of more duties by administrators.	Microsoft's Innovation Report: "Task Scheduler", on pages 19 to 20.	The description of the claim is unclear. NON-INNOVATIVE	[PA] Apple: launchctl program (in Darwin 8.0 and Mac O/S 10.4; 29 April 2005; for the case that this unclear claim pertains to Vista)	[July-T, 109] [March-T, 92]
Task Scheduler	TSCH	Missed Run Restart	Scheduled tasks may fail to run from time to time for a variety of reasons. For example, if there is an interruption in the network when a task needs network support, the task will fail. The Missed Run Restart feature of Task Scheduler automatically restarts a task in the event that the task fails.	July 2005	Missed Run Restart enhances efficiency by automatically rerunning tasks that failed to run.	Microsoft's Innovation Report: "Task Scheduler", on pages 12 to 15.	NON-INNOVATIVE	[PA] nnSoft: nnCron Utility (26 February 2003; http://www.nncron.ru; version 1.88) [PA] U.S. Patent 7,093,252: Self-submitting job for testing a job scheduling/submitting software (IBM; 15 August 2006 (Filed 12 April 2000 as 09/547,647))	[July-T, 109] [March-T, 91]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Task Scheduler	TSCH	Scheduling Executables to Run on a Preset Account	Often a scheduling user, such as an administrator, needs to set tasks to be run in the account of a user at a lower security level. Alternative prior art approaches run scheduled jobs at the security level of the user scheduling them. This created security issues by leaving jobs running with a higher security level in an account which is otherwise a lower-security account. The lower security account would often be unattended while running the scheduled task. The Scheduling Executables to Run on a Preset Account innovation of Task Scheduler allows tasks to be run at accounts without granting the user higher privileges than would otherwise be necessary. Scheduling Executables to Run on a Preset Account allows a job to be run in an account set by the scheduling user, such as an administrator, who schedules the job. The Scheduling Executables to Run on a Preset Account permits the scheduler to schedule the task to be run through a user account with a lower security privilege level than the scheduling user's account. This reduces the amount of damage that a malicious user can do if he gets access to the scheduling account.	December 1999	Scheduling Executables to Run on a Preset Account enhances security by avoiding running jobs with unnecessary security privileges.	Microsoft's Innovation Report: "Task Scheduler", on pages 15 to 17.	NON-INNOVATIVE	[PA] Bell Telephone Laboratories: UNIX Programmer's Manual, Seventh Edition, Volume 1 (399; January 1979; http://cm.bell-labs.com/7thEdMan/v7vol1.pdf; set UserID for the cron utility (p. 399), user account (p. 254)) [PA] VisualCron: VisualCron tool (27 July 2004; http://www.visualcron.com/; version 1.0.6) [PA] IBM: IBM LoadLeveler: User's Guide (IBM Publication number ST00-9696; October 1994; see also IBM LoadLeveler for AIX 5L: Using and Administering http://www.ncsa.uiuc.edu/UserInfo/Resources/Hardware/IBMp690/IBM/usr/lpp/LoadL/html/am2ugmst02.html#ToC) [PA] nnSoft: nnCron Utility (26 February 2003; http://www.nncron.ru; version 1.88)	[July-T, 109] [March-T, 91]
Task Scheduler	TSCH	State-Based Scheduling	The State-Based Scheduling feature of Task Scheduler allows a task to be initiated by machine state instead of upon a preset time. When tasks are scheduled for a particular time, the times could be set when the scheduler presumed the system would be in a certain state. For example, tasks might be set at 1:00 a.m. on the assumption that a computer would likely be idle at that time. However, such an assumption may be wrong. If the general assumption was not correct, resources needed by a user may be diverted, reducing the efficiency of the system for the on-line user. Such inefficiency may occur at inopportune times, as the use of the system at unusual hours may indicate need for the computer on a particularly large or important project. Other tasks may have been scheduled on the assumption that a user will be logged on, when in fact a user is not. State-Based Scheduling eliminates these problems. Rather than using time as a proxy for an event, Task Scheduler provides access to an rich set of triggering machine states, which can be detected in the operating system.	December 1999	State-Based Scheduling enhances efficiency by initiating tasks based on machine state instead of time.	Microsoft's Innovation Report: "Task Scheduler", on pages 7 to 9.	NON-INNOVATIVE	[PA] VisualCron: VisualCron tool (27 July 2004; http://www.visualcron.com/; version 1.0.6)	[July-T, 108] [March-T, 89]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Task Scheduler	TSCH	Transferable Task Scheduling	The Transferable Task Scheduling feature of Task Scheduler allows a task to be scheduled for one account and subsequently used for another account, even if on another machine. For example, an administrator can bundle a number of maintenance tasks such as backup, defragmenting, and other tasks in XML and ship to any number of computers to run automatically and without the need for administrative privileges. The configuration file used to schedule the installations can be transferred, for example, by email, to another administrator, who will thus not have to construct his/her own configuration file for the same tasks. This feature enhances the overall efficiency in system maintenance by allowing task schedules and their accompanying XML commands to be packaged and reused for multiple users or accounts and run under preset conditions. Alternative prior art approaches combine many jobs in a single configuration file, making it difficult, if not impossible to transfer schedules for individual jobs.	July 2005	Transferable Task Scheduling enhances portability by packaging each task with its own configurations.	Microsoft's Innovation Report: "Task Scheduler", on pages 21 to 25.	The description of the claim is unclear. NON-INNOVATIVE	[PA] Apple: Automator (29 April 2005; http://www.automator.us/; released as a part of MAC O/S 10.4)	[July-T, 110] [March-T, 93]
Windows Client Certificate Enrolment Protocol	WCCE	Centralized Certificate Template Repository	WCCS consists of a set of DCOM[MS-DCOM] interfaces that allow clients to request various services from a certificate authority (CA). The Protocol enables clients to enroll for certificates that may be based on certificate templates.	December 1999	Centralized Certificate Template Repository effectively makes request requirements available to clients.	Microsoft's Innovation Report: "Windows Client Certificate Enrollment Protocol", on page 7.	NON-INNOVATIVE	[PA] RedHat: RedHat Documentation, Chapter 2. CA: Working with Certificate Profiles (April 1996; http://www.redhat.com/docs/manuals/cert-system/agent/7.2/ch.Working-with-Certificate-Profiles.html; https://www.redaht.com/docs/manuals/cert-system/agent/profiles.htm; http://wp.netscape.com/certificate/v1.0/faq/index.html#1.; This was previously documented by Netscape in " Working with Certificate Profiles", see the second and third link.) [PA] NIST PKI Project Team: Certificate Issuing and Management Components. Protection Profile (36-37 (Section 6.9); 26 January 2001; http://csrc.nist.gov/pki/documents/CIMC_PP_final-corrections_20010126.pdf) [PA] Sun Microsystems: keytool - Key and Certificate Management Tool (2001; http://web.archive.org/web/20030202134922/java.sun.com/products/jdk/1.2/docs/tooldocs/win32/keytool.html)	[March-T, 87]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Windows Client Certificate Enrolment Protocol	WCCE	Combination of WCCE Technologies	The combination of all the WCCE Technologies.	December 1999	Microsoft is not asserting that the WCCE protocol's individual features are innovative in a stand-alone sense. Instead, the WCCE protocol as a whole is novel when the identified features are combined.	Microsoft's Innovation Report: "Windows Client Certificate Enrollment Protocol"	The claimed innovation is the combination of different features belonging to the same protocol. Combining these individual features is an obvious step for a person skilled in the art. NON-INNOVATIVE		[July-T, 111]
Windows Client Certificate Enrolment Protocol	WCCE	Indexed Certificate Authority	WCSS provides a method for a client to request indexed certificate authority properties from the certificate authority. To allow for Indexed Certificate Authority properties, each certificate authority certificate and each CRL has an index. The protocol further provides a method for a client to obtain additional certificate authority properties from the certificate authority.	December 1999	Indexed Certificate Authority properties allow users to collect important information.	Microsoft's Innovation Report: "Windows Client Certificate Enrollment Protocol", on pages 8 to 11.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] Sun Microsystems: keytool - Key and Certificate Management Tool (2001; http://web.archive.org/web/20030202134922/java.sun.com/products/jdk/1.2/docs/tooldocs/win32/keytool.html)	[March-T, 88]
Windows Client Certificate Enrolment Protocol	WCCE	Indexed Certificates and Certificate Requests	WCCS supports the above description of indexed certificates and certificate requests: RequestId, which is an integer value representing identifier for the request; the certificate request being signed; a disposition property that represents the current status of the request (issued, denied, pending, failed); RequesterName, the name of the requestor of the enrollment; the issued certificate (if issued, depending on the disposition status); the SerialNumber of the issued certificate (if issued, depending on the disposition status).	December 1999	Indexed Certificates and Certificate Requests allow users to access information related to certificates.	Microsoft's Innovation Report: "Windows Client Certificate Enrollment Protocol", on page 7.	NON-INNOVATIVE	[PA] RedHat: RedHat Documentation, Chapter 2. CA: Working with Certificate Profiles (April 1996; http://www.redhat.com/docs/manuals/cert-system/agent/7.2/ch.Working-with-Certificate-Profiles.html; https://www.redaht.com/docs/manuals/cert-system/agent/profiles.htm; http://wp.netscape.com/certificate/v1.0/faq/index.html#1.; This was previously documented by Netscape in " Working with Certificate Profiles", see the second and third link.) [PA] Sun Microsystems: keytool - Key and Certificate Management Tool (2001; http://web.archive.org/web/20030202134922/java.sun.com/products/jdk/1.2/docs/tooldocs/win32/keytool.html)	[March-T, 87]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Windows Client Certificate Enrolment Protocol	WCCE	Private Key Archival	WCCS enables a client to submit a private key to a certificate authority for key archival. Before the client submits the private key, it must initialize a secure channel to the certificate authority. To create the secure channel, the client must retrieve a certificate authority key exchange certificate. The certificate authority key exchange certificate is an encryption certificate for the certificate authority that can be used by clients to encrypt private keys. Using a public key, the client encrypts the private key and sends it to the certificate authority. The protocol provides private key archival as part of the certificate enrolment process. The private key is sent to the certificate authority for archival as part of a certificate request. The certificate authority encrypts the private key using a key archival certificate, which is also termed a key recovery certificate.	December 1999	Private Key Archival allows restoration of lost and destroyed keys.	Microsoft's Innovation Report: "Windows Client Certificate Enrollment Protocol", on pages 11 to 12.	NON-INNOVATIVE	[PA] RFC 2527: Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework (March 1999; http://www.ietf.org/rfc/rfc2527.txt)	[March-T, 88]
World Wide Web Distributed Authoring and Versioning Protocol Extensions	WEBDAV	Combining Commands Using the Extension Header	The WebDAV Extension Header protocol groups multiple commands together in a packet header for execution on a remote machine. The protocol will run the commands sequentially and return the result to the end user. It is desirable when faced with multiple commands to issue to a single server to be able to issue those requests as a collection of objects, so that the end user is not waiting for a response from the server before having to issue the next command.	July 2005	Combining Commands Using the Extension Header promotes usability and efficiency by allowing multiple commands to be executed automatically.	Microsoft's Innovation Report, "WebDAV File System Extensions Protocol ; WebDAV Extension: noroot Depth Protocol; WebDAV Extension: MS-Author-Via Protocol", on pages 9 to 11.	NON-INNOVATIVE	[PA] RFC 2518: HTTP Extensions for Distributed Authoring -- WEBDAV (February 1999; http://tools.ietf.org/html/rfc2518) [PA] RFC 2068: Hypertext Transfer Protocol -- HTTP/1.1 (January 1997; http://tools.ietf.org/html/rfc2068)	[July-T, 130-131] [March-T, 106]
World Wide Web Distributed Authoring and Versioning Protocol Extensions	WEBDAV	Combining Commands Using the Lock Header	WebDAV provides the ability to combine commands with the lock command, thereby eliminating an extra command. The semantics of an existing LOCK header have been extended to enable Resource Locking and unlocking capabilities on GET, PUT and POST commands, eliminating the need to send separate messages. Issuing multiple commands with a single command is desirable to an end user so that the end user is not waiting for a response from the server before having to issue the next command.	July 2005	Combining Commands Using the Lock Header promotes usability and efficiency by allowing multiple commands to be executed as one command.	Microsoft's Innovation Report, "WebDAV File System Extensions Protocol ; WebDAV Extension: noroot Depth Protocol; WebDAV Extension: MS-Author-Via Protocol", on pages 11 to 12.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE		[July-T, 131] [March-T, 107]
World Wide Web Distributed Authoring and Versioning Protocol Extensions	WEBDAV	Extended Error Handling	The current errors returned by the HTTP protocol are not sufficient to support all of the possible error conditions that occur in file handling. The extended (more descriptive) error handling mechanism provides the ability to pass on a detailed error description to the end user.	July 2005	Providing users with more descriptive error messages promotes usability and efficiency by allowing quicker analysis of system failures.	Microsoft's Innovation Report, "WebDAV File System Extensions Protocol ; WebDAV Extension: noroot Depth Protocol; WebDAV Extension: MS-Author-Via Protocol", on pages 12 to 15.	NON-INNOVATIVE	[PA] RFC 2034: SMTP Service Extension for Returning Enhanced Error Codes (October 1996; http://tools.ietf.org/html/rfc2034) [PA] RFC 1893: Enhanced Mail System Status Codes (January 1996; http://tools.ietf.org/html/rfc1893)	[March-T, 107]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Windows Group Policy Protocols	WGP	Dynamic Individualized Policy Configuration	Implementing global and mandatory policy settings for users and computers within a domain has presented various problems for administrators. For one, administrators must somehow learn which computers need updated policies as users have differing network log-in practices. For example, many users forget to log off their computers at the end of the day. Other users frequently work on their computers by remotely connecting to the network. As a result, policy updating needs have varied significantly among users. Microsoft's WGP overcomes such difficulties by having each computer maintain a cached list of its GPOs. When a policy refresh or update is triggered, the policy version number of the computer is compared with the policy version number in the list for the same GPO, then the updated GPO is applied to the computer. Rather than needing to historically track which computers need which updated policies, administrators allow clients to dynamically determine the versions of their policies. Microsoft's WGPP enables administrators to dynamically configure computer settings on a per-user basis.	December 1999	Dynamic Individualized Policy Configuration delivers efficiency, security and reliability in applying policies.	Microsoft's Innovation Report: "Windows Group Policy Protocols", on pages 21 to 24.	NON-INNOVATIVE	[PA] Martin-Flatin, Jean-Philippe: Push vs. Pull in Web-Based Network Management, Version 2 (Eidgenössische Technische Hochschule Lausanne, technical report SSC/1998/022; October 1998; http://arxiv.org/ftp/cs/papers/9811/9811027.pd) [PA] RFC 2748: The COPS (Common Open Policy Service) Protocol (January 2000; http://tools.ietf.org/html/rfc2748) [PA] Boyle, Jim et al: The COPS (Common Open Policy Service) Protocol (IETF Draft; 24 February 1999; http://tools.ietf.org/html/draft-ietf-rap-cops-06; The work on this document had begun in September 1998.) [R] Westerinen, Andrea/Bumpus, Winston: The Continuing Evolution of Distributed Systems (IEICE Transactions on Information and Systems, E86-D(11); 2256-2261; November 2003; http://www.dmtf.org/zdata/e86-d_11_2256.pdf)	[July-T, 113-114] [March-T, 70]
Windows Group Policy Protocols	WGP	Multi-platform Group Policy Distribution	A distributed file system is a file system consisting of multiple, independent storage devices instead of a centralized data repository. In contrast, a directory service acts as a central authority for managing network resources and users as objects in a central database. Administrators have been forced to manage policies for computers in one environment separately from the computers in the other environment. For example, administrators have needed to develop separate replication schemes for the two environments. Microsoft's WGP removes that barrier by offering a scalable framework for managing policies for computers anywhere. Rather than storing files in one environment or the other, policy information is divided between the two environments. For example, policies are stored in the distributed file system while metadata concerning the policies can be stored in Active Directory. Policy retrieval time is reduced in comparison to time involved in retrieving the policies in Active Directory.	December 1999	Multi-Platform Group Policy Distribution provides a scalable and efficient framework for distributing policies.	Microsoft's Innovation Report: "Windows Group Policy Protocols", on pages 19 to 21.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] IBM International Technical Support Organization: MVS/ESA OpenEdition DCE: Application Support Servers CICS and IMS (December 1994; http://www.redbooks.ibm.com/redbooks/pdfs/gg244482.pdf) [PA] Legg, S.: LDUP Update Reconciliation Procedures (IETF Draft; 16 February 1999; http://tools.ietf.org/html/draft-ietf-ldup-urp-00) [PA] Popek, Gerald J.: Replication in Ficus Distributed File Systems (IEEE Computer Society Technical Committee on Operating Systems and Application Environments Newsletter 4(3); 24-29; November 1990; http://citeseer.ist.psu.edu/popek90replication.html)	[July-T, 112-113] [March-T, 69]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Windows Remote Registry Protocol	WINREG	Combination of Innovative Features	The combination of features of the WinReg protocol provides additional benefits and innovations that extend beyond the individual innovations discussed above. As one example, the combination of volatile registry keys and access redirection provides significant adaptability - providing for the management of different types of configuration information (i.e., temporary configurations and configuration information for different versions of applications). This flexibility is not found in other alternative technologies in the prior art.	July 1993	The combination of file based registry keys and dynamic establishment of encrypted and unencrypted connections provide a system with improved manageability and adaptability.	Microsoft's Innovation Report: "Windows Remote Registry", on page 26.	The claimed innovation is the combination of different features belonging to the same protocol. Combining these individual features is an obvious step for a person skilled in the art. NON-INNOVATIVE		[July-T, 120] [March-T, 78]
Windows Remote Registry Protocol	WINREG	Dynamically Establishing Encrypted or Unencrypted Connections	Packet privacy prevents malicious users from compromising the security of a computer system. Malicious users attempt to intercept and tamper with messages transmitted between the client and server. Enabling packet privacy encrypts the messages - making it more difficult for a malicious user to modify the contents of the messages. Packet encryption achieves substantial security benefits. The WinReg protocol dynamically addresses both encrypted and non-encrypted operations based on system capabilities. A client may request a connection with packet privacy, which will be enabled if supported by the server. If encryption is not supported, a lower security connection is established.	July 1993	Dynamically Establishing Encrypted or Unencrypted Connections promotes security and adaptability by allowing a secure connection if possible.	Microsoft's Innovation Report: "Windows Remote Registry", on pages 24 to 26.	The description of the claim is unclear. NON-INNOVATIVE		[July-T, 119] [March-T, 77]
Windows Remote Registry Protocol	WINREG	File-Based Registry Keys	The WinReg protocol allows a user to execute a number of configuration changes specified in a file at the same time, i.e., as a batch of changes, rather than forcing a user to execute a number of separate calls to the registry. In particular, the innovation of using File-Based Registry Keys facilitates the management of server configuration information by allowing configuration data to be shared system wide, among kernel, user, and processes. Using the WinReg File-Based Registry Keys, a user can very simply make a number of changes (e.g., additions and modifications) to configuration information in a single file. The file (or handle to the file) is sent to the server registry, which then applies the various changes to the appropriate keys. This innovative mechanism avoids the need to make a number of requests, one for each change or modification, to the registry.	July 1993	Use of File-Based Registry Keys promotes adaptability, manageability, and efficiency by allowing the batching of updates to the registry.	Microsoft's Innovation Report: "Windows Remote Registry", on pages 21 to 24.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] Microsoft: The use of configuration files (March 1983 (MS-DOS), 1987 (Windows 2.0))	[July-T, 117-118] [March-T, 76]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Windows Remote Registry Protocol	WINREG	Volatile Registry Keys	The WinReg protocol achieves the benefits of adaptability and manageability in the use of a registry by giving a user the option of creating Volatile Registry Keys (i.e. keys that store configuration information that is not required to be persistent). A Volatile Registry Key does not survive a reboot, and thus allows a user to make specific modifications to the registry in the form of temporary configuration information, without permanently changing the configuration of a computer system. Volatile Registry Keys also promote efficiency, because they are not persistent. Storing them in memory eliminates the input/output operation of storing them permanently to a disk. Volatile Registry Keys can prove to be valuable when creating a number of temporary configurations for booting a computer system. Technologies that do not provide for the use of Volatile Registry Keys do not allow configuration information to be stored temporarily. Instead, any change to configuration information is stored permanently as part of the registry, until manually deleted.	July 1993	Volatile Registry Keys promote adaptability, manageability, and efficiency by allowing a user to create a temporary configuration.	Microsoft's Innovation Report: "Windows Remote Registry", on pages 19 to 21.	NON-INNOVATIVE	[PA] Ashton-Tate: dBase II (early 1980s; In view of the fact that the registry is a database, it is felt that this example is sufficient to be quoted as prior art.)	[July-T, 115-116] [March-T, 75]
Windows Print System Remote Protocol	WINSPL	Asynchronous RPC Print Calls	When an application prints a document, the printing commands from the application eventually must be translated to the raw data that a printer can execute. In certain alternative prior art approaches, the printing commands are translated directly to the raw data format and sent to a spool file, which later may be de-spooled to a printer. The raw data format is device-specific and must be sent to the target printer, and if the target printer is unavailable, the whole process of translation and spooling often must be repeated for a different printer. Raw data files also tend to be very large, and translation into a raw data format tends to be time-consuming. WINSPL overcomes those problems by using a device-independent data format to spool print jobs. EMF files are typically smaller than raw data files and are less time-consuming to translate. In addition, a document only needs to be spooled once and can be subsequently de-spooled to send to different printers.	May 2006	Asynchronous RPC Print Calls provide efficiency by reducing application program hanging.	Microsoft's Innovation Report: "Windows Print System Remote, Print Asynchronous Notification and Print Asynch RPC", on pages 8 to 9.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE		[July-T, 122] [March-T, 131]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Windows Print System Remote Protocol	WINSPL	Point-and-Print User Interface	IThe Microsoft's Point-and-Print User Interface automatically installs the printer specified in a printing request on the requesting workstation if the printer has not yet been installed. This is accomplished at least in part by using the "Environment" pointer, which specifies the operating system of the requesting workstation, in the printing request.	July 1996	Microsoft's Point-and-Print feature has advantages over other technologies as it does not require user intervention.	Microsoft's Innovation Report: "Windows Print System Remote, Print Asynchronous Notification and Print Asynch RPC"	NON-INNOVATIVE	[PA] CUPS project: Common Unix Printing System (9 June 1999; http://www.cups.org; http://www.linuxtoday.com/news_story.php3?ltsn=1999-06-09-014-10-NW-SM)	[July-T, 121]
Windows Print System Remote Protocol	WINSPL	Request Sender-Specific Notification	In a network with multiple users and shared distributed resources such as printers, it is desirable for a user who issues a printing request to be able to know the status of the printing job without having to be physically next to the printer. For example, a user requesting a printing job may not be aware that the printer that received the job is out of paper or low on toner, and it would be useful for the user to receive notifications of such conditions. In certain cases, notification may concern private or security information that is not to be viewed by another user. The Microsoft Request Sender-Specific Notification innovation not only enables notification of printer conditions but also ensures that only the user who requested the notification receives it.	July 2005	Request Sender-Specific Notification provides usability and security by alerting users of printer conditions and by restricting notification to the request sender.	Microsoft's Innovation Report: "Windows Print System Remote, Print Asynchronous Notification and Print Asynch RPC", on pages 9 to 10.	NON-INNOVATIVE	[R] Network Printing Alliance: The Network Printing Alliance Protocol (NPAP) (1993; http://www.undocprint.org/formats/printer_control_languages/npap; Was approved in 1997 as IEEE Standard 1284.1 (TIP/SI) Standard for Information Technology for Transport Independent Printer/Scanner Interface. (http://www.undocprint.org/formats/printer_control_languages/tipsi)) [PA] Isaacson, S. et al: Internet Printing Protocol/1.1: Event Notification Specification (IETF Draft; 25 August 1999; http://www3.tools.ietf.org/html/draft-ietf-ipp-not-spec-00)	[July-T, 122-123] [March-T, 131]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Workstation Service Remote Protocol	WSRP	Customizable Buffer Size and "Resume" Handle	WSRP is designed for remotely querying and configuring certain aspects of an SMB network redirector on a remote computer. Examples of information that can be retrieved include information about the users currently active on the remote computer and the information about the transport protocols currently enabled on the remote computer. At least a portion of an answer to a query is retrieved into a buffer. WSRP efficiently uses a customizable buffer size and incorporating an efficient means to identify and retrieve data exceeding the buffer size. The querying application can specify a customized buffer size to suit the anticipated maximum size of the requested data. When the querying application issues a query with a specified buffer size that is smaller than the size of the requested data, a non-zero "resume" handle is generated to mark the location of the end of the data block that is sent to the buffer. This enables the querying application to issue a subsequent query acquiring a block of data starting where the last query left off. The "resume" handle may be employed repeatedly until all data is retrieved. This allows all of the requested data to be efficiently retrieved in multiple querying cycles. WSRP also provides for the querying application to issue a query with a buffer size that is large enough to retrieve all of the requested data in a single query. Moreover, with WSRP, to the extent the system utilizes a smaller number of users or transport protocols, the buffer size may be customized to retrieve the acquired information in fewer steps or even a single step. This allows a smaller network to use a smaller buffer when desired, without the need for preserving a large buffer in the event the network environment changes such that more information about logged-on users or transport protocols must be acquired. By permitting the querying application to choose whether to set a specific buffer size WSRP enables the user to easily adjust the querying operations to optimize the system performance.	July 1993	Customizable Buffer Size and "Resume" Handles provide extensibility to dynamically address the number of users and protocols supported by a system.	Microsoft's Innovation Report: "Workstation Service Remote", on pages 7 to 8.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[PA] Kernighan, Brian W./Ritchie, Dennis M.: The C Programming Language, second edition (Prentice-Hall; 1989; http://www.cs.bell-labs.com/cm/cs/cbook/) [PA] Forsberg, Chuck: The ZMODEM Inter Application File Transfer Protocol (14 October 1988; http://timeline.textfiles.com/1988/10/14/1/FILES/zmodem.txt) [PA] Stonebraker, Michael et al: The design and implementation of INGRES (ACM Transactions on Database Systems 1(3); 189-222; September 1976)	[March-T, 65-66]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Windows Update Service Protocol	WUSP	Automatic Driver Installation	WUSP allows finding and installing the correct driver in the case of a driver fault. It also obtains and installs the driver automatically without requiring user intervention.	July 2005	Automatic Driver Installation promotes system stability and usability by finding and installing appropriate drivers without user intervention in the event of a driver fault.	Microsoft's Innovation Report: "Windows Update Services:Client-Server", on pages 15 to 18.	The claim describes something which was obvious to somebody skilled in the art. NON-INNOVATIVE	[R] Microsoft: Toaster Installation Package (MSDN; April 2005) [R] Jensen, Robert: Configuring an ATi card using YUM and the LIVNA Repository (2007; http://fedorasolved.org/video-solutions/ati-yum-livna/; illustration, not prior art)	[July-T, 127-128] [March-T, 72]
Windows Update Service Protocol	WUSP	Management of Desired State	A client updates its own software when such updates become available by pulling the desired updates, file-by-file, from a server. A client uses WUSP to periodically poll a server for approved updates. The client receives a reduced list of possible updates from the update service from which the client can select desired updates. The client retrieves the desired updates by sending requests to obtain the individual update files. In one prior design approach, the update service must retain state information about each client in order to push update files onto the client. In another prior design approach, the client must request files over a dedicated connection, which limits the number of clients the service is capable of handling. WUSP enables large numbers of clients (e.g., 400 million) to access the update service over a short period of time, by enabling the clients to pull desired update files from one or more servers. A server no longer must retain the update state of each client and fewer system resources must be dedicated for providing the updates to the clients.	July 2005	Management of Desired State promotes scalability, system stability, and usability by pulling appropriate updates from a server on a file-by-file basis. It is innovative in combination with other WUSP technologies.	Microsoft's Innovation Report: "Windows Update Services:Client-Server", on pages 18 to 21.	The claimed innovation is the combination of different features belonging to the same protocol. Combining these individual features is an obvious step for a person skilled in the art. NON-INNOVATIVE	[PA] Brown, Robert G./Pickard, Jonathan: YUM (Yellowdog Updater, Modified) HOWTO (April 2003; http://www.phy.duke.edu/~rgb/General/yum_HOWTO/yum_HOWTO/yum_HOWTO.html)	[July-T, 129] [March-T, 73]

Protocol		Technology	Description of the technology	Date of claim	Claimed benefit	Reference in Microsoft's filing	Assessment	Prior Art	References
Windows Update Service Protocol	WUSP	Scalability by Reducing Download Size	There is significant complexity in that each client may wish to download multiple updates of varying sizes. In some cases, one or more of these updates must be installed before the other updates can be installed, i.e., hierarchical prerequisites. In other cases, some updates are more important than others - e.g., security patches versus new software programs. In a prior design approach, a client would download all possible updates in the same session. Large downloads would tie up the resources of the server and could inhibit other users from obtaining important updates quickly. WUSP prioritizes updates and provides access to less than all possible updates in a given session. First, a determination is made as to which updates are available to a client. Next, the list of available updates is reduced based on the priority of an update, whether the update's prerequisites have been met, whether the update is a prerequisite for another update, and other such rules. WUSP also enables more users to more quickly access security updates.	July 2005	Such selective update information transfer improves processing efficiency by pruning unnecessary or less important content in each download session.	Microsoft's Innovation Report: "Windows Update Services: Client-Server", on pages 7 to 15.	NON-INNOVATIVE	[PA] PocketSoft: RTPatch Software (commericialised since 1991; http://www.rtpatch.com/rtpatch.htm) [PA] Brown, Robert G./Pickard, Jonathan: YUM (Yellowdog Updater, Modified) HOWTO (April 2003; http://www.phy.duke.edu/~rgb/General/yum_HOWTO/yum_HOWTO/yum_HOWTO.html)	[July-T, 126-127] [March-T, 71]