

[MS-OFCGLOS]: Microsoft Office Master Glossary

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that may cover your implementations of the technologies described in the Open Specifications. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, a given Open Specification may be covered by Microsoft [Open Specification Promise](#) or the [Community Promise](#). If you would prefer a written license, or if the technologies described in the Open Specifications are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **Trademarks.** The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit www.microsoft.com/trademarks.
- **Fictitious Names.** The example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications do not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments you are free to take advantage of them. Certain Open Specifications are intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it.

Revision Summary

Date	Revision History	Revision Class	Comments
04/04/2008	0.1		Initial Availability.
06/27/2008	1.0	Major	Added technical content for protocol documentation.
08/15/2008	1.01	Editorial	Revised and edited the technical content.
10/06/2008	1.02	Major	Added technical content for protocol documentation.
01/16/2009	1.03	Editorial	Updated the Intellectual Property Rights Notice.
03/18/2009	1.04	Major	Added technical content for protocol documentation.
07/13/2009	1.05	Major	Revised and edited the technical content.
08/28/2009	1.06	Editorial	Revised and edited the technical content.
11/06/2009	1.07	Major	Revised, edited and added technical content.
02/19/2010	1.08	Major	Revised, edited and added technical content.
03/31/2010	1.09	Major	Revised, edited and added technical content.
04/30/2010	1.10	Major	Revised, edited and added technical content.
06/07/2010	1.11	Minor	Updated the technical content.
06/29/2010	1.12	Minor	Clarified the meaning of the technical content.
07/23/2010	1.13	Minor	Clarified the meaning of the technical content.
09/27/2010	1.14	Minor	Clarified the meaning of the technical content.
11/15/2010	1.15	Minor	Clarified the meaning of the technical content.
12/17/2010	1.15	No change	No changes to the meaning, language, or formatting of the technical content.
03/18/2011	1.16	Minor	Clarified the meaning of the technical content.
06/10/2011	1.17	Minor	Clarified the meaning of the technical content.
01/20/2012	1.18	Minor	Clarified the meaning of the technical content.
04/11/2012	1.18	No change	No changes to the meaning, language, or formatting of the technical content.
07/16/2012	2.0	Major	Significantly changed the technical content.
10/08/2012	2.1	Minor	Clarified the meaning of the technical content.
02/11/2013	2.2	Minor	Clarified the meaning of the technical content.
07/30/2013	2.3	Minor	Clarified the meaning of the technical content.

Date	Revision History	Revision Class	Comments
11/18/2013	2.4	Minor	Clarified the meaning of the technical content.
02/10/2014	2.5	Minor	Clarified the meaning of the technical content.
04/30/2014	2.5	No change	No changes to the meaning, language, or formatting of the technical content.
07/31/2014	2.6	Minor	Clarified the meaning of the technical content.
10/30/2014	3.0	Major	Significantly changed the technical content.

Table of Contents

1	Non-Alphanumeric	6
2	0-9	7
3	A	8
4	B	21
5	C.....	28
6	D	51
7	E.....	67
8	F.....	74
9	G	83
10	H	87
11	I	91
12	J	97
13	K	98
14	L.....	100
15	M.....	105
16	N	115
17	O	120
18	P.....	127
19	Q	140
20	R	142
21	S.....	155
22	T.....	181
23	U	190
24	V	195
25	W	198
26	X	203
27	Y.....	205
28	Z.....	206

29 Change Tracking..... 207

1 Non-Alphanumeric

2 0-9

101 Progress Report: A response that indicates the progress of a **SIP request**.

200 OK: A **response** to indicate that the **request** has succeeded.

202 Accepted: A response that indicates that a request was accepted for processing.

3-D Phong shading: A shading algorithm that is used to apply shading to 3-D charts. The algorithm interpolates color between points on the surface of a chart to give a smooth 3-D appearance.

403 Forbidden: A response that indicates that a protocol server understood but denies a request.

88 object class: An **object class** as specified in the X.500 directory specification ([\[X501\]](#) section 8.4.3). An **88 object class** can be instantiated as a new **object**, like a **structural object class**, and on an existing **object**, like an **auxiliary object class**.

3 A

A1: A **reference style** in which each **column** (2) is identified sequentially from left-to-right with a letter or series of letters in alphabetical order. Column headings are ordered A-Z, then AA-AZ, BA-BZ... ZA-ZZ, AAA-AAZ, and so forth. Each row is numbered sequentially from the top down.

absolute path: A string that identifies the location of a file and that begins with a drive identifier and root directory or network share and ends with the complete file name. Examples are C:\Documents\Work\example.txt and \\netshare\Documents\Work\example.txt.

absolute reference: A reference to a fixed location on a **sheet** (1). An absolute reference always refers to the same range, even if the formula that contains it is moved or copied to a new location.

absolute space: An area of a drawing that occupies an entire document or page. The value for absolute space is typically expressed in **English Metric Units (EMUs)**, but it can be defined by the host application.

absolute URI: An absolute **Uniform Resource Identifier (URI)**, as described in [\[RFC3986\]](#).

absolute URL: The full Internet address of a page or other World Wide Web resource. The absolute URL includes a protocol, such as "http," a network location, and an optional path and file name — for example, <http://www.treyresearch.net/>.

Abstract Syntax Notation One (ASN.1): A notation to define complex data types to carry a message, without concern for their binary representation, across a network. **ASN.1** defines an encoding to specify the data types with a notation that does not necessarily determine the representation of each value. **ASN.1** encoding rules are sets of rules used to transform data that is specified in the **ASN.1** language into a standard format that can be decoded on any system that has a decoder based on the same set of rules. **ASN.1** and its encoding rules were once part of the same standard. They have since been separated, but it is still common for the terms **ASN.1** and **Basic Encoding Rules (BER)** to be used to mean the same thing, though this is not the case. Different encoding rules can be applied to a given **ASN.1** definition. The choice of encoding rules used is an option of the protocol designer. ASN.1 is described in the following specifications: [\[ITUX660\]](#) for general procedures; [\[ITUX680\]](#) for syntax specification; [\[ITUX690\]](#) for the **Basic Encoding Rules (BER)**, Canonical Encoding Rules (CER), and Distinguished Encoding Rules (DER) encoding rules; and [\[ITUX691\]](#) for the **Packed Encoding Rules (PER)**. Further background information on ASN.1 is also available in [DUBUISSON].

abstract type: A type used in this specification whose representation need not be standardized for interoperability because the type's use is internal to the specification. See **concrete type**.

accelerator key: Any combination of keys that are pressed simultaneously to run a command.

access control entry (ACE): An entry in an **access control list (ACL)** that contains a set of user rights and a **security identifier (SID)** that identifies a principal for whom the rights are allowed, denied, or audited.

access control list (ACL): A list of **access control entries (ACEs)** that collectively describe the security rules for authorizing access to some resource; for example, an object or set of objects.

access protocols: A set of protocols that are supported by proxies to enable protocol clients and protocol servers to communicate with and share proxy services. A single proxy can support

multiple proxy protocols, such as an **HTTP proxy** that is configured to support **HTTP** with proxy headers, secure tunnel proxy, and SOCKS.

access URL: An internal **Uniform Resource Locator (URL)** that is used by a **crawler** to identify and gain access to an item.

AccessChecker: A type of **MethodInstance** that can be called to retrieve the permissions that the calling **security principal** (2) has for each of a collection of EntityInstances identified by the specified EntityInstanceIds.

account: (1) A collection of data and settings for a SharePoint Workspace or Groove identity that represents a user. This includes shared spaces, messages, and preferences that are associated with a user's identity. An account can reside on one or more devices.

(2) A **user** (including machine account), **group**, or **alias** object. Also a synonym for security principal or principal.

account configuration code: A unique code that is generated by a management server. It is used to bind an identity to a member of a management server.

account key: A secret key that is shared between a relay server and a client account for **account authentication** (2). A protocol client generates this key when it creates a new account, and then registers this key on a relay server through a registration sequence. The relay server uses this key to authenticate the account and enable the protocol client to retrieve **identity-targeted messages** from the server.

account URL: A unique identifier for an **account**, as described in [\[RFC3986\]](#).

accounting: Information gathered and maintained by the **management service** about the runtime behavior of processes. The **management service** provides an accounting state switch with two settings: enabled and disabled. When enabled, accounting information is gathered and persisted across invocations of the **management service**. Accounting information gathered by the **management service** on one computer can be persisted by the **management service** on a different computer. When the accounting state is disabled, no accounting data is gathered or persisted.

acknowledgment (ACK): A signal passed between communicating processes or computers to signify successful receipt of a transmission as part of a communications protocol.

action: (1) The smallest unit of work in a workflow system. An action can contain one or more tasks that define work that **actors** need to do. Actions are deployed and registered in the workflow system to be activated by protocol client users.

(2) A unit of work that can be performed by a workflow and is typically defined in a workflow markup file.

(3) A discrete operation that is executed on an incoming **Message object** when all **conditions** in the same **rule** (4) are TRUE. A rule contains one or more actions.

(4) A string that is returned as part of a GetAction response in the Desired State Configuration Pull Model Protocol [MS-DSCPM].

(5) A command exposed by a **service** which takes one or more input or output arguments and which may have a return value. For more information, see [\[UPNPARCH1.1\]](#) sections 2 and 3.

(6) A remote procedure call from the control point to a particular service on the device.

(7) A command that is exposed by a **service**, as defined in [\[UPNPARCH1.1\]](#) section i.7.

(8) An interactivity event in a report, such as a hyperlink, bookmark link, or drillthrough link, that is associated with an item in a report.

(9) A business rule argument that determines what occurs when the business rule is run at validation time.

(10) An OLAP object, such as a cube, dimension, and cell, that has an action associated with it, so that a user can perform that action when browsing OLAP data. For example, a user can jump to a URL, execute a command, or drill through to data.

Action: A type of **MetadataObject** that represents a URL that triggers the display or manipulation of data related to an Entity or EntityInstance. Actions are contained by an Entity. Actions contain **ActionParameters**.

action instance: The runtime instance of a specific **action** (1). Action instances are building blocks for an **activity flow**. Several action instances can be chained together to form an activity flow, and multiple action instances of the same action can exist in a single activity flow.

ActionParameter: A type of **MetadataObject** that defines how to parameterize the URL of an **Action** with specific data about an EntityInstance. ActionParameters are contained by Actions.

activation: (1) An operation that creates a new **action instance**.

(2) In **COM**, a local mechanism by which a client provides the **CLSID** of an **object class** (3) and obtains an **object** (3), either an **object** from that **object class** or a **class factory** that is able to create such **objects**.

(3) In the **DCOM** protocol, a mechanism by which a client provides the **CLSID** of an **object class** (4) and obtains an **object** (4), either from that **object class** or a **class factory** that is able to create such **objects**. For more information, see [\[MS-DCOM\]](#).

(4) The process of creating a server object.

active cell: The cell that is currently selected in a worksheet.

Active Directory: A general-purpose network **directory service**. **Active Directory** also refers to the Windows implementation of a **directory service**. **Active Directory** stores information about a variety of **objects** in the network. Importantly, user accounts, computer accounts, groups, and all related credential information used by the Windows implementation of **Kerberos** are stored in **Active Directory**. See also **Lightweight Directory Access Protocol (LDAP)** versions 2 and 3, **Kerberos**, and **DNS**. For more information, see [\[MS-AUTHSOD\]](#) section 1.1.1.5.2 and [\[MS-ADTS\]](#). **Active Directory** is either deployed as **Active Directory Domain Services (AD DS)** or **Active Directory Lightweight Directory Services (AD LDS)**. [\[MS-ADTS\]](#) describes both forms.

Active Directory account creation mode: A type of account creation mode that retrieves and uses user accounts in a specific AD DS **organizational unit**.

Active Directory Domain Services (AD DS): An operating system **directory service (DS)** implemented by a **domain controller (DC)**. The **DS** provides a data store for **objects** that is distributed across multiple **DCs**. The **DCs** interoperate as peers to ensure that a local change to an **object** replicates correctly across **DCs**. For more information, see [\[MS-AUTHSOD\]](#) section 1.1.1.5.2. For information about product versions, see [\[MS-ADTS\]](#).

Active Directory Lightweight Directory Services (AD LDS): A **directory service (DS)** implemented by a **domain controller (DC)**. The most significant difference between **AD LDS** and **Active Directory Domain Services (AD DS)** is that **AD LDS** does not host **domain naming contexts (domain NCs)**. A server can host multiple **AD LDS DCs**. Each **DC** is an independent **AD LDS** instance, with its own independent state. **AD LDS** can be run as an operating system **DS** or as a directory service provided by a standalone application (ADAM). For more information, see [MS-ADTS].

Active Directory partition: A synonym for naming context (NC) replica.

Active Directory Service Interfaces (ADSI): A directory service model and a set of Component Object Model (COM) interfaces. ADSI enables Windows applications and AD DS clients to gain access to several network directory services, including AD DS.

active selection: The current selection of cells, rows, or columns that includes the **active cell** in a datasheet.

active sheet: The sheet that is currently selected.

ActiveX control: A reusable software control, such as a check box or button, that uses ActiveX technology and provides options to users or runs macros or scripts that automate a task. See also **ActiveX object**.

ActiveX Data Objects (ADO): A data access interface that connects to, retrieves, manipulates, and updates data in **Object Linking and Embedding (OLE)** database-compliant data sources.

ActiveX object: An object that is supplied by a component that supports automation.

activity: (1) An object that stores information about either an **action** (1) or an **activity model**.

(2) A type of event, such as "In a meeting," that provides information about the availability and status of a **presentity**.

(3) A synchronization boundary; ORPC calls to objects within the boundary are serialized based on their causality identifiers.

(4) Used as specified in [\[C706\]](#) section 9.5.

activity flow: A running instance of a workflow that consists of a sequence of **action instances** and **activity model** instances. Action instances and activity model instances can be sequenced in any order to create a single activity flow.

activity model: A predefined sequence of **actions** (1).

ActivityTrackingFilter: A **FilterDescriptor** type that is used when querying a line-of-business (LOB) system. Its value specifies a **GUID** for the current operation.

actor: A person or process that starts or participates in an **activity flow**. An actor can be an initiator or a target.

AD LDS: See **Active Directory Lightweight Directory Services (AD LDS)**.

adapter: The hardware that connects to a particular network segment. A bound LAN card is one example of an **adapter**. Similarly, a computer with two modems, each capable of connecting to a remote network, has two adapters, one to represent each modem.

add-in: Supplemental functionality that is provided by an external application or macro to extend the capabilities of an application.

add-in function: A worksheet function that is provided by an **add-in**, instead of being built-in.

address book: A collection of **Address Book objects**, each of which are contained in any number of **address lists**.

address book contact: A user, **contact** (2), or group object that is obtained from AD DS, including a subset of the AD DS attributes that are associated with the object, and is stored in an address book file.

address book file: A file that contains a set of **address book contact** records.

Address Book object: An entity in an **address book** that contains a set of **attributes** (1), each attribute with a set of associated values.

Address Book Server (ABS): A component that produces **address book files** on a daily basis.

address list: A collection of distinct **Address Book objects**.

address-of-record: A **Session Initiation Protocol (SIP) URI** that specifies a domain with a location service that can map the URI to another URI for a user, as described in [\[RFC3261\]](#).

adjacent cell: A cell that is in the same row as and adjoins the current cell in a worksheet.

adjust handle: A user interface control that is located on an object frame and is used to increase or decrease the size of that object.

Advanced Encryption Standard (AES): A block **cipher** that supersedes the **Data Encryption Standard (DES)**. **AES** can be used to protect electronic data. The AES algorithm can be used to encrypt (encipher) and decrypt (decipher) information. **Encryption** converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called **plaintext**. AES is a symmetric cipher, meaning that the same **key** is used for the **encryption** and decryption operations. It is also a block cipher, meaning that it operates on fixed-size blocks of **plaintext** and ciphertext, and requires the size of the **plaintext** as well as the ciphertext to be an exact multiple of this block size. AES is specified in [\[FIPS197\]](#).

Advanced Systems Format (ASF): An extensible file format that is designed to facilitate streaming digital media data over a network. This file format is used by Windows Media.

AES Counter Mode: A type of counter-mode encryption that generates encryption key streams by using **Advanced Encryption Standard (AES)** cipher and successive integers.

after event: An event whose handler runs only after the action that raised the event is complete. Unlike a before event, an after event handler cannot cancel the action that caused the event. See also **before event**.

agent: See **endpoint** (5).

aggregatable server: A **COM server** that can be contained by another **COM server** and can allow its **interfaces** to be used as if they were defined by the containing **server**.

aggregation: (1) A mechanism for reusing objects. The outer object exposes interfaces from one or more inner objects as if they were implemented on the outer object itself.

(2) An operation in which multiple instances of one or more dependent **categories** (4), which are typically published by different Session Initiation Protocol (SIP) clients of the same user, are processed to produce an instance of a category. After this category instance is created, it can be published to multiple containers and notified to subscribers in the same way as any other category.

aggregation function: A function, such as sum or average, that appears in the total row of a table and is used to summarize data.

Aggressive Nomination: The process of selecting a valid **candidate pair** for media flow by sending **Simple Traversal of UDP through NAT (STUN)** binding requests that include the flag for every STUN binding request such that the first candidate pair that is validated is used for media flow.

alert: (1) An **Internet message** that is sent to subscribers automatically to notify them when user-defined criteria are met. Alerts are generated automatically when items such as documents, webpages, list items, sites, or other resources on a server are changed.

(2) A message that is passed to a protocol client to notify it when specific criteria are met.

alert metadata: The values that are contained in the X-headers of an **alert** (1).

alert subscription: A request to receive an **Internet message** automatically when user-defined criteria are met. Such messages are generated automatically when items such as documents, webpages, list items, sites, or other resources on a server are changed.

alias: (1) An alternate name that can be used to reference an object or element.

(2) A simple identifier that is typically used as a short name for a **namespace**.

(3) A **group** (1) that is local to a particular machine (as opposed to a **group** that has security permissions and settings for the entire **domain**).

ALL: See **OLAP All member**.

alternate startup directory: A secondary location that stores files to be opened by an application when the application starts.

American National Standards Institute (ANSI) character set: A **character set** (1) defined by a **code page** approved by the American National Standards Institute (ANSI). The term "ANSI" as used to signify Windows code pages is a historical reference and a misnomer that persists in the Windows community. The source of this misnomer stems from the fact that the Windows code page 1252 was originally based on an ANSI draft, which became International Organization for Standardization (ISO) Standard 8859-1 [\[ISO/IEC-8859-1\]](#). In Windows, the ANSI character set can be any of the following code pages: 1252, 1250, 1251, 1253, 1254, 1255, 1256, 1257, 1258, 874, 932, 936, 949, or 950. For example, "ANSI application" is usually a reference to a non-**Unicode** or code-page-based application. Therefore, "ANSI character set" is often misused to refer to one of the character sets defined by a Windows code page that can be used as an active system code page; for example, character sets defined by code page 1252 or character sets defined by code page 950. Windows is now based on **Unicode**, so the use of ANSI character sets is strongly discouraged unless they are used to interoperate with legacy applications or legacy data.

Analysis Services: The abbreviated name for Microsoft SQL Server Analysis Services, which is used to create and maintain multidimensional data that is sent to client applications in response to queries. Also referred to as Online Analytical Processing (OLAP) server.

ancestor: (1) A PivotTable member that is above the current PivotTable member in a hierarchy.

(2) In a tree structure, an element from which other elements inherit attributes

(3) A record that contains or is contained in another record.

anchor: (1) A set of qualifiers and quantifiers that specifies the location of an element or object within a document. These values are typically relative to another element or known location in the document, such as the edge of a page or margin.

(2) An opaque data element generated by an **update server** to identify the occurrence of a software **update**-related event in a manner that distinguishes temporally separate occurrences of the event.

anchor content source: A **content source** that is used to import the **anchor text** from links between items into the **full-text index catalog**.

anchor crawl: A process in which **anchor text** from links between items is added to a **full-text index catalog**.

anchor text: The text that is included with a hyperlink to describe the target content of a hyperlink.

animation: A record of synthetic, successive still images that produce an illusion of movement when played back.

anonymous access: A mechanism that does not require users to specify a user name or password for **authentication** (1).

anonymous authentication: An **authentication mode** in which neither party verifies the identity of the other party.

anonymous user: A user who presents no credentials when identifying himself or herself. The process for determining an anonymous user can differ based on the authentication protocol, and the documentation for the relevant authentication protocol should be consulted.

answer: A message that is sent in response to an **offer** that is received from an offerer.

anti-moniker: A Component Object Model (COM) object that is the inverse of a simple **moniker** and has no internal structure; it is the inverse of a COM implementation of a file, an item, or a pointer moniker. An anti-moniker that is composed to the right of a file moniker, item moniker, or pointer moniker composes to nothing.

app: (1) See **web application** (1).

(2) See **app for Office**.

(3) A set of instructions that a computer uses to perform a specific task, such as word processing, accounting, or data management.

(4) See **app for SharePoint**.

app for Office: A cloud-enabled app that integrates rich, scenario-focused content and services into an Office application or equivalent protocol client.

app for SharePoint: A cloud-enabled software module that uses HTML, JavaScript, or other industry-standard web technologies, in addition to possible server components, to integrate rich, scenario-focused content and services into SharePoint.

app host header name: A unique name assigned to an **app instance**.

app instance: An instantiation of an **app** on a specific site.

app package: An implementation-specific file that specifies an **app**.

app principal: Designates an authenticated entity that is not a user.

app product identifier: A unique designation that is shared by all versions of an **app**.

application: A participant that is responsible for beginning, propagating, and completing an atomic transaction. An application communicates with a transaction manager in order to begin and complete transactions. An application communicates with a transaction manager in order to marshal transactions to and from other applications. An application also communicates in application-specific ways with a resource manager in order to submit requests for work on resources.

application identifier: (1) A unique integer that identifies a protocol client application.

(2) A string that is used to look up information in a single sign-on (SSO) database.

(3) A globally unique identifier (GUID) that uniquely identifies a **game**.

application manifest: An **XML** file that describes the contents and requirements for a **deployment package** (2).

application NC: A specific type of **naming context (NC)**, or an instance of that type, that supports only full replicas (no partial replicas). An **application NC** cannot contain **security principal objects**. An **application NC** can contain **dynamic objects**. A **forest** can have zero or more **application NCs**. Application NCs do not appear in the **global catalog (GC)**. The root of a **domain NC** is an object of **class** domainDns.

application server: A computer that provides infrastructure and services for applications that are hosted on a server farm.

Application Sharing Multipoint Control Unit (ASMCU): A **Multipoint Control Unit (MCU)** that supports application sharing conferencing.

approval line: A sequence of approval participants in an approval workflow.

archive: The Fax Archive Folder, as described in section 3.1.1.

array: A **Remoting Type** that is an ordered collection of values. The values are identified by their position and position is determined by a set of integer indices. The number of indices required to represent the position is called the Rank of the **Array**. An **Array** is part of the **Remoting Data Model** and also specifies the **Remoting Type** of its items. For more information, [MS-NRTP] section 3.1.1.

array formula: A formula that performs multiple calculations on one or more sets of values, and then returns either a single result or multiple results. Array formulas are enclosed in braces ({}) and are entered by pressing CTRL+SHIFT+ENTER.

ascending order: A sort order in which text strings are arranged in alphabetical order, numerical values are arranged from smallest to largest, and dates and times are arranged from oldest to newest.

ASCII: The American Standard Code for Information Interchange (ASCII) is an 8-bit character-encoding scheme based on the English alphabet. ASCII codes represent text in computers,

communications equipment, and other devices that work with text. ASCII refers to a single 8-bit ASCII character or an array of 8-bit ASCII characters with the high bit of each character set to zero.

ASN.1: Abstract Syntax Notation One. ASN.1 is used to describe Kerberos datagrams as a sequence of components, sent in messages. ASN.1 is described in the following specifications: [\[ITUX660\]](#) for general procedures; [\[ITUX680\]](#) for syntax specification, and [\[ITUX690\]](#) for the Basic Encoding Rules (BER), Canonical Encoding Rules (CER), and **Distinguished Encoding Rules (DER)** encoding rules.

ASP.NET: A web server technology for dynamically rendering HTML pages using a combination of HTML, Javascript, CSS, and server-side logic. For more information, see [\[ASPNET\]](#).

ASP.NET control: A server-side component that encapsulates user interface and related functionality. An ASP.NET server control derives directly or indirectly from the System.Web.UI.Control class. The superset of ASP.NET server controls includes web server controls, HTML server controls, and ASP.NET mobile controls.

assembly: (1) A collection of one or more files that is versioned and deployed as a unit. An assembly is the primary building block of a .NET Framework application. All managed types and resources are contained within an assembly and are marked either as accessible only within the assembly or as accessible from code in other assemblies. Assemblies also play a key role in security. The code access security system uses information about an assembly to determine the set of permissions that is granted to code in the assembly.

(2) A managed application module containing class metadata and managed code as an object in SQL Server, against which common language runtime (CLR) functions, stored procedures, triggers, user-defined aggregates, and user-defined types can be created in SQL Server.

assembly name: The name of a collection of one or more files that is versioned and deployed as a unit. See also **assembly**.

association: A named independent relationship between two EntityType definitions. Associations in the **Entity Data Model (EDM)** are first-class concepts and are always bidirectional. Indeed, the first-class nature of associations helps distinguish the **EDM** from the relational model. Every association includes exactly two association ends.

Association: A **MethodInstance** that enables the traversal and manipulation of a data model relationship between a set of source **Entities** and a single destination Entity. An Association can retrieve, associate, and disassociate EntityInstances of a destination Entity if given EntityInstances of other source Entities.

association form: A form that provides parameters for a **workflow association**.

AssociationGroup: A **MetadataObject** that provides a logical grouping of **AssociationReferences**. All of the **Associations** that are identified by AssociationReferences in the group operate on a single physical mapping of source **EntityInstances** to destination EntityInstances in a line-of-business (LOB) system. All AssociationReferences in the group have the same AssociationReference sources and destinations, and collectively define the source and destination **Entities** of the AssociationGroup.

AssociationNavigator: A type of **MethodInstance** that can be called to retrieve destination **EntityInstances** that are associated with a single specified EntityInstance for each of the sources of the specified **Association**.

AssociationReference: An entry in an **AssociationGroup** that refers to an **Association**. The sources of the AssociationReference are the sources of the referenced Association, and the

destination of the AssociationReference is the destination of the referenced Association. The opposite is true if the AssociationReference is defined to be a reverse reference, for Associations with one source Entity.

Associator: A type of **MethodInstance** that can be called to associate the specified, destination EntityInstance with a single specified EntityInstance for each of the sources of the specified **Association**.

async delta: A delta that is sent to only a subset of the **endpoints** (3) in a shared space. An async delta does not have any dependent deltas.

Asynchronous JavaScript + XML (AJAX): A web programming model that incorporates a set of web technologies including Extensible HyperText Markup Language (XHTML), **cascading style sheets (CSS)**, Document Object Model (DOM), **XML**, Extensible Stylesheet Language Transformation (XSLT), **XMLHttpRequest (XHR)**, and JavaScript. AJAX is designed to make user interaction with the web more responsive.

atom: A unit of information that cannot be divided into smaller parts, and is accepted or rejected in its entirety. See also **Atom Publishing Protocol (AtomPub)**.

atom feed: An **XML** structure that contains metadata about content, such as the language version and the date when the content was last modified, and is sent to subscribers by using the Atom Publishing Protocol (AtomPub), as described in [\[RFC4287\]](#).

Atom Publishing Protocol (AtomPub): An application-level protocol for publishing and editing web resources, as described in [\[RFC5023\]](#).

atom record: A record that contains presentation data. Analogous to a file system, atom records are similar to files that contain data and container records are similar to directories that provide structure and hierarchy for atom records.

atomic transaction: A shared activity that provides mechanisms for achieving the atomicity, consistency, isolation, and durability (ACID) properties when state changes occur inside participating **resource managers**.

attachment: An external file that is included with an **Internet message** or associated with an item in a SharePoint list.

Attachment object: A set of properties that represents a file, **Message object**, or structured storage that is attached to a Message object and is visible through the **attachments table** for a Message object.

attachments table: A **Table object** whose rows represent the **Attachment objects** that are attached to a **Message object**.

attribute: (1) A characteristic of some object or entity, typically encoded as a name-value pair.

(2) (A specialization of the previous definition.) An identifier for a single or multivalued data element that is associated with a directory object. An object consists of its attributes and their values. For example, cn (common name), street (street address), and mail (email addresses) can all be attributes of a user object. An attribute's schema, including the syntax of its values, is defined in an attributeSchema object.

(3) A characteristic of some **object** or entity, typically encoded as a name-value pair.

(4) (A specialization of the previous definition.) An identifier for a single or multivalued data element that is associated with a directory **object**. An **object** consists of its **attributes** and

their values. For example, cn (common name), street (street address), and mail (email addresses) can all be **attributes** of a **user object**. An **attribute's** schema, including the syntax of its values, is defined in an attributeSchema **object**.

attribute group: A collection of attributes that can be used to decorate an **XML element**, as described in [\[XMLSCHEMA1\]](#).

attribute hierarchy: A single-level **hierarchy** that uses only an **attribute** (1) or a **column** (1) from a source, back-end relational database as its hierarchy. An attribute hierarchy typically has the same name as the attribute and is always associated with the attribute on which it is based. An all-level member can optionally be enabled for an attribute hierarchy. See also OLAP hierarchy.

attribute syntax: Specifies the format and range of permissible values of an attribute. The syntax of an attribute is defined by several attributes on the attributeSchema object. Attribute syntaxes supported by **Active Directory** include Boolean, Enumeration, Integer, LargeInteger, String(UTC-Time), Object(DS-DN), and String(Unicode).

audience: A named group of users that is used for targeting content.

audio healer: One or more digital signal processing algorithms designed to mask or conceal human-perceptible audio distortions that are caused by packet loss and **jitter**.

Audio Interchange File Format (AIFF): A sound file format that was originally used on Macintosh and Silicon Graphics (SGI) computers. AIFF stores waveform files in an 8-bit monaural format. See also **waveform (WAV)**.

audio video profile (AVP): A Real-Time Transport Protocol (RTP) profile that is used specifically with audio and video, as described in [\[RFC3551\]](#). It provides interpretations of generic fields that are suitable for audio and video media sessions.

Audio/Video Edge Server (A/V Edge Server): A protocol server that implements the Traversal Using Relay NAT (TURN) Extensions Protocol, as described in [\[MS-TURN\]](#). The protocol server provides connectivity to a protocol client that is behind a network entity, if the network entity provides network address translation (NAT).

Audio/Video Multipoint Control Unit (AVMCU): A **Multipoint Control Unit (MCU)** that supports audio-video (AV) conferencing.

audit entry: Information that is recorded about an operation on an object that is stored on a server.

audit log: (1) A collection of data about successful and failed operations on objects for which auditing is enabled on a server.

(2) A record of activities performed by the Dynamic Host Configuration Protocol (DHCP) **server**. The name of the **audit log** file is based on the current day of the week. For example, on Monday the name of the **audit log** file is DhcpSrvLog-Mon.

Augmented Backus-Naur Form (ABNF): A modified version of Backus-Naur Form (BNF), commonly used by Internet specifications. ABNF notation balances compactness and simplicity with reasonable representational power. ABNF differs from standard BNF in its definitions and uses of naming rules, repetition, alternatives, order-independence, and value ranges. For more information, see [\[RFC5234\]](#).

authenticated context: The runtime state that is associated with the successful authentication of a security principal between the client and the server, such as the security principal itself,

the cryptographic key that was generated during authentication, and the rights and privileges of this security principal.

authenticated user: A built-in security group specified in [\[MS-WSO\]](#) whose members include all users that can be authenticated by a computer.

authentication: (1) The ability of one entity to determine the identity of another entity.

(2) The act of proving an identity to a server while providing key material that binds the identity to subsequent communications.

(3) The ability of one entity to determine the identity of another entity by proving an identity to a **server** while providing key material that binds the identity to subsequent communications.

authentication mode: One of several modes in which an authentication exchange may be performed.

authentication server: The entity that verifies that a person or thing is who or what it claims to be (typically using a cryptographic protocol) and issues a ticket or token attesting to the validity of the claim. The total set of authentication protocol **security support providers (SSPs)** that are typically available on a Windows server release.

Authentication Service (AS): A service that issues ticket granting tickets (TGTs), which are used for authenticating **principals** within the **realm** or **domain** served by the **Authentication Service**.

author: The user who created a **list item**.

authoritative: A DNS server is **authoritative** for a portion of the DNS namespace if it hosts a primary or secondary **zone** for that portion of the DNS namespace.

authority: (1) The first portion of a peer name. For secure peer names, this is a hash of a public key represented as 40 hexadecimal characters in printable form. For unsecured peer names, this is "0".

(2) A hierarchical element in a **URI scheme** used for delegating governance of the name space defined by the remainder of the **URI**, as defined in [\[RFC3986\]](#) section 3.2.

authority hops: The number of site levels to be navigated from a start address to a specific item.

authorization: The secure computation of roles and accesses granted to an identity.

AutoCaption: A feature that adds a **caption** to an object automatically when the object is inserted in a document.

AutoFilter: A mechanism that can be used to filter tabular data based on user-defined criteria such as values, strings, and formatting.

AutoFilter item: A value that is used to populate an **AutoFilter**.

AutoFormat: A built-in set of complementary formatting options that can be applied to ranges of cells and other objects in a document.

automatic calculation mode: A **calculation mode** in which formulas in a worksheet are recalculated automatically whenever the data changes. See also **manual calculation mode**.

Automation server: An application that enables its objects, methods, and properties to be controlled by other applications through **OLE** Automation.

Automation type library: A file or a component within a file that contains OLE Automation standard descriptions of exposed objects, properties, and methods for an application.

AutoRecover: A feature that recovers document and application states in the event of a hardware or software failure.

auto-ringback: A process in which a **call park service (CPS)** automatically transfers a parked **call** from the **parking lot** to the **user agent** who originally parked the call.

AutoShow: A filter option that enables users to display a specified number of the top- or bottom-most items within a PivotTable field.

auxiliary class: See **auxiliary object class**.

auxiliary object class: An **object class** that cannot be instantiated in the directory but can be either added to, or removed from, an existing **object** to make its **attributes** available for use on that **object**; or associated with an **abstract** or **structural object class** to add its **attributes** to that **abstract** or **structural object class**.

availability: A numerical value that indicates whether a user can be interrupted for communication. The higher the number, the less available the user.

available site template: An XML-based collection of predefined or user-defined settings that are stored as a site definition configuration or a site template, and can be used when creating a site.

average weighted value: A type of **rollup** value. It indicates an average that factors the weighted value of all of the child values that are contained within it.

4 B

back link attribute: A **constructed attribute** whose values include **object references** (for example, an **attribute** of **syntax** Object(DS-DN)). The **back link values** are derived from the values of a related **attribute**, a **forward link attribute**, on other **objects**. If *f* is the **forward link attribute**, one **back link value** exists on **object** *o* for each **object** *r* that contains a value of *o* for **attribute** *f*. The relationship between the **forward link attributes** and **back link attributes** is expressed using the **linkId attribute** on the **attributeSchema objects** representing the two **attributes**. The forward link's **linkId** is an even number, and the back link's **linkId** is the forward link's **linkId** plus one. For more information, see [\[MS-ADTS\]](#) section 3.1.1.1.6.

back link value: The value of a **back link attribute**.

back-end database server: A server that hosts data, configuration settings, and stored procedures that are associated with one or more applications.

background color: A color against which characters, patterns, and graphics are displayed. See also **foreground color**.

backward link: A hyperlink between a referenced document and a referencing party. For example, if Document A contains a hyperlink to Document B, then Document B has a backward link to Document A.

banding: (1) A process and collection of settings that are used to define thresholds or boundaries between changes in indicator statuses. See also **column banding** and **row banding**.

(2) A printing technique in which an application prints an image by dividing it into a number of bands and sending each band to the printer separately.

bandwidth management endpoint: A protocol client that communicates with a protocol server to discover and enforce applicable bandwidth policies, and to track and send updates about bandwidth utilization to that server.

base: The base of a host **candidate** is the host candidate itself. The base of server reflexive candidates and peer reflexive candidates is the host candidate from which they are derived. The base of a relayed candidate is the relayed candidate itself.

base field type: An XML-based schema that defines the type of data, such as formatted text or an integer, that can be entered and stored in a field in a **list** (1). Every field in a **list** (1) is derived from a specific base field type.

base type: An XML-based schema that defines the data and rendering fields that can be used in a **list** (1). Every list is derived from a specific base type.

base URI: A **Uniform Resource Identifier (URI)** that is specified for a web resource to convert all relative URIs in that resource to **absolute URIs**. A base URI ends with either a file name, such as `http://www.example.com/sample.htm`, or a slash, such as `http://www.example.com/subdir/`.

base URL: A URL that is specified for a web resource to convert all relative URLs in that resource to **absolute URLs**. A base URL ends with either a file name, such as `http://www.example.com/sample.htm`, or a slash, such as `http://www.example.com/subdir/`. See also **absolute URL**.

base view: An XML-based schema that defines the data and rendering fields that can be used in a **list view**. Every list view is derived from a specific base view.

base view identifier: An integer that uniquely identifies a view definition for a **list** (1).

base16: A binary-to-text encoding scheme whereby an arbitrary sequence of bytes is converted to a sequence of printable **ASCII** characters. Base16 uses only the digits 0 through 9 and the letters A through F.

base64: A binary-to-text encoding scheme whereby an arbitrary sequence of bytes is converted to a sequence of printable **ASCII** characters.

base64 encoding: A binary-to-text encoding scheme whereby an arbitrary sequence of bytes is converted to a sequence of printable **ASCII** characters, as described in [\[RFC4648\]](#).

baseline: The imaginary line to which the bottom of the lowercase "x" character in a font **typeface** is aligned.

basic authentication scheme: An HTTP-based **authentication** (2) method that enables a protocol client to authenticate itself by passing a user identifier and password, as described in [\[RFC2617\]](#).

Basic Encoding Rules (BER): A set of encoding rules for **ASN.1** notation. These encoding schemes allow the identification, extraction, and decoding of data structures. These encoding rules are defined in [\[ITUX690\]](#).

basic page: A **Web Parts Page** that contains only one Web Part zone and, by default, a Content Editor Web Part.

basic scope index: A scope index file that contains records with **basic scope index keys** or anchor scope index keys.

basic scope index key: An **index key** that references a scope index record and contains information about a property and its value.

basic toolbar: A toolbar that consists of a row, column, or block of buttons, each of which perform an action when activated. Unlike a **menu toolbar**, which displays only text labels, a basic toolbar can display both text and icons.

BatchingPositionFilter: A **FilterDescriptor** type that is used when querying a line-of-business (LOB) system. Its value represents the current position of a batch, if the LOB system can return data in batches. When requesting a new batch, the filter can be populated with the position of the last batch.

BatchingTerminationFilter: A **FilterDescriptor** type that is used when querying a line-of-business (LOB) system. Its value can be used to identify the last batch, if the LOB system can return data in batches.

before event: A synchronous event whose handler runs completely before the action that raised the event is finalized. Unlike an after event, a before event handler can cancel the action that caused the event, before that action or related actions are complete. See also **after event**.

beginning-of-file (BOF) key: An **index key** that is stored near the beginning of a content index file. It references a content index record that stores the maximum occurrence for a specified property.

best bet: A URL that a site collection administrator assigns to a keyword as being relevant for that keyword. See also **visual best bet**.

Best Effort NOTIFY (BENOTIFY): A **Session Initiation Protocol (SIP)** method that is used to send notifications to a subscriber, as described in [\[MS-SIP\]](#). Unlike the NOTIFY method, the BENOTIFY method does not require the recipient of the request to send a **SIP response**.

best route: The optimal route to a network **destination**, based on specified criteria. This concept is based on the fact that there is a certain "cost" involved in taking a route across a network. The **best route** to take is the one with the lowest cost, based on specified criteria. This criteria can include the number of networks crossed, the type of network crossed (for example, public or private), or a monetary or bandwidth limit.

beta: A pre-released version of a product that is sent to customers and partners for evaluation and feedback.

B-frame: A bidirectional video frame that references both the previous frame and the next frame.

big-endian: Multiple-byte values that are byte-ordered with the most significant byte stored in the memory location with the lowest address.

Binary Interchange File Format (BIFF): The binary file formats that are used to save Excel workbooks.

binary large image or picture (BLIP): A binary data structure that stores information about a **metafile** image or bitmap picture.

binary large object (BLOB): (1) A discrete packet of data that is stored in a database and is treated as a sequence of uninterpreted bytes.

(2) A collection of binary data stored as a single entity in a database.

BinarySecurityDescriptorAccessor: A type of **MethodInstance** that can be called to retrieve a sequence of bytes from a line-of-business (LOB) system. The system-specific byte sequence describes a set of **security principals** (2) and the associated permissions that each **security principal** (2) has for the EntityInstance identified by a specified EntityInstanceId.

bind: (1) The process of connecting controls to fields or groups in the **data source** (2) of an InfoPath form. When controls are bound to fields and groups, changes to the data in a control automatically update the data that is in the corresponding fields or groups in the data source. Similarly, changes to the data in the data source automatically update the data that is displayed in the controls that are bound to the corresponding fields and groups.

(2) To associate two EntityType [\[MC-CSDL\]](#) instances. An EntityType instance in a data service (described by using **Entity Data Model (EDM)** constructs) may be related to one or more other **conceptual schema definition language (CSDL)** instances. This relationship is represented by using an **association** in an **EDM**. The **cardinality** of a relationship can be determined by inspecting the **EDM** that describes the data service. The act of associating two EntityType instances is known as "binding" and of disassociating two instances is known as "unbinding". If two EntityType instances are already associated, they are considered to be "bound".

bitmap: A collection of structures that contain a representation of a graphical image, a **logical palette**, dimensions and other information.

BitStream: A sequence of bits that represents the compressed data for a **full-text index catalog**.

BitStream file: A content index file, a scope index file, or a content index extension (.cix) file that is used to store compressed data for a **full-text index catalog**. It stores the data as a series of BitStreams that are organized into BitStream pages.

blind carbon copy (bcc) recipient: An addressee whose name is not visible to other addressees of an **Internet message**.

block: (1) A set of **deltas** that are used to define an order for those deltas. Each block consists of one or more groups of deltas.

(2) A subdivision of a segment. Each segment is divided into blocks of equal size (64 kilobytes (KB)) except for the last block in the last segment, which can be smaller if the content size is not a multiple of the standard segment sizes. In version 2.0 Content Information, segments are not divided into blocks.

(3) A chunk of **content** that composes a **segment**. Each **segment** is divided into one or more **blocks**. Every **block** belongs to a specific **segment**, and within a **segment**, **blocks** are identified by their progressive index. (Block 0 is the first **block** in the **segment**, block 1 is the second, and so on.) See [\[MS-PCCRC\]](#) for more details.

block cipher: A cryptographic algorithm that transforms a group of plaintext bits, referred to as a block, into a fixed-size block of cipher text. When the process is reversed, a fixed-size block of cipher text is transformed into a block of plaintext bits. See also **stream cipher**.

block-level formatting: A type of formatting that can be applied to a field or **column** (2) in a table. It is applied to all existing records and automatically to new records.

blog: (1) A website that contains a series of posts about a subject and is arranged in reverse chronological order. Also referred to as web log.

(2) The process of writing or publishing entries to a blog.

body part: A part of an Internet message, as described in [\[RFC2045\]](#).

bookmark: (1) An entity that is used in a document to denote the beginning and ending character positions of specific text in the document, and optionally, metadata about that text or its relationship to other referenced parts of the document.

(2) A data structure that the server uses to point to a position in the **Table object**. There are three pre-defined bookmarks (beginning, end, and current). A custom bookmark is a server-specific data structure that can be stored by the client for easily navigating a **Table object**.

(3) A marker that uniquely identifies a **row** within a set of rows.

(4) An anchor that is used in a report to assist navigation, typically through the use of hyperlinks. A bookmark link in a report sends the user to another location in the report.

Boolean: An operation or expression that can be evaluated only as either true or false.

border: A line that can be applied to the outer edge of a cell, shape, object, or chart element. A border can be variously formatted for style, color, and thickness.

border formatting: A set of properties that, as a whole, specify the appearance of a border, such as color, line style, and thickness.

border style: See **border formatting**.

border thickness: A property of a border that specifies how thick a border line is drawn.

bot: A structured HTML comment that is processed by a front-end web server when the containing document is opened by or saved to the server. Also referred to as web bot.

bottom N filter: A filter that matches the smallest numerical values or oldest time and date values in a specified range.

bottom N filter by count: A type of **bottom N filter** that matches the N smallest numerical values or the N oldest time and date values.

bottom N filter by percent: A type of **bottom N filter** that matches the N percent smallest numerical values or the N percent oldest time and date values.

bottom N filter by sum: A type of **bottom N filter** that matches the smallest numerical values or the oldest time and date values whose sum is equal to or greater than N.

bounding rectangle: A frame that encompasses an object. A bounding rectangle is not rotated and, therefore, always aligns along the x and y axes.

broadcast: (1) A style of resource location in which a client makes a request to all parties on the network simultaneously (a one-to-many communication). Also, a mode of resource location that does not use a name service.

(2) A style of resource location or data transmission in which a client makes a request to all parties on a network simultaneously (a one-to-many communication). Also, a mode of resource location that does not use a name service.

(3) An action of sending the same fax to multiple **recipients**.

(4) The sending of a frame to the Ethernet broadcast domain by an LLTD-capable station.

(5) Live or prerecorded **content** that can be **streamed** to more than one client simultaneously. The server **streams** the **content** to all clients from the same location, and does not allow clients to seek.

broadcast session: A sharing session initiated by a presenter that is used for sharing the presenter's view of a document with one or more attendees.

browser-compatible form template: A form template that is designed for publication to a protocol server that is running InfoPath Forms Services.

browser-enable: The process of converting an InfoPath form template into a format that can be rendered in a web browser, and publishing it to and activating it on a protocol server that is running InfoPath Forms Services.

browser-enabled form template: A form template that is published to a protocol server that is running InfoPath Forms Services and is also activated for use on that server.

bubble size: A value that represents the diameter of a bubble in a bubble chart.

bucket: (1) A collection of items that were requested by a search application during a **crawl**. An item can be a person, a document, or any other type of item that can be crawled.

(2) A positive integer value that represents a mapping for a specific error signature.

(3) A positive integer value that is assigned to a particular error signature by a hosted error reporting service.

bucket web: A site that is used to store content for a specific **category** (1).

build: (1) An **animation** effect that is applied to content on a **presentation slide**. The complete animation for a given piece of content is specified as a sequence of builds, where each build causes parts of the content to appear, disappear, move, or be emphasized in some manner.

(2) See **build number**.

build dependency set: A serialized .NET Framework object that represents a set of file dependencies.

build identifier: An integer that identifies a **build** (1).

build number: (1) A part of a sequential numbering system that is used to differentiate one version of a software product from another.

(2) A unique number identifying the version of an application, in this case the Terminal Services (TS) client.

built-in control: A control that is included with Microsoft InfoPath and appears by default in the Controls pane.

built-in name: A member of the group of defined names that are reserved for specific functionality.

BulkAssociatedIdEnumerator: A type of **MethodInstance** that can be called to retrieve pairs of EntityInstanceIds of source EntityInstances and EntityInstanceIds of corresponding destination EntityInstances for a specified **Association**. The specified EntityInstances are either a source or a destination in the specified Association.

BulkAssociationNavigator: A type of **MethodInstance** that can be called to retrieve destination EntityInstances that are associated with multiple specified EntityInstances for each of the sources of the specified **Association**.

BulkIdEnumerator: A type of **MethodInstance** that can be called to retrieve a set of EntityInstanceIds and a small subset of important Fields of the EntityInstances that are identified by the specified set of EntityInstanceIds.

BulkSpecificFinder: A type of **MethodInstance** that can be called to return a set of specific EntityInstances of an Entity, given a set of corresponding EntityInstanceIds.

Business Connectivity Services (BCS): A set of services that enables interaction and integration with back-end data in a **line-of-business (LOB) system**, including external data and related services. BCS includes the **Business Data Connectivity (BDC)** service.

Business Data Connectivity (BDC): A shared service that stores information about business application data that exists outside a server farm. It can be used to display business data in lists, Web Parts, search results, user profiles, and custom applications. Previously referred to as Business Data Catalog.

business logic: (1) A set of rules, formulas, validation, and code that define the limits and methods for processing data that is entered into an InfoPath form.

(2) The part of an application that processes data according to the requirements defined in a **line-of-business (LOB) system**. It refers to the routines that perform the data entry,

update, query, and report processing, and more specifically to the processing that takes place behind the scenes rather than the presentation logic that is required to display the data.

Business Logic Module: A module that contains Business Logic software and is called to enforce data constraints or perform tasks that are loaded and executed in a host-specific run-time environment.

business object: An object that performs a defined set of operations, such as data validation or **business logic** (2) rules, related to a business process or workflow.

business rule: A user-defined process that can proactively manage data within the Master Data Services database.

ButtonPopup control: A type of Button control that displays a menu of related commands when activated.

byte order mark: A Unicode character that is used to indicate that text is encoded in UTF-8, UTF-16, or UTF-32.

5 C

cabinet (.cab) file: A single file that stores multiple compressed files to facilitate storage or transmission.

cached frame: A video frame that is cached for later use by an encoder and a decoder. A cached frame acts as a reference frame for the next **Super P-frame (SP-frame)**. I-frames and SP-frames typically are cached frames.

calculate: The process by which computations in a workbook are performed.

calculated column: A **column** (2) in a table that contains a formula that is copied automatically to each record in the column.

calculation mode: A setting that determines whether the formulas in a worksheet are recalculated automatically or manually. See also **automatic calculation mode** and **manual calculation mode**.

Calendar object: A **Message object** that represents an event, which can be a one-time event or a recurring event. The Calendar object includes properties that specify event details such as description, organizer, date and time, and status.

call: A communication between **peers** that is configured for a multimedia conversation.

call park service (CPS): A server **endpoint** (5) that allows a **user agent** to make a **call** inactive without terminating that call. The call can then be reactivated by the same user agent, by using the same or a different **endpoint** (5), or a different user agent. See also **parking lot**.

callback: (1) A concept in which the originator of a **call** is called back by the responder. In dial-up communication (like ISDN/PSTN), the originator of the dial-up hangs up after indicating the interest to be called back. The responder then calls up the originator to establish the communication.

(2) The mechanism through which a remote access client gets called back by the server in order to establish connectivity.

callee: An **endpoint** (5) to which a **call** is initiated by a **caller**.

caller: (1) An **endpoint** (5) that initiates a **call** to establish a media session.

(2) The originator of a **call**. The **network access client (NAC)** is typically the **caller**. The **NAC** and **NAS** might choose to negotiate and use **callback**, in which case the **caller** role is reversed for the **callback** itself, with the **NAS** being the **caller**.

camera: A virtual representation of a camera that controls the position of the viewer window inside the 3-D environment.

candidate: A set of **transport addresses** that form an atomic unit for use with a media session. For example, in the case of Real-Time Transport Protocol (RTP) there are two transport addresses for each candidate, one for RTP and another for the Real-Time Transport Control Protocol (RTCP). A candidate has properties such as type, priority, foundation, and **base**.

candidate identifier: A random string that uniquely identifies a **candidate**.

candidate pair: A set of candidates that is formed from a **local candidate** and a **remote candidate**.

canonical URL: An **absolute URL** that identifies a space, tool, or component the same way on any device.

canvas: An area upon which multiple shapes can be drawn or displayed. The shapes can be moved and resized as a unit because they are contained within the drawing canvas.

caption: One or more characters that can be used as a label for display purposes or as an identifier.

carbon copy (cc) recipient: In an **Internet message**, an addressee whose name is visible to other addressees and is not necessarily expected to take any action. The message is for informational purposes only for that addressee.

card selector: Software that enables a user to select a digital identity to transmit to a relying party. When a user selects a card, the card selector obtains the **claims** (2) from the associated claims provider and transmits those **claims** (2) to the relying party application on behalf of the user.

cardinality: The measure of the number of elements in a set.

Cartridge: A unit of **physical media** on which information may be stored. Cartridges come in various types, including 8-mm tape, magnetic disks, optical disks, and CD-ROMs. Some **cartridges** have multiple **sides**.

cascading style sheet (CSS): An extension to **HTML** that enables authors and users of HTML documents to attach style sheets to those documents, as described in [\[CSS-LEVEL1\]](#) and [\[CSS-LEVEL2\]](#). A style sheet includes typographical information about the appearance of a page, including the font for text on the page.

catalog: (1) A table that defines the structure and relationships of a set of tables in a database.

(2) A data store that holds the configuration properties for **components** and **conglomerations**.

(3) The highest-level unit of organization in the **indexing service**. It represents a set of **indexed** documents against which queries can be executed by using the [\[MS-MCIS\]](#).

(4) The highest-level unit of organization in the Windows Search service. It represents a set of indexed documents against which queries can be executed by using the [\[MS-WSP\]](#).

catalog friendly URL: A web address that is designed to be easily readable by both people and search engine web crawler programs. This type of URL has additional segments appended to control the webpage content.

catalog friendly URL suffix: The additional segment that is appended to a friendly **Uniform Resource Locator (URL)** in order to construct a **catalog friendly URL**.

category: (1) A custom string that is used to group one or more documents.

(2) A string that is used as a suggestion for a document category on a site.

(3) A subdivision of items into useful groups such as geographical regions. For example, categories that represent geographical regions could be North, South, East, and West.

(4) An enhanced presence concept that is used by a **Session Initiation Protocol (SIP)** client to publish or subscribe to **presence** (2) information. A category enables basic identification of the data that is being published; it implies an agreed-upon schema for interpreting the data. A category name identifies a contract between a publisher and a subscriber.

(5) A grouping of rows in a **Table object** that all have the same value for a specified property.

(6) A logical grouping of **updates** identified by a **GUID** and described by **metadata**. A category can be treated as an **update** with no associated **content**.

(7) A hierarchical grouping of rows. For example, a query result that contains author and title columns can be categorized based on author. Each group of rows containing the same value for author would constitute a category.

(8) A group of updates. Each update belongs to zero or more update categories. An update category can be a product category that contains updates for a particular product, or a classification category that contains updates of a particular classification (for example, all security updates). A category can have a parent category as well as child categories.

category subscriber: A **SIP protocol client** that sent a **category** (4) **SUBSCRIBE** request.

CDATA section: A section in an **XML document** that is bracketed by [!CDATA[and]] characters. All data in this section, including markup tags, is treated as normal characters by an **XML** parser.

cell: A box that is formed by the intersection of a **row** (2) and a **column** (2) in a worksheet or a table. A cell can contain numbers, strings, and formulas, and various formats can be applied to that data.

cell contents: The data inside a cell, such as text, values, formulas, and cell error values.

cell error value: Any of a number of special values that are returned as a result of an unsuccessful formula calculation.

cell formatting: The set of properties that, as a whole, specify the appearance of a cell, such as font characteristics and fill color.

cell margin: A measurement of the distance between the **border** of a cell and the nearest pixel in a character or digit of data in the cell. There are top, bottom, right, and left margins. See also **cell spacing**.

cell reference: A set of coordinates that a cell occupies on a worksheet. For example, "B3" is the reference of a cell that appears at the intersection of column "B" and row "3".

cell spacing: A measurement of the distance between the cells of a table or worksheet. Most tables and worksheets are implemented with contiguous cells, in which case the cell spacing value is 0 (zero). See also **cell margin**.

cell value: The text or numeric content of a cell, or the results of a formula. A cell value does not include a formula expression, cell formatting, or other metadata.

center-across-selection alignment: A formatting setting that centers cell content horizontally within a selected range of cells.

Central Administration site: A SharePoint site that an administrator can use to manage all of the sites and servers in a server farm that is running SharePoint Products and Technologies.

CER server: A designated server application that acts as a recipient for the **error report level 1 data** and **error report level 2 data** that is created by the Corporate Error Reporting V.2 Protocol.

certificate: (1) A certificate is a collection of **attributes** (1) and extensions that can be stored persistently. The set of attributes in a certificate can vary depending on the intended usage of the certificate. A certificate securely binds a public key to the entity that holds the corresponding private key. A certificate is commonly used for **authentication** (2) and secure exchange of information on open networks, such as the Internet, extranets, and intranets. Certificates are digitally signed by the issuing **certification authority (CA)** (1) and can be issued for a user, a computer, or a service. The most widely accepted format for certificates is defined by the ITU-T X.509 version 3 international standards. For more information about attributes and extensions, see [\[RFC3280\]](#) and [\[X509\]](#) sections 7 and 8.

(2) When referring to X.509v3 certificates, that information consists of a public key, a **distinguished name (DN)** (3) of some entity assumed to have control over the private key corresponding to the **public key** in the certificate, and some number of other attributes and extensions assumed to relate to the entity thus referenced. Other forms of certificates can bind other pieces of information.

(3) As used in this document, **certificates** are expressed in [XRML] section 1.2.

certificate authority (CA): See **certification authority (CA)**.

certificate chain: A sequence of **certificates** (1), where each certificate in the sequence is signed by the subsequent certificate. The last certificate in the chain is normally a self-signed certificate.

certification: The **certificate** (1) request and issuance process whereby an end entity (EE) first makes itself known to a **certification authority (CA)** (1) (directly, or through a registration authority) through the submission of a certificate enrollment request, prior to that **CA** issuing a **certificate** (1) or **certificates** (1) for that EE.

certification authority (CA): (1) A third party that issues public key **certificates** (1). Certificates serve to bind public keys to a user identity. Each user and certification authority (CA) can decide whether to trust another user or CA for a specific purpose, and whether this trust should be transitive.

(2) A software component that issues digital (X.509) **certificates** (2) to identities based on a public/private key pair. For more information, see [\[RFC2865\]](#).

(3) A third party that issues **public key certificates**. **Certificates** serve to bind **public keys** to a user identity. Each user and **certification authority (CA)** may decide whether to trust another user or **CA** for a specific purpose, and whether this trust should be transitive. For more information, see [\[RFC3280\]](#).

CGAPI: An API that is implemented by **grammar checkers** that have been licensed to Microsoft Corporation by external vendors.

challenge: A piece of data used to authenticate a user. Typically a challenge takes the form of a **nonce**.

Challenge-Handshake Authentication Protocol (CHAP): A protocol for user authentication to a remote resource. For more information, see [\[RFC1994\]](#) and [\[RFC2759\]](#).

change log: A log of changes, such as add and delete, that are made to objects that are stored on a **back-end database server**. Applications can use this information to identify changes that occurred on those objects.

change token: A serialized token that can be used to determine whether changes occurred in the system. It can also be used to deserialize packages in the correct sequence during import or restore operations.

ChangedIdEnumerator: A type of **MethodInstance** that can be called to retrieve EntityInstanceIds of EntityInstances that were modified in a line-of-business (LOB) system after a specified time.

character pitch: A quality that measures the number of characters that can be printed in a horizontal inch. Pitch is typically used to measure monospace fonts.

character set: (1) A mapping between the characters of a written language and the values that are used to represent those characters to a computer.

(2) The range of characters used to represent textual data within a **MIME body part**, as described in [\[RFC2046\]](#).

(3) A mapping of characters to their identifying code values. For more information, see [\[MSDN-CS\]](#).

chart: An object that displays data or the relationships between sets of data in a visual form.

chart area: A region in a chart object that is used to position chart elements, render axes, and plot data.

chart data table: See **data table** (2).

chart sheet: A single logical container that is used to create and store charts in a workbook.

check in: The process of placing a file or project into a source repository. This releases the lock for editing and enables other users to view the updated file or check out the file. See also **check out**.

Check List: An ordered list of **candidate pairs** that determines the order in which connectivity checks are performed for those candidate pairs.

check out: The process of retrieving a writable copy of a file or project from a source repository. This locks the file for editing to prevent other users from overwriting or editing it inadvertently. See also **check in**.

checked out: A **publishing level** that indicates that a document has been created and locked for exclusive editing by a user in a version control system.

checksum: A value that is the summation of a byte stream. By comparing the checksums computed from a data item at two different times, one can quickly assess whether the data items are identical.

child: (1) An object that is immediately below the current object in a hierarchy.

(2) A data item within the Master Data Services (MDS) system that has a superior data item. A child in MDS can be a leaf member or a consolidated member.

child element: In an **XML document**, an element that is subordinate to and is contained by another element, which is referred to as the parent element.

child item query: A set of filters and options for retrieving child objects in a collection of **CSOM Objects**.

child PivotTable member: A PivotTable member that is one level lower in a dimension hierarchy, relative to another PivotTable member, which is referred to as its parent member. For example, a child of a Year member might be Quarter.

chunk: A sequence of words that are treated as a single unit by a module that checks spelling.

CIM: See **Common Information Model (CIM)**.

cipher: A cryptographic algorithm used to encrypt and decrypt files and messages.

cipher block chaining (CBC): A method of encrypting multiple blocks of plaintext with a block cipher such that each ciphertext block is dependent on all previously processed plaintext blocks. In the **CBC** mode of operation, the first block of plaintext is XOR'd with an Initialization Vector (IV). Each subsequent block of plaintext is XOR'd with the previously generated ciphertext block before encryption with the underlying block cipher. To prevent certain attacks, the IV must be unpredictable, and no IV should be used more than once with the same key. **CBC** is specified in [\[SP800-38A\]](#) section 6.2.

cipher suite: A set of cryptographic algorithms used to encrypt and decrypt files and messages.

ciphertext: The encrypted form of a message. Ciphertext is achieved by encrypting the plaintext form of a message, and can be transformed back to plaintext by decrypting it with the proper key. Without that transformation, a ciphertext contains no distinguishable information.

claim: (1) A set of operations that are performed on a workflow task to specify the user who owns it.

(2) A statement that one subject makes about itself or another subject. For example, the statement can be about a name, identity, key, group, privilege, or capability. Claims have a provider that issues them, and they are given one or more values. They are also defined by a claim value type and, possibly, associated metadata.

(3) An assertion about a security principal expressed as an n-tuple containing an {Identifier, ValueType and m-Values of type ValueType} where $m \geq 1$. A claim with only 1 value in the n-tuple is called a **single-valued claim** and a claim with more than 1 value is called a **multi-valued claim**.

(4) A declaration made by an entity (for example, name, identity, key, group, privilege, and capability). For more information, see [\[WSFedPRP\]](#) sections 1.4 and 2.

claim issuer: A **claims provider** that issues a **claim** (2).

claim type: A statement that is part of a **claim** (2) and provides context for a claim value. It represents the type of claim and is typically a **Uniform Resource Identifier (URI)**. Examples include FirstName and Role.

claim value: A string that represents the value of a statement in a **claim** (2). It specifies what is being asserted by a claim.

claim-based authentication mode: A set of operations that is used to establish trust relationships between **claims providers** and relying party applications. It involves the exchange of identifying **certificates** (1) that make it possible for a relying party to trust the content of a **claim** (2) that is issued by a claims provider.

claims provider: A software component or service that can be used to issue a **claim** (2) during sign-in operations and to display, resolve, and provide search capabilities for claims in a **card selector**.

claims provider schema: A schema that is used to specify which fields can be returned as metadata for a **claim** (2) that is issued by a specific claims provider.

class: (1) User-defined binary data that is associated with a key.

(2) A **Remoting Type** that encapsulates a set of named values and a set of methods that operate on those values. The named values are called Members of the Class. A Class is part of the **Remoting Data Model**. For more information, see [\[MS-NRTP\]](#) section 3.1.1.

(3) See **object class**.

(4) A reference to a class module whose methods and properties can be used within a report.

class factory: An object (3 or 4) whose purpose is to create objects (3 or 4) from a specific object class (3 or 4).

class identifier (CLSID): A **GUID** that identifies a software component; for instance, a DCOM **object class** (4) or a **COM class**.

class module: A module that contains the definition for a new object. Each instance of a class creates a new object, and procedures that are defined in the module become properties and methods of the object.

class name: The name that is used to refer to a class module that provides an implementation of a behavior.

classifier: A Unicode string used in conjunction with an authority to form a Peer Name.

clear all state: A condition in which no filter is applied to a worksheet, list, or PivotTable report.

client: (1) A computer on which the remote procedure call (RPC) client is executing.

(2) An execution environment that holds object references and issues object RPC (ORPC) calls.

(3) In DFS-R, a replicating machine acts as a client when it receives replicated files from its upstream partner. Use of the terminology **client** stipulates that the machine contact its upstream server, and is responsible for initiating communication related to receiving replicated files. It does not imply anything about the operating system version or the function of the machine.

(4) The sending endpoint of a web services request message, and receiver of any resulting web services response message.

(5) For the Peer Content Caching and Retrieval Framework, a client is a client-role peer; that is, a peer that is searching for content, either from the server or from other peers or hosted caches. In the context of the Retrieval Protocol, a client is a peer that requests a block-range from a server_role_peer. It acts as a Web Services Dynamic Discovery (WS-Discovery) [\[WS-Discovery\]](#) client.

(6) Synonym for **client computer** (4).

(7) In [\[MS-GPOL\]](#), the capitalized use of this term refers to a **domain** member, including the **domain controller (DC)**, that is involved in a **policy application** sequence.

- (8) The entity that initiates the **HTTP** connection.
- (9) A client device that is capable of issuing OMA-DM commands to a server and responding to OMA-DM commands issued by a server.
- (10) Identifies the system that consumes WMI services and initiates DCOM ([\[MS-DCOM\]](#)) calls to WMI servers.
- (11) The entity that has created the logging message, or an entity that receives a logging message from a client. In the latter case, the client is a proxy.
- (12) The software that is used by a **user** to access the service. It represents the **user** in [MS-PASS]. A synonym is **client** application.
- (13) Used as described in [\[RFC2616\]](#) section 1.3.
- (14) The term "Client" that is defined in [\[WS-Discovery1.1\]](#).
- (15) The client application using the **WS-Management** Protocol to access the management **service**, on the local or a remote machine.
- (16) A client, also called a client computer, is a computer that receives and applies settings of a **Group Policy Object (GPO)**, as specified in [MS-GPOL].
- (17) A user participating in or intending to participate in collaboration.
- (18) The **target location** machine.
- (19) The entity that initiates communication with the **hosted cache**, to offer it **segments** of data.
- (20) An application or a system that accesses a Web service endpoint as defined in [\[WSAddressing\]](#).
- (21) A **client** application that uses the WS-Management Protocol (see [\[DMTF-DSP0226\]](#)) to access the management **service** on a local or remote computer.
- (22) A **domain** member that is involved in a **policy application** mode sequence.
- (23) Any process that initiates **commands** for execution on a server by using the PowerShell Remoting Protocol.

client area: (1) The area of the desktop that is available for a window or notification icon to paint on.

(2) In an application, the display area that is used to create data, such as drawing or typing functions. The client area does not include toolbars, menus, or status bars.

client computer: (1) A computer that instigates a connection to a well-known port on a server.

(2) A computer that receives and applies settings from a **Group Policy Object (GPO)**, as specified in [MS-GPOL].

(3) A computer that gets its **updates** from an **update server**. A client can be a desktop computer, a server, or the **update server**. For more information, see [\[MS-WUSP\]](#) and [\[MS-WSUSSS\]](#).

(4) The client machine in the **domain** or network topology of clients, servers, and **domain controllers**. Alternatively, a computer that is not a **domain controller server**; the computer may or may not be joined to a domain.

Client Scale Secure Real-Time Transport Protocol (Client Scale-SRTP): A protocol that is used by applications that receive media from and send media to only one peer. It is a variation of the **Scale Secure Real-Time Transport Protocol (SSRTP)**, as described in [\[MS-SSRTP\]](#).

client/server mode: A mode that consists of one server with many client connections (one-to-many). From the perspective of each client, there is only one connection: the connection to the server.

clipboard format: An unsigned integer that uniquely identifies the format of a data packet that is stored in a **binary large object (BLOB)** and can be shared between processes through the operating system clipboard or other means.

cluster: (1) A group of computers that are able to dynamically assign resource tasks among nodes in a group.

(2) A group of computers that are able to dynamically assign resource tasks among nodes in a group. The group of computers that can be accessed as though they are a single host. A **cluster** is generally accessed by using a virtual IP address. For more information, see [\[MSFT-WLBS\]](#).

(3) The smallest allocation unit on a **volume**.

cluster node: Cluster node defined in [\[MS-CMRP\]](#) section 1.3.

cluster resource group: Resource group defined in [MS-CMRP] section 1.1.

coclass: A component **object** (an association between a **class identifier (CLSID)** and a set of named implementations of IUnknown) that is defined using the **coclass** keyword.

code page: An ordered set of characters of a specific script in which a numerical index (code-point value) is associated with each character. Code pages are a means of providing support for **character sets** (1) and keyboard layouts used in different countries. Devices such as the display and keyboard can be configured to use a specific code page and to switch from one code page (such as the United States) to another (such as Portugal) at the user's request.

codec: An algorithm that is used to convert media between digital formats, especially between raw media data and a format that is more suitable for a specific purpose. Encoding converts the raw data to a digital format. Decoding reverses the process.

Collaborative Application Markup Language (CAML): An XML-based language that is used to describe various elements, such as queries and views, in sites that are based on SharePoint Products and Technologies.

collapse: The process of closing a level in a dimension hierarchy on a PivotTable report to hide or aggregate lower-level details in the data.

collapsed outline state: A state in which the content that is nested within an outline is not displayed.

collation: A set of rules that determines how data is compared, ordered, and presented.

collation order: A rule for establishing a sequence for textual information.

colleague: A user who has a social networking relationship with another user.

Colleague Tracker Web Part: A type of **Web Part** that users can add to a My Site to track changes to the profiles of their colleagues.

collection: (1) A grouping of one or more EDM types that are type compatible. A collection can be used as the return type for a FunctionImport.

(2) A **resource** that contains a set of **URIs** that identify member **resources**. Use of this term is consistent with what is specified in [\[RFC4918\]](#) section 5.2.

(3) A user-defined group of data items from the same entity.

(4) An element that is used when a Function element is declared whose parameter or return type is not a single value but many. For example, a Function element may return a collection of varchar, that is, collection(varchar).

color gradient: A gradual progression from one color to another color, or from one shade to another shade of the same color.

color level: The intensity value of a color.

color matching: The conversion of a color, sent from its original color space, to its visually closest color in the destination color space. See also **Image Color Management (ICM)**.

color palette: A collection of colors that is available to format text, shapes, cells, and chart elements.

color scale: A specific range of colors that is used to give additional meaning to data by assigning certain values to colors in the spectrum.

color scheme: A table of color values that enables colors to be referenced by an index value in the table instead of a color value. See also **color palette**.

color space: (1) A system that describes color numerically by mapping color components to a multidimensional coordinate system. The number of dimensions is typically two, three, or four. For example, if colors are expressed as a combination of the three components red, green, and blue, a three-dimensional space can describe all possible colors. Grayscale colors can be mapped to a two-dimensional color space. If transparency is considered a component, four dimensions are appropriate. Also referred to as color model.

(2) A mapping of color components to a multidimensional coordinate system. The number of dimensions is generally two, three, or four. For example, if colors are expressed as a combination of the three components red, green, and blue, a three-dimensional space is sufficient to describe all possible colors.

(3) Any method of representing colors for printing or electronic display.

color stop: A color at a specific position in a **color gradient**.

column: (1) See **field** (3).

(2) A single set of data that is displayed vertically in a worksheet or a table.

(3) See **column chart**.

(4) The container for a single type of information in a **row**. Columns map to property names and specify what properties are used for the search query's **command tree** elements.

column banding: A table formatting option that applies **background colors** to alternating **columns** (2) to increase legibility.

column chart: A chart that displays data in vertical bars to facilitate data comparison.

column field: A field that is contained in the PivotTable area where the **column** (2) values are shown.

column formula: A formula that is used in a **calculated column**.

column outline: A nested grouping of **columns** (2) in a worksheet.

COM class: An **object class** (3).

COM server: A **server** that provides access to a component **object** (an association between a **CLSID** and a set of named implementations of IUnknown).

command: Any entity that can be executed on the server.

command tree: A combination of **restrictions** (1) and sort orders that are specified for a search query.

comment: An annotation that is associated with a cell, text, or other object to provide context-specific information or reviewer feedback.

Common Information Model (CIM): The **Distributed Management Task Force (DMTF)** model that describes how to represent real-world computer and network objects. CIM uses an object-oriented paradigm, where managed objects are modeled using the concepts of classes and instances. See [\[DMTF-DSP0004\]](#).

Common Intermediate Format (CIF): A picture format, described in the H.263 standard, that is used to specify the horizontal and vertical resolutions of pixels in YCbCr sequences in video signals.

common language runtime (CLR): (1) The core runtime engine in the Microsoft .NET Framework for executing applications. The common language runtime supplies managed code with services such as cross-language integration, code access security, object lifetime management, and debugging and profiling support.

(2) A runtime library that acts as an agent to manages code at execution time, providing core services such as memory management, thread management, and remoting, while also enforcing strict type safety and other forms of code accuracy that promote security and robustness. The Microsoft implementation of the Common Language Infrastructure (CLI), as specified in [\[ECMA-335\]](#).

Common Views folder: A **special folder** that contains the data for default views that are standard for a message store and can be used by any user of a client that accesses the message store.

compact axis: A state in which PivotTable members from different levels in a hierarchy are displayed in a single **column** (2).

ComparisonFilter: A **FilterDescriptor** type that is used when querying a line-of-business (LOB) system. An LOB system can compare a ComparisonFilter value with the value of a specific Field of a set of EntityInstances and only those EntityInstances where the Field values pass the comparison test can be returned.

complex type: (1) An element that can contain other elements or **attributes** (1) and appears as <complexType> in an **XML document**. See also **simple type**.

(2) A type that represents a set of related information. Like the entity type, it consists of one or more properties of the EDM simple type or complex types; however, unlike the entity type, the complex type does not have an EntityKey element or a NavigationProperty element.

component: A representation of a constituent **transport address** if a **candidate** consists of a set of transport addresses. For example, media streams that are based on the Real-Time Transfer Protocol (RTP) have two components, one for RTP and another for the Real-Time Transfer Control Protocol (RTCP).

component birth date: An integer that is associated with a full-text index component. It defines the order in which the components were created in a **full-text index catalog**.

component configuration entry: An entry in the catalog that represents a particular configuration of a component.

component identifier: A simple integer that identifies each component in a **candidate** and increments by one for each component.

Component Object Model (COM): An object-oriented programming model that defines how objects interact within a single process or between processes. In **COM**, clients have access to an object through interfaces implemented on the object. For more information, see [MS-DCOM].

composite field index: An index that uses more than one column in a table to index data.

compound file: (1) A structure for storing a file system, similar to a simplified FAT file system inside a single file, by dividing the single file into sectors.

(2) A file that is created as defined in [MS-CFB] and that is capable of storing data that is structured as storage and streams.

compound scope index: A file that is in a search scope index and contains records that store compound scope index keys or anchor scope index keys.

computed field: A field that can perform data manipulation and display functions by using the contents of other fields.

computer name: The **DNS** or NetBIOS name.

computer object: An **object** of class computer. A **computer object** is a **security principal object**; the principal is the operating system running on the computer. The shared secret allows the operating system running on the computer to authenticate itself independently of any user running on the system. See **security principal**.

conceptual schema definition language (CSDL): A language that is based on XML and that can be used to define conceptual models that are based on the **Entity Data Model (EDM)**. For more information, see [MC-CSDL].

concrete type: A type used in this specification whose representation must be standardized for interoperability. Specific cases include types in the **IDL** definition of an **RPC** interface, types sent over **RPC** but whose representation is unknown to **RPC**, and types stored as byte strings in **directory attributes**.

condition: (1) A logical expression comparing one or more properties in all incoming **Message objects** against a set of clauses. This logical expression can evaluate to TRUE or FALSE.

(2) A **condition** of a **policy** that specifies one of the fields in a **DHCP Client** request and the value that the field should contain to match the **condition**. The **condition** also contains an index that identifies the expression with which the **condition** is associated.

(3) A predicate (for example, the machine is idle) that must be satisfied for a **task** to run. A **task** runs when any of its **triggers** and all of its conditions are met.

(4) A method of controlling which **RAP** is selected as the **current resource policy**. Conditions are rules that are automatically triggered in response to notifications of any of the **conditional events**. A condition is composed of a **condition state** and **RAP**. When a **conditional event** is triggered, conditions with the associated Name attribute value are evaluated in the order of their ID attribute value; that is, a condition with the ID value 0 will be evaluated first and so on. In condition evaluation, the **condition state** is evaluated and if it is found to be TRUE, the **RAP** associated with that condition is selected as the **current resource policy**. If no condition has its **condition state** as TRUE, the condition with the name ANY is evaluated.

(5) A business rule argument that determines when to apply the actions of the business rule. Conditions can be parsed together by using the logical operators AND and OR.

condition state: A part of a **condition** consisting of a predicate that evaluates some current state of the computer being managed. The predicate is a series of expressions separated by AND and OR operators, evaluated in order. Expressions are selected from the following fixed set: an equality or inequality test of the amount of hardware memory, an equality or inequality test of the number of processors, or a predicate test of the online or offline status of a **cluster node** or **cluster resource group**.

conditional events: Unscheduled events that can trigger the following WSRM policy changes: Processor hot add, Memory hot add, Cluster node goes up or down, or Cluster resource group goes online or offline.

conditional formatting: A mechanism that changes the appearance of a user interface element based on the evaluation of a rule or expression.

conference: (1) A **Real-Time Transport Protocol (RTP)** session that includes more than one **participant** (2).

(2) An **RTP session** involving multiple **participants**.

(3) A set of two or more communicating users along with the software they are using to communicate.

conference control command: See **conference control request**.

conference control request: A request that is sent by a conference client to modify a conference or the state of a conference participant.

conference URI (conference-URI): A **Session Initiation Protocol (SIP) URI** that uniquely identifies the **focus** of a conference.

Conference-Id: A string of printable **ASCII** characters that uniquely identifies a **conference**.

configuration database: A database that is stored on a **back-end database server** and contains both persisted objects and site collection metadata for lookup purposes.

configuration naming context (config NC): A **naming context (NC)** that contains configuration information. In **Active Directory**, a single **config NC** is shared among all **domain controllers (DCs)** in the forest. A **config NC** cannot contain **security principal objects**.

confirmation: A message that asks a user to verify an action before the user performs it.

conglomeration: (1) A collection of **component configuration entries**, together with a component-independent configuration that is conceptually shared by the **component configuration entries**. A conglomeration is identified by a **conglomeration identifier**.

(2) A collection of **event classes** and **subscriptions** together with independent configuration data that is conceptually shared by the both the **event classes** and **subscriptions**. A conglomeration is identified by a **conglomeration identifier**.

conglomeration identifier: A **GUID** that identifies a **conglomeration**.

connected data: Data that is stored in the same workbook from which it is being referenced, or data that is stored in a database repository.

connected network: A network of computers in which any two computers can communicate directly through a common transport protocol (for example, TCP/IP or SPX/IPX). A computer can belong to multiple connected networks.

connection: (1) A link between two devices that uses the **Simple Symmetric Transport Protocol (SSTP)**. Each connection can support one or more SSTP sessions.

(2) A link that two physical machines or applications share to pass data back and forth.

(3) Each user that has a session with a server can create multiple share connections, or resource connections, using that user ID. This resource connection is created using a tree connect **Server Message Block (SMB)** and is identified by an **SMB** TreeID or TID.

(4) Firewall rules are specified to apply to connections. Every packet is associated with a connection based on TCP, UDP, or IP endpoint parameters; see [\[IANAPORT\]](#).

(5) In DFS-R, a pair of client and server replication partners.

(6) In OleTx, an ordered set of logically related messages. The relationship between the messages is defined by the higher-layer protocol, but they are guaranteed to be delivered exactly one time and in order relative to other messages in the connection.

(7) Either a **TCP** or **NetBIOS** over TCP connection between an SMB 2 Protocol client and an SMB 2 Protocol server.

(8) A time-bounded association between two **endpoints** that allows the two **endpoints** to exchange messages.

(9) A logical communication path identified by a pair of sockets, as defined in [\[RFC793\]](#).

(10) An instantiation of the protocol that can be used as a scoping entity for channel. The server may instantiate multiple simultaneous connections to the same client.

(11) The successful completion of necessary protocol arrangements (authentication, network parameters negotiation, and so on) between a remote client computer and the RRAS server to set up a dial-up or **virtual private networking (VPN)** association. **Connection** enables the remote client computer to function on the RRAS server network as if it were connected to the server network directly.

Connection Join (Join): The process by which a **connection session** is established.

Connection Session: After **FRS** discovers a connection from **Active Directory**, **FRS** establishes a connection session with the remote connection **partner** based on the information provided by the connection object. The connection is called "joined" when a connection session is successfully established. This connection session is disconnected once the connection **schedule** is off (forbidding **file** replication on the connection).

connection string: (1) A series of arguments, delimited by a semicolon, that defines the location of a database and how to connect to it.

(2) A character string expression that uniquely identifies the data store to use for a particular query or set of queries and the methods, including authentication information and configuration options, for connecting to that data store.

connectionless protocol: A transport protocol that enables **endpoints** (5) to communicate without a previous connection arrangement and that treats each packet independently as a **datagram**. Examples of connectionless protocols are Internet Protocol (IP) and User Datagram Protocol (UDP).

connection-oriented transport protocol: A transport protocol that enables **endpoints** (5) to communicate after first establishing a connection and that treats each packet according to the connection state. An example of a connection-oriented transport protocol is Transmission Control Protocol (TCP).

connectivity check: A **Simple Traversal of UDP through NAT (STUN)** binding request that is sent to validate connectivity between the local and remote candidates in a **candidate pair**.

constructed attribute: (1) An attribute whose values are computed from normal attributes (for read) and/or have effects on the values of normal attributes (for write).

(2) See [\[MS-ADTS\]](#) section 3.1.1.1.4.

contact: (1) A presence entity (**presentity**) whose presence information can be tracked.

(2) An object of the contact class that represents a company or person whom a user can contact.

(3) A person, company, or other entity that is stored in a directory and is associated with one or more unique identifiers and **attributes** (2), such as an Internet message address or login name.

(4) A **node** that publishes a **contact record**. **Contacts** are used by **graph maintenance** to detect partitions.

contact identifier: A **universally unique identifier (UUID)** that identifies a partner in the MSDTC Connection Manager: OleTx Transports Protocol. These **UUIDs** are frequently converted to and from string representations. This string representation must follow the format specified in [\[C706\]](#) Appendix A. In addition, the **UUIDs** must be compared, as specified in C706-AppendixAUUID.

contact record: A **record** published by a **contact** that includes the **contact's** address and the **graph signature** at the time of publication.

container: (1) A data model that is used to store published **presence** (1) information and a list of subscribers who are permitted to view that information. It enables a publisher to publish

different data values of the same **category** (4) and instance, which enables different subscribers to see different values.

(2) An **object** in the directory that can serve as the parent for other **objects**. In the absence of schema constraints, all **objects** would be **containers**. The schema allows only **objects** of specific classes to be **containers**.

container record: A record that defines the structure and hierarchy of **atom records** and other container records.

content: (1) Multimedia data. **content** is always in **ASF**, for example, a single **ASF** music file or a single **ASF** video file. Data in general. A file that an application accesses. Examples of content include web pages and documents stored on either web servers or SMB file servers.

(2) Items that correspond to a file that an application attempts to access. Examples of **content** include web pages and documents stored on either HTTP servers or SMB file servers. Each **content** item consists of an ordered collection of one or more **segments**.

(3) A package that contains all the associated files for an **update** that is to be installed on a **client computer**.

(4) Identified by a unique name under a given multicast namespace. The **content metadata** cannot change during the lifetime of a multicast session, and is required to allow random access to the data.

content app: An **app for Office** that appears within the content of a **document**.

content database: A database that is stored on a **back-end database server** and contains stored procedures, site collections, and the contents of those site collections.

content index extension (.cix) file: A file that is part of a **full-text index catalog**. It is used to store compressed document identifiers and OccCount values for data that is stored in an associated content index file.

content index file: A file that is part of a **full-text index catalog**. It is used to store data from items as an inverted index and it enables searches for specific terms across items.

content index record: A part of a content index file that is used to store all of the document identifiers for items that have a unique combination of a token and a property identifier.

Content Metadata: Specifies an opaque binary data that is associated with the content.

content source: A set of options for specifying the type of content to be crawled and the start addresses for the content to be indexed. A content source is defined by the protocol handler that is used to access specific systems, such as SharePoint sites, file systems, and external websites. A content source can contain up to 500 start addresses.

content type: A named and uniquely identifiable collection of settings and fields that store metadata for individual items in a SharePoint list. One or more content types can be associated with a list, which restricts the contents to items of those types.

content type group: A named category of **content types** that is used to organize content types of a similar purpose.

content type identifier: A unique identifier that is assigned to a **content type**.

content type order: The sequence in which **content types** are displayed.

content type package: A file that contains the definition of and related objects for a **content type**.

content type schema: An **XML** definition that describes the contents of a **content type**.

content type subscriber: A site collection that is connected to a shared service application that provides **content types**.

Content-Type header: A message header field whose value describes the type of data that is in the body of the message.

context: (1) A collection of context properties that describe an execution environment.

(2) An abstract concept that represents an association between a resource and a set of messages that are exchanged between a **client** and a **server**. A context is uniquely identified by a **context identifier**.

(3) Logical container spaces where objects exist "together" in memory and can efficiently communicate with each other.

context identifier: (1) A **GUID** that identifies a **context**.

(2) A set of name-value pairs where each name in the set is unique.

context site: A site that corresponds to the context of the current request.

contextual tab: A tab on the ribbon that displays commands related to the **active selection** or object.

contributing source (CSRC): A source of a **stream** of **RTP packets** that has contributed to the combined **stream** produced by an RTP **mixer**. The **mixer** inserts a list of the synchronization source (SSRC) identifiers of the sources that contributed to the generation of a particular packet into the RTP header of that packet. This list is called the CSRC list. An example application is audio conferencing where a **mixer** indicates all the talkers whose speech was combined to produce the outgoing packet, allowing the receiver to indicate the current talker, even though all the audio packets contain the same SSRC identifier (that of the **mixer**). See [\[RFC3550\]](#) section 3.

control: A graphical user interface object that users interact with when working with applications, forms, documents, webpages, and other types of files.

control button: A button in the user interface.

control level: The permissions that are granted to a **participant** in a **shared** desktop. The **control levels** include "view" (the **participant** is able to see, but not interact with, **shared** content), "full" (the **participant** is able to both see and interact with **shared** content), and "none" (the **participant** can neither see nor interact with **shared** content).

control template: A fragment of **HTML** and **ASP.NET** markup that customizes and extends the functionality of an **ASP.NET control**.

controlled agent: An Interactive Connectivity Establishment (ICE) agent that waits for the controlling agent to select the final **candidate pairs** to be used.

controlling agent: An **Interactive Connectivity Establishment (ICE)** agent that is responsible for selecting and signaling the final **candidate pair** that is selected by connectivity checks. The controlling agent signals the final **candidates** in a **Simple Traversal**

of UDP through NAT (STUN) binding request and an updated offer. In a session, one of the agents is a controlling agent and the other agent is a controlled agent.

conversation: (1) A single representation of a send/response series of email messages. A conversation appears in the Inbox as one unit and allows the user to view and read the series of related email messages in a single effort.

(2) In **LU 6.2, conversations** connect transaction programs, and are used by the transaction programs to transfer messages. For a more complete definition, see [\[LU62Peer\]](#).

conversion group: A data structure that contains information about one or more **conversion items** in a conversion job. The items are organized into a hierarchy that is based on input and output path values for the conversion items.

conversion item: A data structure that contains information about operations to convert a file from one file format to another. This information includes a unique identifier for the conversion item and the location of the source file to convert.

conversion job: A data structure that contains information about one or more **conversion items** or conversion groups that are associated with it. This information includes preferred settings for conversion operations to be performed for the conversion items that it contains.

cookie: (1) A small data file that is stored on a user's computer and carries state information between participating protocol servers and protocol clients.

(2) A randomly generated, 16-byte sequence that is used to authenticate the client to the server during the creation of a multitransport connection.

(3) An HTTP header that carries state information between participating origin servers and user agents. For more information, see [\[RFC2109\]](#).

coordinate space: A space based on Cartesian coordinates, which provides a means of specifying the location of each point in the space. A two-dimensional coordinate space requires two axes that are perpendicular and equal in length. Three two-dimensional coordinate spaces are generally used to describe an output surface: world, **page**, and **device**. To scale device-independent output for a particular physical device, a rectangular area in the world or **page** coordinate space is mapped into the **device** coordinate space using a **transform**.

Coordinated Universal Time (UTC): A high-precision atomic time standard that approximately tracks Universal Time (UT). It is the basis for legal, civil time all over the Earth. Time zones around the world are expressed as positive and negative offsets from UTC. In this role, it is also referred to as Zulu time (Z) and Greenwich Mean Time (GMT). In these specifications, all references to UTC refer to the time at UTC-0 (or GMT).

crawl: The process of traversing a URL space to acquire items to record in a **search catalog**.

crawl account: A user account that has access to all of the content that is traversed by a crawl component.

crawl component: A search component that traverses content in a URL space and acquires items to be stored in a **full-text index catalog** and metadata index.

crawl log: A set of properties that provides information about the results of crawling a **display URL**. The information includes whether the crawl was successful, the content source of the display URL, and the level, message, time, and identifier for any errors that occur.

crawl mapping: A mapping that associates an **access URL**, which is used to obtain an item from a content source, and a **display URL**, which is the address of the item.

crawl queue: A data structure that stores the list of items to crawl next.

crawl rule: A set of preferences that applies to a specific URL or range of URLs. A crawl rule can be used to include or exclude items in a crawl and to specify the content access account to use when crawling that URL or range of URLs.

crawled property: A type of metadata that can be discovered during a crawl and applied to one or more items. It can be promoted to a managed property. See also **managed property**.

crawler: A process that browses and indexes content from a content source.

Creator: A type of **MethodInstance** that can be called to create a new EntityInstance. The set of Fields that are required to create the EntityInstance is referred to as the Creator View.

credential: Previously established, **authentication** (2) data that is used by a security principal to establish its own identity. When used in reference to the Netlogon Protocol, it is the data that is stored in the NETLOGON_CREDENTIAL structure.

cross-site scripting: A type of security vulnerability that enables malicious users to insert client-side script into webpages and to run that script when those pages are viewed by other users. The script might then gain access to user-specific data, such as cookies, cached objects, and application settings. Also referred to as XSS.

Cryptographic Application Programming Interface (CAPI) or CryptoAPI: The Microsoft cryptographic application programming interface (API). An API that enables application developers to add **authentication** (2), encoding, and encryption to Windows-based applications.

cryptographic context: A set of cryptographic state information that is maintained in a Secure Real-Time Transport Protocol (SRTP) stream.

cryptographic hash function: A function that maps an input of any length to a short output bit string of fixed length, such that finding an input that maps to a particular bit string of the correct output length, or even finding two inputs that map to the same output bit string, is computationally infeasible. For more information, see [SCHNEIER] chapters 2 and 18.

cryptographic service provider: An independent software module that performs **authentication** (2), encoding, and encryption services that Windows-based applications access through the CryptoAPI.

cryptographic service provider (CSP): A software module that implements cryptographic functions for calling applications that generates digital signatures. Multiple **CSPs** may be installed. A **CSP** is identified by a name represented by a NULL-terminated Unicode string.

CSOM action: An individual method, property, or lookup operation that is performed by a protocol server in a request.

CSOM action list: A sequential list of **CSOM actions** that are defined in a CSOM request to be executed by a protocol server.

CSOM array: An ordered collection of values that can be used in an **XML** request or **JSON** response text. The values are identified by their position and their position is determined by a zero-based integer index.

CSOM binary: An array of 8-bit, unsigned integers that can be used in an **XML** request or as a string in **JSON** response text.

CSOM Boolean: A **Boolean** value that can be used in an **XML** request or **JSON** response text. A CSOM Boolean value is either "true" or "false".

CSOM Byte: An 8-bit, unsigned integer value that represents the BYTE type, as described in [\[MS-DTYP\]](#). The range of CSOM Byte values is 0-255 and it has different representations, depending on whether it is used in an **XML** request or **JSON** response text.

CSOM Char: A **Unicode** character value that can be used in an **XML** request or as a string in **JSON** response text.

CSOM DateTime: An Int64 value that represents the number of 100-nanosecond time intervals that have elapsed since 12:00:00, January 1, 0001. It can be used in an **XML** request or as a string in **JSON** response text. The value can represent time intervals through 23:59:59.9999999, December 31, 9999. It can also specify whether a local, **UTC**, or no **time zone** applies.

CSOM dictionary: An object that contains an unordered collection of key/value pairs that can be used in an **XML** request or **JSON** response text. Each key in a CSOM dictionary has a unique name.

CSOM Double: A 64-bit, double-precision, floating-point value, which is the DOUBLE type described in [\[MS-DTYP\]](#), that can be used in an **XML** request or as a number in **JSON** response text. The range of CSOM Double values is from "-1.79769313486232e308" to "1.79769313486232e308".

CSOM error: An object that contains information about an error that occurred on a protocol server when processing a request.

CSOM expando field: A field that stores data for an instance of a **CSOM Object** and is not defined explicitly in the corresponding **CSOM Object type**.

CSOM GUID: A **GUID**, as described in [\[MS-DTYP\]](#), that can be used in an **XML** request or as a string in **JSON** response text.

CSOM Int16: A 16-bit, signed integer value, which is the INT16 type described in [\[MS-DTYP\]](#), that can be used in an **XML** request or as a number in **JSON** response text. The range of CSOM Int16 values is from "-32768" to "32767".

CSOM Int32: A 32-bit, signed integer value, which is the INT32 type described in [\[MS-DTYP\]](#), that can be used in an **XML** request or as a number in **JSON** response text. The range of CSOM Int32 values is from "-2147483648" to "2147483647".

CSOM Int64: A 64-bit, signed integer value, which is the INT64 type described in [\[MS-DTYP\]](#), that can be used in an **XML** request or as a number in **JSON** response text. The range of CSOM Int64 values is from "-9223372036854775808" to "9223372036854775807".

CSOM method: A procedure that is executed by a protocol server for a **CSOM Object**.

CSOM Object: An object that contains a set of members, which are named values and methods. It has a Unicode string value, which is referred to as a CSOM type name, that identifies its type.

CSOM Object type: A reference to a standard definition of methods, properties, and behavior for a logical object in the SharePoint Client-Side Object Model.

CSOM property: A representation of a field of data that is stored for a type of **CSOM Object**.

CSOM SByte: An 8-bit, signed integer value, which is the INT8 type described in [MS-DTYP], that can be used in an **XML** request or as a number in **JSON** response text. The range of CSOM SByte values is from "-128" to "127".

CSOM Single: A 32-bit, single-precision, floating-point value, which is the FLOAT type described in [MS-DTYP], that can be used in an **XML** request or as a number in **JSON** response text. The range of CSOM Single values is from "-3.402823e38" to "3.402823e38".

CSOM String: A representation of text as a series of **Unicode** characters. It can be used in an **XML** request or **JSON** response text.

CSOM type: A predefined set of named values that enable a protocol client to access standard descriptions of exposed objects, members, and enumerations. A CSOM type can be a **CSOM Object type**, CSOM value object type, or CSOM enumeration.

CSOM type identifier: A **GUID** that is used to identify a **CSOM type**.

CSOM type name: A **Unicode** string that identifies the type of a **CSOM Object**.

CSOM UInt16: A 16-bit, unsigned integer value, which is the UINT16 type described in [MS-DTYP], that can be used in an **XML** request or as a number in **JSON** response text. The range of CSOM UInt16 values is from "0" to "65535".

CSOM UInt32: A 32-bit, unsigned integer value, which is the UINT32 type described in [MS-DTYP], that can be used in an **XML** request or as a number in **JSON** response text. The range of CSOM UInt32 values is from "0" to "4294967295".

CSOM UInt64: A 64-bit, unsigned integer value, which is the UINT64 type described in [MS-DTYP], that can be used in an **XML** request or as a number in **JSON** response text. The range of CSOM UInt64 values is from "0" to "18446744073709551615".

CSOM value object: An object that contains a set of named values, which are referred to as members. It has a Unicode string value, referred to as a CSOM type name, that identifies its type.

CSOM value object type: A CSOM type that contains a set of named values, which are referred to as members. It has type information, which is identified by a **Unicode** string, and is associated with a specific identifier, which is a **CSOM GUID**.

CSS: See **cascading style sheet (CSS)**.

cube: A set of data that is organized and summarized into a multidimensional structure that is defined by a set of **dimensions** (1) and **measures**.

cube function: A function that is used to extract and display Online Analytical Processing (OLAP) data sets and values.

culture name: A part of a language identification tagging system, as described in [RFC1766](#). Culture names adhere to the format "<languagecode2>-<country/regioncode2>." If a two-letter language code is not available, a three-letter code that is derived from [ISO-639](#) is used.

curly braced GUID string: The string representation of a 128-bit globally unique identifier (**GUID**) using the form {XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}, where X denotes a hexadecimal digit. The string representation between the enclosing braces is the standard

representation of a GUID as described in [RFC4122] section 3. Unlike a GUIDString, a curly braced GUID string includes enclosing braces.

current navigation menu: The navigation menu that appears vertically on the left side of the default **master page** and shows the set of current **navigation nodes**.

current resource policy: While in the running **management state**, the **management service** always selects exactly one **RAP** to be the **current resource policy**.

current user: The user who is authenticated during processing operations on a **front-end web server** or a **back-end database server**.

current version: The latest version of a document that is available to a user, based on the permissions of the user and the publishing level of the document.

cursor: (1) A data structure providing sequential access over a **message queue**. A cursor has a current pointer that lies between the head and tail pointer of the **queue**. The pointer can be moved forward or backward through an operation on the cursor (Next). A **message** at the current pointer can be accessed through a nondestructive read (Peek) operation or a destructive read (Receive) operation.

(2) An entity that is used as a mechanism to work with one **row** or a small block of **rows** (at one time) in a set of data returned in a result set. A **cursor** is positioned on a single **row** within the result set. After the **cursor** is positioned on a **row**, operations can be performed on that **row** or on a block of **rows** starting at that position.

(3) The current position within a **result set**.

custodian: A user that is part of a discovery litigation that allows attorneys to associate users with the **discovery sources**.

custom action: An extension to the user interface, such as a button on a toolbar or a link on a site settings page.

custom filter: A filter that contains preconfigured expressions in which users can optionally enter a string to filter data.

custom label filter: A custom filter that is applied to string labels for data.

custom list: A user-defined **list** (2) or enumeration that can be used to sort data in a worksheet.

custom rollup: An **aggregation** (1) calculation that is customized for a dimension level, dimension member, or measure. A custom rollup contains a custom formula or operator, overrides the aggregate functions of a cube's measures, and is defined on a hierarchy.

custom toolbar: A type of toolbar that contains a user-defined set of controls and is not included in an application by default. A custom toolbar has a toolbar identifier value of "1".

custom toolbar control: A user-defined control that can be added to a toolbar. A custom toolbar control has a **toolbar control identifier (TCID)** value of "1" and can be one of the following types of controls: ActiveX, Button, ComboBox, DropDown, Edit, or Popup.

custom value filter: A custom filter that is applied to the numerical values of data.

custom view: A collection of display and print settings that users can name and save. Users can switch between custom views to change settings quickly.

customized: (1) A document whose content is stored in a content database instead of a front-end file system. Also referred to as unhosted.

(2) A **column** (1) or content type whose schema is stored in a content database instead of a front-end file system. Also referred to as unhosted.

cyclic redundancy check (CRC): An algorithm used to produce a **checksum** (a small, fixed number of bits) against a block of data, such as a packet of network traffic or a block of a computer file. The CRC is used to detect errors after transmission or storage. A CRC is designed to catch random errors, as opposed to intentional errors. If errors might be introduced by a motivated and intelligent adversary, a **cryptographic hash function** should be used instead.

6 D

DAO: See **Data Access Objects (DAO)**.

dashboard: A visual interface that displays a related group of interactive scorecard and report views. It provides views into key measures that are relevant to a business practice or process. Dashboard elements provide capabilities, such as shared filters, that enable users to perform tasks such as highlighting trends, comparing data, and controlling the data that is displayed.

Data Access Objects (DAO): A programming interface that can be used to access and manipulate database objects.

data adapter: Code that submits data to and retrieves data from an external data source. Also referred to as data provider.

data bar: A graphical representation of cell content as a bar graph.

data connection: (1) A link between an application and a data source. Data connections can be used to query and submit data.

(2) A collection of information, such as the type and location, that defines how to connect to an external data source, such as a database, **web service**, SharePoint list, or **XML** file.

(3) A connection between an InfoPath form template and an external data source, as specified by settings in an InfoPath **form template (.xsn) file** or a **Universal Data Connection (.udc, .udcx) file**.

data connection library: A SharePoint library that contains a collection of universal data connection (.udcx) and Office data connection (.odc) files.

data consolidation: The process of combining tabular data from various worksheets into a single list.

data culture: The language that is used to specify number formatting for data.

Data Encryption Standard (DES): A specification for **encryption** of computer data that uses a 56-bit key developed by IBM and adopted by the U.S. government as a standard in 1976. For more information see [\[FIPS46-3\]](#).

data macro: A component that implements application logic and enables recognition of built-in actions and tasks for list items.

data marker: A customizable symbol or shape that identifies a data point on a line, scatter, or radar chart. A data marker can be formatted with various sizes and colors.

data point: (1) An individual value that is plotted in a chart and is represented together with other data points by bars, **columns** (2), lines, pie or doughnut slices, dots, and various other shapes, which are referred to as data markers. Data markers of the same color constitute a data series.

(2) A representation of a PivotTable item in a PivotTable data field contained in a PivotChart report.

(3) A prototype for the data values that are displayed by a chart series. Data points can be displayed in different shapes depending on the **chart** type.

data provider: A known data source that is specific to a target type and that provides data to a collector type.

data range: A set of consecutive scale-out partition keys.

data recovery: A process in which files are repaired through error correction or restored from backup media.

data region: A region of a table that encompasses the range of cells that contains the table records. A data region does not include the **header row** (1), insert row, or total row of a table.

data source: (1) A database, web service, disk, file, or other collection of information from which data is queried or submitted. Supported data sources vary based on application and data provider.

(2) A collection of fields and groups that define and store the data for an InfoPath form. Controls in a form are bound to the fields and groups in the data sources of the form. See also **main data source** and **secondary data source**.

(3) A specified data source type, connection string, and credentials, which can be saved separately to a report server and shared among report projects or embedded in a report definition (.rdl) file.

(4) A physical data source.

data source control: An object that can be added to an **ASP.NET** webpage and encapsulates the necessary logic to connect to a data source, such as a database or **XML** file, and that can execute queries or other data-access commands. A data source control can in turn provide data to other controls on that page.

data table: (1) A range of cells that is designated to perform what-if analysis for formulas, based on various input values.

(2) A grid that can be added to some charts and contains the numeric data that is plotted in the chart.

data type: (1) A property of a field that defines the kind of data that is stored in the field, or defines the kind of data returned by an expression when the expression is evaluated.

(2) A string that specifies the format of data that a printing application sends to a printer in a **print job**. Data types include **enhanced metafile spool format (EMFSPool)** and **RAW format**. For rules governing **data type** names, see section 2.2.4.2.

data validation: The process of testing the accuracy of data; a set of rules that specify the type and range of data that users can enter.

data validation criteria: See **data validation**.

data value: An instance of a **Remoting Type**, which may be a **Class**, **Array**, **Enum**, or Primitive. A **Data Value** is part of the **Remoting Data Model**. For more information, see [MS-NRTP] section 3.1.1.

database: (1) For the purposes of the Netlogon RPC, a database is a collection of user accounts, machine accounts, aliases, groups, and policies, managed by a component. The database, or the component managing the database, must expose a mechanism to enable Netlogon to

gather changes from and apply changes to the database. Additionally, it must export a database serial number in order to track changes for efficient replication.

(2) In **Distributed File System Replication (DFS-R)**, the database maintained by the Microsoft implementation of **DFS-R** maintains the local version chain vector and one record for each resource that is tracked, including **tombstones** for deleted resources, such that deletion of files can be propagated in a timely fashion.

(3) The set of all non-expired **records** published in a **graph**.

database application: A set of objects, including tables, queries, forms, reports, macros, and code modules, that are stored in a database structure.

database object: (1) An object such as a table, query, form, report, macro, or module that can be referenced by name in a database, database application, or database project.

(2) A representation of a named set of attribute value pairs that a protocol exposes.

DataClass: A type of **MetadataObject** that represents a type of a business data object obtained from a **line-of-business (LOB) system**. Instances of a DataClass have transient identity. DataClasses are contained by **LobSystems** and Methods.

datagram: A style of communication offered by a network transport protocol where each message is contained within a single network packet. In this style, there is no requirement for establishing a session prior to communication, as opposed to a connection-oriented style.

dataset: (1) A set of multidimensional data that is returned when a multidimensional expression (MDX) SELECT statement is executed. A dataset represents a slice of a cube as defined by the members and axes that are specified in the query.

(2) A named specification that includes a data source definition, a query definition, and optional parameter values, calculated fields, and filtering and collation information as part of a report definition (.rdl) file. An .rdl file can have multiple datasets.

datasheet: A worksheet window that contains the source data for a Microsoft Graph chart object.

date system: A method of calculating calendar dates and times.

datetime: A data type that represents the date and time when a document can be normalized and indexed as a numeric value by a search application. The range and degree of granularity varies according to search application and implementation.

DCOM: See **Distributed Component Object Model (DCOM)**. Can also refer to the Distributed Component Object Model (DCOM) Remote Protocol Specification [MS-DCOM].

DDE: See **Dynamic Data Exchange (DDE)**.

DDE link: A connection between a **Dynamic Data Exchange (DDE)** source document and a destination document.

DDE server: An application that responds to a **Dynamic Data Exchange (DDE)** request from a DDE client application.

DDE topic: A general classification of information about a **Dynamic Data Exchange (DDE)** server within which multiple, specific data items related to the topic can be exchanged.

declarative workflow: A workflow that is created with XAML (Extensible Application Markup Language) files and does not require precompiled code to run.

decryption: In cryptography, the process of transforming encrypted information to its original clear text form.

deep refinement: A type of query refinement that is based on the aggregation of managed property statistics for all of the results of a search query. See also **shallow refinement**.

default candidate: A **candidate** that is designated for streaming media before connectivity checks can be finished. The candidate that is most likely to stream media to the remote **endpoint** (5) successfully is designated as the default candidate.

default candidate pair: A **candidate pair** that consists of the **caller's default candidate** and the **callee's** default candidate.

default column: The **column** (2) that is used if no column is specified.

default filter value: The filter value that is used if no filter is specified.

default font face color: The font face color that is applied to a cell if no font face color is specified.

default list view: The view of a SharePoint list that the owner of the list selected to appear when users browse to the list without specifying a view.

default mobile list view: The view of a SharePoint list that the owner of the list selected to appear when users browse to the list by using a mobile device and without specifying a view.

default row: The row that is used if no row is specified.

default sheet: The sheet that is displayed if no sheet is specified.

default sheet tab color: The color that is used for a worksheet tab if no color is specified.

default view: The layout and organization of a document or list that appears automatically when users open that document or display that list.

DefaultValue: A value that is associated with a **TypeDescriptor**, in the context of a **MethodInstance**, and is used to instantiate **Parameter** values when calling native APIs in a line-of-business (LOB) system. The type of the value is consistent with the data type represented by the **TypeDescriptor**.

defined name: A word or string of characters in a formula that represents a cell, range of cells, formula, or constant value.

delegate: A user or resource that has permissions to act on behalf of another user or resource.

delegation: (1) A model of communication between server components in which the caller can make requests on behalf of a user by passing a service ticket that was retrieved for that user.

(2) A name server (NS) record set in a parent **zone** that lists the name servers **authoritative** for a delegated subzone.

delegator: A user or resource for which another user or resource has permission to act on its behalf.

delete crawl: A process that is started automatically after a content source or start address deletion occurs and removes associated items from a **search catalog**.

DeletedIdEnumerator: A type of **MethodInstance** that can be called to retrieve EntityInstanceIds of EntityInstances that were deleted from a line-of-business (LOB) system after the specified time.

deleted-object: An **object** that has been deleted, but remains in storage until a configured amount of time (the **deleted-object lifetime**) has passed, after which the **object** is transformed to a **recycled-object**. Unlike a **recycled-object** or a **tombstone**, a **deleted-object** maintains virtually all the state of the **object** before deletion, and may be undeleted without loss of information. **Deleted-objects** exist only when the **Recycle Bin optional feature** is enabled.

deleted-object lifetime: The time period that a **deleted-object** is kept in storage before it is transformed into a **recycled-object**.

Deleter: A type of **MethodInstance** that can be called to delete an EntityInstance with a specified EntityInstanceId.

delta: (1) A unit of transactional consistency in a **shared space**. A delta can contain one or more commands.

(2) One of a set of possible changes that can be made to a **database**.

delta address book file: An **address book file** that contains only the differences between two complete address book files. Differences can include changed values, added objects, and deleted objects.

delta import: A step in the staging process that reads in only the changes that have occurred in a connected data source since the last import.

delta synchronization: A staging step that processes only those objects that have pending imports.

dependent lookup field: A lookup field that displays additional data for an item that is returned by a primary lookup field. See also **primary lookup field**.

deployment: (1) A collection of protocol clients and protocol **servers** (2) that belong to the same enterprise.

(2) An administratively specified decision to make a specific **update revision** available to a specific **target group**.

deployment manifest: An **XML** file that describes the identity and version of a **deployment package** (2).

deployment package: (1) A collection of files that represent a serialized snapshot of data. A deployment package is stored as **XML** files that describe the deployment objects and their relationships, and a binary file for each object. Optionally, the resulting set of files can be compressed into one or more files in the compressed PRIME data format (CMP).

(2) A collection of files that can be used to deploy and manage customizations, such as **add-ins**, to a computer. It consists of an **application manifest**, a deployment manifest, and related package files.

deprecated term: A term that persists in the term store but cannot be used in future applications of metadata.

derived transport address: An address that derives from a local transport address. It is obtained by using protocols such as Simple Traversal of UDP through NAT (STUN) and Traversal Using Relay NAT (TURN). When a packet is sent to a derived transport address it arrives at the local transport address from which it is derived.

descendant: A member that is below the current member in a hierarchy.

descendant content type: Any **content type** that inherits settings from another content type.

descending order: A sort order in which text strings are arranged in reverse alphabetical order, numerical values are arranged from largest to smallest, and dates and times are arranged from newest to oldest.

deserialize: See **unmarshal** (1).

designer: A visual design surface for adding and arranging controls on a user form and writing code for those controls.

destination: A network entry in the **routing table** represented by a network address and a network mask.

destination server: (1) A protocol server to which a file is copied.

(2) The host name (as specified in [\[RFC1738\]](#) section 5) in the destination URL. This is the host where the **CER server** is running.

device: (1) A client or server computer that uses a **device URL** to identify itself as an **endpoint** (5) for synchronizing account data.

(2) Any peripheral or part of a computer system that can send or receive data.

(3) The Devices Profile for Web Services (DPWS) term for a special instance of a service that is discoverable and contains other services with metadata describing those services.

(4) A logical device and/or a container that may embed other logical devices and that embeds one or more services and advertises its presence on network(s). For more information, see [\[UPNPARCH1.1\]](#) sections 1 and 2.

(5) A device can be any UPnP-enabled device.

device key: A secret key that is shared between a relay server and a client device for device **authentication** (2).

device URL: A unique identifier for a client device, as described in [\[RFC3986\]](#).

device-independent bitmap (DIB): (1) A file format that was designed to help ensure that bitmap graphics that were created by using one application can be loaded and displayed in another application exactly as they appeared in the originating application.

(2) A container for bitmapped graphics, which specifies characteristics of the **bitmap** such that it can be created using one application and loaded and displayed in another application, while retaining an identical appearance.

DFS-R: A service that keeps **DFS** and **SYSVOL** folders in sync automatically. DFS-R is a state-based, multimaster replication system that supports replication scheduling and bandwidth throttling. This is a rewrite and new version of **FRS**. For more information, see [\[MS-FRS2\]](#).

DHCP client: The **remote procedure call (RPC) clients** that use the Dynamic Host Configuration Protocol Server Management Protocol (DHCPM) to configure, manage, and monitor the Dynamic Host Configuration Protocol (DHCP) **server**.

diagonal-down: A cell **border formatting** that displays a line diagonally from the top left corner of a cell to the bottom right corner.

diagonal-up: A cell **border formatting** that displays a line diagonally from the bottom left corner of a cell to the top right corner.

dial plan: The rules that govern the translation of dial strings into **SIP** and tel **URIs**, either global or local, as described in [\[RFC3966\]](#).

dial string: The numbers, symbols, and pauses that users enter to place a phone call. It is consumed by one or more network entities and understood in the context of the configuration of those entities. It is used to generate an **address-of-record** or identifier to route a **call**.

dialog: (1) A peer-to-peer **Session Initiation Protocol (SIP)** relationship that exists between two **user agents** and persists for a period of time. A dialog is established by **SIP messages**, such as a 2xx response to an INVITE request, and is identified by a call identifier, a local tag, and a remote tag.

(2) The exchange of messages between client and server over a given SMB connection.

(3) A peer-to-peer SIP relationship between two user agents that persists for some time. A dialog is established by SIP messages (for example, a 2xx response to an INVITE request). A dialog is identified by a call identifier, a local tag, and a remote tag.

dialog sheet: A single logical container that is used to create a custom dialog box.

dictionary: A collection of key/value pairs. Each pair consists of a unique key and an associated value. Values in the dictionary are retrieved by providing a key for which the dictionary returns the associated value.

digest: The fixed-length output string from a one-way hash function that takes a variable-length input string and is probabilistically unique for every different input string. Also a cryptographic checksum of a data (octet) stream.

digital certificate: See the "digital certificate definition standard," as described in [\[X509\]](#).

digital certificate store: A database that stores a variety of **digital certificates** and information about those certificates, including attributes and constraints.

digital signature: (1) A message authenticator that is typically derived from a cryptographic operation by using an asymmetric algorithm and private key. When a symmetric algorithm is used for this purpose, the authenticator is typically referred to as a Message Authentication Code (MAC).

(2) A value that is generated by using a digital signature algorithm, taking as input a private key and an arbitrary-length string, such that a specific verification algorithm is satisfied by the value, the input string, and the public key corresponding to the input private key.

(3) A message authenticator that is typically derived from a cryptographic operation using an asymmetric algorithm and **private key**. When a symmetric algorithm is used for this purpose, the authenticator is typically called a **Message Authentication Code (MAC)**. In some contexts, the term **digital signature** is used to refer to either type of authenticator; however, in this Windows Client Certificate Enrollment Protocol, the term **digital signature** is used only for authenticators created by asymmetric algorithms. For more information, see [SCHNEIER] chapters 2 and 20.

dimension: (1) A structural attribute of a cube, which is an organized hierarchy of categories (levels) that describe data in a fact table. These categories typically describe a similar set of members upon which the user bases an analysis.

(2) A categorization of data in rows or **columns** (2) in an Excel worksheet.

(3) A structural attribute of a cube, which is an organized hierarchy of categories (levels) that describe data in the fact table.

directory: (1) The database that stores information about objects such as users, groups, computers, printers, and the **directory service** that makes this information available to users and applications.

(2) A **forest**.

directory name: A segment of a **store-relative URL** that refers to a directory. A directory name is everything that appears before the last slash in a store-relative form URL.

directory object: (1) A **Lightweight Directory Access Protocol (LDAP)** object, as described in [RFC2251], that is a specialization of an object.

(2) A **Lightweight Directory Access Protocol (LDAP) object**, as specified in [RFC2251], that is a specialization of an **object**.

(3) An **Active Directory object**, which is a specialization of the "object" concept that is described in [MS-ADTS] section 1 or [MS-DRSR] section 1, Introduction, under Pervasive Concepts. An **Active Directory object** can be identified by the objectGUID **attribute** of a **dsname** according to the matching rules defined in [MS-DRSR] section 5.50, DSNAME. The **parent-identifying attribute** (not exposed as an **LDAP attribute**) is parent. **Active Directory objects** are similar to **LDAP entries**, as defined in [RFC2251]; the differences are specified in [MS-ADTS] section 3.1.1.3.1.

directory partition: A synonym for **Active Directory partition** and naming context (NC) replica.

directory server: A persistent storage for DNS **zones** and records. A DNS server can access DNS data stored in a **directory server** using the **LDAP** protocol or a similar directory access mechanism.

directory service (DS): (1) A service that stores and organizes information about a computer network's users and network shares, and that allows network administrators to manage users' access to the shares. See also **Active Directory**.

(2) An entity that maintains a collection of objects. These objects can be remotely manipulated either by the Message Queuing (MSMQ): Directory Service Protocol, as specified in [MS-MQDS], or by the Lightweight Directory Access Protocol (v3), as specified in [RFC2251].

(3) A distributed data storage system that allows computers connected to a network to store, edit, and retrieve information.

DirectPlay: A network communication library included with the Microsoft **DirectX** application programming interfaces. **DirectPlay** is a high-level software interface between applications and communication services that makes it easy to connect games over the Internet, a modem link, or a network.

DirectPlay 4: A programming library that implements the IDirectPlay4 programming interface.

DirectPlay 4 provides peer-to-peer session-layer services to applications, including session lifetime management, data management, and media abstraction. **DirectPlay 4** first shipped with the DirectX 6 multimedia toolkit. Later versions continued to ship up to, and including, DirectX 9. **DirectPlay 4** was subsequently deprecated. The **DirectPlay 4** DLL continues to ship in current versions of Windows operating systems, but the development library is no longer shipping in Microsoft development tools and software development kits (SDKs).

DirectPlay 8: A programming library that implements the IDirectPlay8 programming interface.

DirectPlay 8 provides peer-to-peer session-layer services to applications, including session lifetime management, data management, and media abstraction. **DirectPlay 8** first shipped with the DirectX 8 software development toolkit. Later versions continued to ship up to, and including, DirectX 9. **DirectPlay 8** was subsequently deprecated. The **DirectPlay 8** DLL continues to ship in current versions of Windows operating systems, but the development library is no longer shipping in Microsoft development tools and Software Development Kits (SDKs).

DirectX: Microsoft **DirectX** is a collection of application programming interfaces for handling tasks related to multimedia, especially game programming and video, on Microsoft platforms.

DirectX Diagnostic (DXDiag): DXDiag.exe is an application that uses the DirectPlay DXDiag Usage Protocol [\[MS-DPDX\]](#) traffic.

dirty: The condition of an entity, such as a component or a file, that indicates that the entity or properties of the entity were changed after the entity was last saved.

Disassociator: A type of **MethodInstance** that can be called to remove an association between a specified destination EntityInstance and a single specified EntityInstance for each of the sources of a specified Association.

disconnecter object: A **staging object** that is not linked to an object in the **metaverse**.

discovery case: A site that contains information relevant to an **electronic discovery (eDiscovery)** case such as a **custodian**, a **discovery source**, and saved searches.

discovery center: See **discovery console**.

discovery console: A **site collection** that contains multiple **discovery cases**.

discovery source: A repository of documents and other types of content that are relevant to the **electronic discovery (eDiscovery)** case.

discretionary access control list (DACL): An **access control list (ACL)** that is controlled by the owner of an object and that specifies the access particular users or groups can have to the object.

discussion board: A list in which users can read, post, and reply to messages from other users who are members of the same discussion board.

discussion bookmark: A data structure that is used to store the location of a comment in a web discussion about specific text in a document or on a webpage. See also [web discussion](#).

discussion item: A remark or response that is posted to an online discussion forum such as a newsgroup, SharePoint list, or electronic bulletin board.

disk extent: A contiguous set of one or more disk sectors. A disk extent can be used as a partition or part of a volume, or it can be free, which indicates that it is not in use or that it may be unusable for creating partitions or volumes.

DispID: See [IDispatch identifier \(DispID\)](#).

display folder: A folder into which attributes, measures, calculated members, and key performance indicators can be organized to facilitate browsing.

display form: A form that is used to display a list item.

display name: A text string that is used to identify a principal or other object in the user interface. Also referred to as title.

display units: An axis-formatting option that determines how numeric units are displayed on a value axis.

display URL: The URL that is displayed on a search results page for each search result. This can be different than an access URL. See also [access URL](#).

displayed version: Document version information that is formatted for display in the user interface. The displayed version uses the format MajorVersion.MinorVersion, where MajorVersion is the published version number and MinorVersion is the draft version number, separated by a decimal point. See also [major version](#) and [minor version](#).

Distinguished Encoding Rules (DER): A method for encoding a data object based on Basic Encoding Rules (BER) encoding but with additional constraints. DER is used to encode X.509 [certificates](#) (2) that need to be digitally signed or to have their signatures verified.

distinguished name (DN): (1) A name that uniquely identifies an object by using the [relative distinguished name \(RDN\)](#) for the object, and the names of container objects and domains that contain the object. The distinguished name (DN) identifies the object and its location in a tree.

(2) In the [Active Directory](#) directory service, the unique identifier of an object in [Active Directory](#), as described in [MS-ADTS] and [\[RFC2251\]](#).

(3) In X.500, the globally unique name string that identifies an entity in an X.500 directory, as described in [\[X500\]](#). The DN consists of several components and is used in X.509 [certificates](#) (2) to identify the subject and issuer principals, as described in [\[X509\]](#).

(4) In [Lightweight Directory Access Protocol \(LDAP\)](#), an [LDAP Distinguished Name](#), as described in [\[RFC2251\]](#) section 4.1.3. The DN of an object is the DN of its parent, preceded by the RDN of the object. For example: CN=David Thompson, OU=Users, DC=Microsoft, DC=COM. For definitions of CN and OU, see [\[RFC2256\]](#) sections 5.4 and 5.12, respectively.

(5) A name that uniquely identifies an object by using the [relative distinguished name \(RDN\)](#) for the object, plus the names of container objects and domains that contain the object. The **DN** identifies the object as well as its location in a tree.

(6) In the **Active Directory** directory service, the unique identifier of an object in **Active Directory**, as specified in [MS-ADTS] and [\[RFC2251\]](#).

(7) In X.500, the globally unique name string that identifies an entity in an X.500 directory, as specified in [\[X500\]](#). The **DN** consists of several components and is used in X.509 certificates to identify the subject and issuer principals, as specified in [\[X509\]](#).

(8) In **Lightweight Directory Access Protocol (LDAP)**, an **LDAP DN**, as specified in [\[RFC2251\]](#) section 4.1.3. The **DN** of an object is the **DN** of its parent, preceded by the **RDN** of the object. For example: CN=David Thompson,OU=Users,DC=Microsoft,DC=COM. For definitions of CN and OU, see [\[RFC2256\]](#) sections 5.4 and 5.12, respectively.

distributed alignment: A formatting setting that spreads text evenly, both vertically and horizontally, between the edges of a cell, object, or page. Distributed alignment is used primarily with East Asian languages. See also **justify distributed**.

Distributed Component Object Model (DCOM): The Microsoft Component Object Model (COM) specification that defines how components communicate over networks, as specified in [\[MS-DCOM\]](#).

Distributed File System (DFS): A file system that logically groups physical shared folders located on different servers by transparently connecting them to one or more hierarchical namespaces. **DFS** also provides fault-tolerance and load-sharing capabilities. **DFS** refers to the Microsoft DFS available in Windows Server platforms.

Distributed File System Replication (DFS-R): A service that keeps **DFS** folders in sync automatically. **DFS-R** is a state-based, multi-master replication system that supports replication scheduling and bandwidth throttling. This is a rewrite and new version of the **File Replication Service (FRS)**. For more information, see [MS-FRS2].

Distributed Management Task Force (DMTF): An industry organization that develops management standards and integration technology for enterprise and Internet environments.

distributed object: A collection of interfaces that enable a protocol client and a protocol **server** (2) to exchange messages with each other, and to use those messages to connect or disconnect from distributed objects and to call remote methods that have a predefined set of parameters. Each **instance** of a distributed object has a unique identifier, which ensures that messages are routed to the correct object.

distribution list: (1) A collection of users, computers, contacts, or other groups that is used only for email distribution, and addressed as a single recipient.

(2) An **Active Directory** object that can contain explicit references only to destinations published in **Active Directory**; that is, to **public queues**, queue aliases, and other distribution lists, but not to private and URL-named queues.

DocID skip: A **forward link** that allows the reader of a **content index record** or a scope index record to skip a group of **document identifiers**.

DocIDDelta: A number that represents the incremental difference in value between a document identifier and the document identifier that immediately precedes it in a list that is sorted in **ascending order**.

docked: A condition where a toolbar is attached to the **docking area** of an application window.

docked location: A specific position of a toolbar within the **docking area** of an application window.

docking area: An area that is adjacent to the edge of an application window. A toolbar can be moved and attached to a docking area.

document: (1) An object in a **content database** such as a file, folder, **list** (1), or **site** (2). Each object is identified by a **URI**.

(2) The term "document" that is defined in XMD/2.

document flag: A 4-byte unsigned integer bit mask that provides metadata about the document.

document identifier: (1) An integer that uniquely identifies a crawled item.

(2) A GUID that identifies a document.

(3) A string that uniquely identifies an item in a search index.

(4) A unique 32-bit, unsigned integer identifier that is consistent across all queries for each document corresponding to a search result.

document library: A type of list that is a container for documents and folders.

document property: A name/value pair that serves as metadata for a document.

document stream: A byte stream that is associated with a document, such as the content of a file. Some documents do not have document streams.

document template: (1) A file that serves as the basis for new documents.

(2) A file that contains predefined formatting, layout, text, or graphics and that serves as the basis for new documents with a similar design or purpose.

document version: A copy of a list item that has a version number. A document version can be either a historical version or a current version.

Document Workspace site: A SharePoint site that is based on a Document Workspace site template and has a template identifier value of "1". A Document Workspace site is used for planning, posting, and working together on a document or a set of related documents.

domain: (1) A set of users and computers sharing a common namespace and management infrastructure. At least one computer member of the set must act as a **domain controller (DC)** and host a member list that identifies all members of the domain, as well as optionally hosting the **Active Directory** service. The domain controller provides **authentication** (2) of members, creating a unit of trust for its members. Each domain has an identifier that is shared among its members.

(2) A set of users and computers sharing a common namespace and management infrastructure. At least one computer member of the set must act as a **domain controller** and host a member list that identifies all members of the domain, as well as optionally hosting the **Active Directory** service. The domain controller provides authentication of members, creating a unit of trust for its members. Each domain has an identifier that is shared among its members. For more information, see [MS-AUTHSOD] section 1.1.1.5 and [MS-ADTS].

(3) A capture of the data semantics. Example domains include email address, gender, and state.

domain account: A stored set of **attributes** (2) representing a principal used to authenticate a user or machine to an **Active Directory** domain.

domain certificate: An X.509 **certificate** (2) that is associated with a management domain, as described in [\[X509\]](#). It contains the public key that is used to help secure registration transactions between protocol clients and protocol servers.

domain client in a workstation role: A domain member that offers other services to other domain clients.

domain controller (DC): The service, running on a server, that implements **Active Directory**, or the server hosting this service. The service hosts the data store for **objects** and interoperates with other **DCs** to ensure that a local change to an **object** replicates correctly across all **DCs**. When **Active Directory** is operating as **Active Directory Domain Services (AD DS)**, the **DC** contains full NC replicas of the **configuration naming context (config NC)**, **schema naming context (schema NC)**, and one of the **domain NCs** in its **forest**. If the **AD DS DC** is a **global catalog server (GC server)**, it contains partial NC replicas of the remaining **domain NCs** in its **forest**. For more information, see [MS-AUTHSOD] section 1.1.1.5.2. When **Active Directory** is operating as **Active Directory Lightweight Directory Services (AD LDS)**, several **AD LDS DCs** can run on one server. When **Active Directory** is operating as **AD DS**, only one **AD DS DC** can run on one server. However, several **AD LDS DCs** can coexist with one **AD DS DC** on one server. The **AD LDS DC** contains full NC replicas of the **config NC** and the **schema NC** in its **forest**.

domain controller server: A domain member, which can be a client or a server that offers other services to its clients. When the domain client acts as a supplicant to another domain client, the supplicant is referred to as a **domain client in a workstation role** and the latter as a domain client in a server role.

domain group: A container for security and distribution groups. A domain group can also contain other domain groups.

domain local group: An **Active Directory group** (1) that allows **user objects**, **global groups**, and **universal groups** from any **domain** as members. It also allows other domain local groups from within its **domain** as members. A **group object** *g* is a **domain local group** if and only if `GROUP_TYPE_RESOURCE_GROUP` is present in `g!groupType`. A security-enabled **domain local group** is valid for inclusion within **access control lists (ACLs)** from its own **domain**. If a **domain** is in **mixed mode**, then a security-enabled **domain local group** in that **domain** allows only **user objects** as members.

domain member (member machine): A machine that is joined to a domain by sharing a secret between the machine and the domain.

domain name: (1) The name given by an administrator to a collection of networked computers that share a common directory. Part of the domain naming service naming structure, domain names consist of a sequence of name labels separated by periods.

(2) A name with a structure indicated by dots.

(3) A **domain name** (2) used by the **Domain Name System (DNS)**.

(4) A **domain name** (3) or a **NetBIOS name** that identifies a **domain**.

Domain Name System (DNS): A hierarchical, distributed database that contains mappings of **domain names** (1) to various types of data, such as IP addresses. DNS enables the location of computers and services by user-friendly names, and it also enables the discovery of other information stored in the database.

domain naming context (domain NC): (1) A partition of the directory that contains information about the domain and is replicated with other **domain controllers (DCs)** in the same domain.

(2) A **naming context (NC)** whose replicas are able to contain **security principal** objects. No other **NC replica** can contain **security principal** objects. The **distinguished name (DN)** of a **domain NC** takes the form "dc=n1,dc=n2, ... dc=nk" where each ni satisfies the syntactic requirements of a DNS name component. For more information, see [\[RFC1034\]](#). Such a **DN** corresponds to the **domain naming service name**: "n1.n2.nk". This is the **domain naming service name** of the **domain NC**. **Domain NCs** appear in the **global catalog (GC)**. A **forest** has one or more **domain NCs**. The root of a **domain NC** is an object of class domainDns.

(3) A specific type of **naming context (NC)** that represents a **domain**. A **domain NC** can contain **security principal objects**; no other type of **NC** can contain **security principal objects**. **Domain NCs** appear in the **global catalog (GC)**. A **domain NC** is hosted by one or more **domain controllers (DCs)** operating as **AD DS**. In **AD DS**, a **forest** has one or more **domain NCs**. The root of a **domain NC** is an **object of class** domainDNS; for directory replication [MS-DRSR], see **domainDNS**. A **domain NC** cannot exist in **AD LDS**.

domain naming service name: The **fully qualified domain name (FQDN)** as known by the domain name system (DNS), as specified in [\[RFC1035\]](#) and [\[RFC1123\]](#).

domain user: A user with an account in the domain's user account database.

domainDNS: A specific **object class**. The root of a **domain NC** or an **application NC** is an **object of class** domainDNS. The **DN** of such an **object** takes the form dc=n1,dc=n2, ... dc=nk, where each ni satisfies the syntactic requirements of a **fully qualified domain name (FQDN)** component (for more information, see [\[RFC1034\]](#)). Such a **DN** corresponds to the **FQDN** n1.n2.nk. This is the **FQDN** of the **NC**, and it allows **replicas** of the **NC** to be located by using DNS.

dominant speaker: A **participant** (2) whose speech is both detected by a **mixer** and perceived to be dominant at a specific moment. Heuristics typically are used to determine the dominant speaker.

double accounting: An underline style that places two lines beneath the formatted text. Double accounting is frequently used to indicate totals.

down bar: See **up-down bar**.

draft: A version of a document or list item that does not have a publishing level of "Published" or "Checked Out".

drawing: A collection of drawing objects, such as shapes, curves, or WordArt, that are viewed together as a single image.

drawing canvas: See **canvas** and **drawing space**.

drawing group: A collection of images that are designated by the user as a single group of images and manipulated as a single **drawing object**.

drawing object: A shape, curve, line, WordArt, or other type of graphical object that can be inserted into a document.

drawing space: An area of the **absolute space** that is being drawn, after all of the rotation and scaling is complete. For example, a shadow is typically drawn relative to a shape, and is

therefore in the drawing space of that shape. The value for drawing space is expressed in **English Metric Units (EMUs)**. See also **absolute space**.

drill indicator: A symbol that indicates whether a PivotTable member can be expanded or collapsed.

drilldown: A technique that is used to navigate hierarchical data, starting from general data and moving to increasingly finer levels of detail.

drillthrough: (1) A query that is used to retrieve individual records that were used to calculate an aggregate value.

(2) A means in a client application to view a more detailed view of a subset of the data after clicking on a displayed instance of data. The displayed instance of data contains an action with a drillthrough link, and clicking on the link executes a semantic query that returns more detailed results.

(3) The OLAP capability to go beyond browsing the data in a cube and to drill into the original data store.

drive: (1) See **volume**.

(2) A device that can read or write to a **cartridge**. A **library** has at least one **drive**.

drive letter: (1) One of the 26 alphabetical characters A-Z, in uppercase or lowercase, that is assigned to a volume. Drive letters serve as a namespace through which data on the volume can be accessed. A volume with a drive letter can be referred to with the drive letter followed by a colon (for example, C:).

(2) A letter from the English character set (A, B, C...Z) that is assigned to a removable storage device that is physically connected to the client device and logically connected to a session that the client connects to using the RDP protocol.

drop lines: A set of supplemental lines on an area chart or a line chart. Drop lines increase the legibility of a chart by connecting each data point in a series to the category axis.

dsname: (1) A tuple that contains between one and three identifiers for an object. The term **dsname** does not stand for anything. The possible identifiers are the object's **GUID** (attribute objectGuid), **security identifier (SID)** (attribute objectSid), and **distinguished name (DN)** (attribute distinguishedName). A **dsname** can appear in a protocol message and as an attribute value (for example, a value of an attribute with syntax Object(DS-DN)). Given a **DSName**, an **object** can be identified within a set of **NC replicas** according to the matching rules defined in [MS-DRSR] section 5.49.

(2) A **dsname** is a field 3-tuple<guid: **GUID**, sid: **security identifier (SID)**, dn: **distinguished name (DN)**>. A **dsname** can appear in a protocol message and as a value of an attribute. In either context, it identifies an object. If all three fields are null, the **dsname** is null. As a value of an attribute, a **dsname** always contains a non-null **GUID** and **DN**, and sometimes contains a non-null **SID**. Such a **dsname** n refers to the unique object o such that o.objectGuid = n.guid. The **SID** and **DN** are not used for identification in this case. As a value within a protocol message, a non-null **dsname** n refers to: if n.guid ≠ null, the unique object o such that o.objectGuid = n.guid (failing if no such object); otherwise if n.dn ≠ null, the unique object o such that o.distinguishedName = n.dn (failing if no such object); otherwise the unique object o such that o.objectSid = n.sid. Note that the **SID** is used only if no other part of the dsname is specified. If o is an object, the function dsname(o) equals [o.objectGuid, o.objectSid, o.distinguishedName].

dual interface: An interface that can act either as a dispinterface or a Distributed Component Object Model (DCOM) interface.

dual-tone multi-frequency (DTMF): In telephony systems, a signaling system in which each digit is associated with two specific frequencies. This system typically is associated with touch-tone keypads for telephones.

duplicate: A search result that is identified as having identical or near identical content.

duplicate result removal: An operation to compare the similarity of items and remove duplicates from search results.

Dynamic Data Exchange (DDE): An inter-process communication method that is featured in Windows. DDE allows two or more applications that are running simultaneously to exchange data and commands.

dynamic endpoint: A network-specific server address that is requested and assigned at run time. For more information, see [\[C706\]](#).

Dynamic Host Configuration Protocol (DHCP): A protocol that provides a framework for passing configuration information to hosts on a TCP/IP network, as described in [\[RFC2131\]](#).

Dynamic Host Configuration Protocol (DHCP) client: An Internet host using DHCP to obtain configuration parameters such as network addresses.

Dynamic Hypertext Markup Language (DHTML): An extension of the **Hypertext Markup Language (HTML)** that allows applications to change styles and attributes of page elements (objects) and to replace existing elements (objects) with new ones.

Dynamic Link Library (DLL): A set of executable routines that typically serve a specific function and are stored separately as a file with a .dll file name extension. The routines are loaded only when they are needed by the application that calls them.

dynamic object: An object with a time-to-die (attribute msDS-Entry-Time-To-Die). The directory service garbage-collects a **dynamic object** immediately after its time-to-die has passed. The constructed attribute entryTTL gives a **dynamic object's** current time-to-live, that is, the difference between the current time and msDS-Entry-Time-To-Die. For more information, see [\[RFC2589\]](#).

dynamic rank: A rank component that indicates how well query text matches an indexed item. See also **static rank**.

dynamic teaser: See **hit highlighted summary**.

dynamic web template: An HTML-based master copy of a page that contains settings, formatting, and elements such as text, graphics, page layout, styles, and regions of a page that can be modified. Dynamic web templates have a .dwt file name extension.

7 E

early media: Media, such as audio and video, that is exchanged before a specific session is accepted by the called user. During a dialog, early media occurs when the initial INVITE is sent, until the **user agent server (UAS)** generates a final response.

East Asian character: A character that is part of the Simplified Chinese, Traditional Chinese, Japanese, or Korean **character set** (1).

edit form: A form that enables users to edit a list item.

edit session: A **session** (2) that is based on a workbook file and during which changes by one or more users are persisted to that file.

editor: The user who last modified an item or document in a SharePoint list.

effect: A user-specified **camera** motion that occurs for the duration of a **scene**.

electronic codebook (ECB): A **block cipher** mode that does not use feedback and encrypts each block individually. Blocks of identical plaintext, either in the same message or in a different message that is encrypted with the same key, are transformed into identical ciphertext blocks. Initialization vectors cannot be used.

electronic discovery (eDiscovery): A type of legal discovery that focuses on electronic (computer) communications and files.

ElGamal encryption: A public-key encryption scheme, as described in [\[CRYPTO\]](#).

email address: A string that identifies a user and enables the user to receive Internet messages.

embed code: A block of data containing information needed to embed a video in a user interface element. This information can include the path to the video, the height and width of the video, and so on.

embedded image: An **image** that is stored within a document rather than being linked to a source file that is outside the document.

embedded object: (1) An object that is created by using one application and is hosted in a document that was created by using another application. Embedding an object, rather than inserting or pasting it, ensures that the object retains its original format. Users can double-click an embedded object and edit it with the toolbars and menus from the application that was used to create it. See also **Object Linking and Embedding (OLE)**.

(2) Application data that is stored in documents from other applications.

empty GUID: A 128-bit, 16-byte identification number that is represented by all zeros.

empty string: (1) A string object or variable that is initialized with the value "".

(2) A non-initialized string object that has a null value.

encrypted document: A document that was converted from plaintext into cipher text to disguise the content of the document when it is stored or sent.

encryption: In cryptography, the process of obscuring information to make it unreadable without special knowledge.

encryption key: One of the input parameters to an **encryption** algorithm. Generally speaking, an encryption algorithm takes as input a clear-text message and a key, and results in a cipher-text message. The corresponding **decryption** algorithm takes a cipher-text message, and the key, and results in the original clear-text message.

end user presence: A set of **attributes** (1) for a user who is participating in an **edit session**.

end-of-file (EOF) key: An **index key** that is stored near the end of a content index file. It references a content index record that stores the maximum occurrence for a specified property.

endpoint: (1) A client that is on a network and is requesting access to a network access server (NAS).

(2) A network-specific address of a remote procedure call (RPC) server process for remote procedure calls. The actual name and type of the endpoint depends on the RPC protocol sequence that is being used. For example, for RPC over TCP (RPC Protocol Sequence ncacn_ip_tcp), an endpoint might be TCP port 1025. For RPC over Server Message Block (RPC Protocol Sequence ncacn_np), an endpoint might be the name of a named pipe. For more information, see [\[C706\]](#).

(3) A participant that uses the Microsoft Groove Dynamics Protocol, as described in [\[MS-GRVDYNM\]](#), to synchronize with a shared space. An endpoint is identified by the combination of an identity URL and a client device URL. Each endpoint maintains a copy of the data in a shared space.

(4) A communication port that is exposed by an **application server** for a specific shared service and to which messages can be addressed.

(5) A device that is connected to a computer network.

(6) A **client** on the network that is requesting access to a **network access server (NAS)**.

(7) A network-specific address of a remote procedure call (RPC) server process for remote procedure calls. The actual name and type of the **endpoint** depends on the **RPC** protocol sequence being used. For example, for RPC over TCP (RPC Protocol Sequence ncacn_ip_tcp), an **endpoint** might be TCP port 1025. For RPC over Server Message Block (SMB) (RPC Protocol Sequence ncacn_np), an **endpoint** might be the name of a **named pipe**. For more information, see [\[C706\]](#).

(8) In the context of a web service, a network target to which a **SOAP** message can be addressed. See [\[WSADDR\]](#).

(9) An entity, processor, or resource that can be referenced where Web service messages are originated or targeted.

(10) A node that sends or receives a **protocol stream**.

(11) A tuple (composed of an IP address, port, and protocol number) that uniquely identifies a communication **endpoint**.

(12) The IP address of a network interface on which the Dynamic Host Configuration Protocol (DHCP) **server** is listening for **DHCP client** requests.

(13) A **resource** that can be addressed by an **endpoint reference**.

endpoint identifier (EPID): A unique identifier of a Session Initiation Protocol (SIP) **endpoint** (5). It is formed by combining the value of an epid parameter in a From or To header field with the **address-of-record** in the corresponding header field.

endpoint reference (EPR): (1) A resource that conveys the information that is needed to address an **endpoint**.

(2) As specified in section 2 of [\[WSA\]](#).

(3) A combination of WS-Addressing ([\[WSAddressing\]](#)) and **WS-Management**-addressing elements that together describe an address for a **resource** in the **SOAP** message header.

engine: A component that creates and executes commands, and uses the Microsoft Groove Dynamics Protocol, as described in [\[MS-GRVDYNM\]](#), to transport and order those commands.

English Metric Unit (EMU): A measurement in computer typography. There are 635 EMUs per twip, 6,350 EMUs per half-point, 12,700 EMUs per point, and 914,400 EMUs per inch. These units are used to translate on-screen layouts to printed layouts for specified printer hardware.

enhanced metafile format (EMF): A file format that supports the device-independent definitions of images.

enhanced metafile spool format (EMFSPPOOL): A format that specifies a structure of **enhanced metafile format (EMF)** records used for defining application and device-independent printer **spool files**.

enhanced presence: A presence model that uses **categories** (4) to specify presence information and uses **containers** to authorize **subscribers**. This model includes **Session Initiation Protocol (SIP)** extensions for publishing and subscribing to presence information and for specifying access control lists for subscribers. It uses the msrtc-event-categories presence document format.

Enhanced ScreenTip: A small, pop-up window that provides context-sensitive Help when users point to an item on the **ribbon**.

enterprise: A unit of administration of a network of **MSMQ queue managers**. An enterprise consists of an **MSMQ Directory Service**, one or more **connected networks**, and one or more **MSMQ sites**.

entity: (1) An instance of an EntityType element that has a unique identity and an independent existence. An entity is an operational unit of consistency.

(2) The payload of a transfer (by analogy to the definition in [\[RFC2616\]](#)).

(3) Any document on a server that is accessible by using a **Hypertext Transfer Protocol (HTTP)** URL.

(4) A unit that is part of the system such as a component or an element.

(5) A single business object about which data can be stored. It is the subject of a table in a relational database.

(6) Tabular data that is stored within the Master Data Services (MSD) system.

Entity: A type of **DataClass** that represents a type of business data object that is stored in a line-of-business (LOB) system and whose instances have a persistent EntityInstanceId.

Entity Data Model (EDM): A set of concepts that describes the structure of data, regardless of its stored form, as described in [\[MC-CSDL\]](#).

EntityInstance: A set of **Field** (4) values that have a unique identity that represents a specific instance of an Entity, and are stored in a line-of-business (LOB) system.

EntityInstanceId: A set of **Field** (4) values of an EntityInstance that collectively and uniquely identify an EntityInstance in a line-of-business (LOB) system.

entry point: A starting address for an **assembly** that is written in the form `NamespaceName.ClassName`.

entry point header: A header field whose values specify the horizontal and vertical dimensions of a video frame. See also **sequence header**.

Enum: A Primitive type whose members are constrained to a set of values. The Primitive type is considered to be an underlying **Remoting Type** of the **Enum**. Each value has a name associated with it. An **Enum** is part of the **Remoting Data Model**, and an abbreviation for "enumeration." For more information, see [\[MS-NRTP\]](#) section 3.1.1.

enumerator: A **station** that seeks all LLTD-capable **stations** on the link by using **quick discovery**.

envelope: A container that stores the information that is used to send a document, workbook, or presentation in an email message. The information includes the intended recipients, the subject of the email message, and any **attachments** to be included.

error report: Information contained in a set of files that describes a problem event that has occurred on the system. The report is typically compressed into a single file for transmission.

error report level 1 data: The data that is transmitted to the **CER server** that contains basic information about the problem.

error report level 2 data: The information that is contained in a set of files that describe a problem event that has occurred on the system. The report is typically compressed into a single file for transmission.

error signature: An ordered collection of strings that represents an individual error or class of errors.

error subpath: A fragment of a directory path on a Server Message Block (SMB) Protocol file server that is composed of strings in an error signature and is used to direct error reports on the file share, as described in [\[MS-CER\]](#).

event: (1) Any significant occurrence in a system or an application that requires users to be notified or an entry to be added to a log.

(2) An action or occurrence to which an application might respond. Examples include state changes, data transfers, key presses, and mouse movements.

(3) A discrete unit of historical data that an application exposes that may be relevant to other applications. An example of an event would be a particular user logging on to the computer.

(4) As defined in [\[UPNPARCH1.1\]](#) section i.7, a notification of one or more changes in state variables exposed by a **service**.

event class: (1) A collection of events that are grouped together based on criteria that the publishing application specifies.

(2) A collection of historical data grouped together using criteria specified by the publishing application.

event handler: A software routine that executes in response to an event.

event host: A site collection, **site** (2), **list** (1), list item, **workflow** (2), feature, or content type that hosts an event receiver.

event interface: A collection of **event methods**. An **event class** contains one or more **event interfaces**.

event log: A collection of records, each of which corresponds to an event.

event method: A method called by the **publisher-subscriber framework** when the **publisher** application generates an **event**.

event package: A specification that defines a set of state information to be reported by a notifying **Session Initiation Protocol (SIP)** client to a subscriber. An event package also defines further syntax and semantics based on the framework that is required to convey such state information.

event receiver: A structured modular component that enables built-in or user-defined managed code classes to act upon objects, such as list items, **lists** (1), or content types, when specific triggering actions occur.

event sink: (1) A structured, modular component that enables built-in or user-defined classes to act on documents in document libraries when specific triggering actions occur. Event sinks are a deprecated, implementation-specific capability of Windows SharePoint Services 2.0. In Windows SharePoint Services 3.0 and SharePoint Foundation 2010, they are replaced by the capabilities of event receivers.

(2) A destination for an event stream within the CEP platform. In the current version, only output adapters can be event sinks.

Excel Linked Library (XLL): A **Dynamic Link Library (DLL)** that is authored to function as an **add-in** for Microsoft Excel.

Excel macro (XLM): A programming language that provides development capability in Microsoft Excel. XLM was superseded by VBA.

exclusion list: (1) A list of items to exclude from query results and to remove from a search index the next time that a crawl occurs.

(2) A list of processes that cannot be managed because of the negative system impact such management could create. Processes in an exclusion list are unmanaged and can consume resources freely. Both system-defined and user-defined exclusion lists are defined.

exclusive lock: A condition in which one protocol client or protocol server can read or write data, but no transaction can acquire a **shared lock** on the data until the exclusive lock is released.

expand: The process of opening a level in a dimension hierarchy on a PivotTable report to view data from lower levels in the user interface.

expand/collapse button: A user interface control that is used to determine which hierarchical level is displayed in an outline, or in row and column groupings.

expanded outline state: A state in which nested content within an outline is displayed.

ExpandingGrid control: A type of **ButtonPopup control** that displays and sets a value from a continuous range of possible values when the user drags across the menu area.

expire: A process in which an object, such as an external data connection, becomes invalid because its allotted time period has ended.

explicit authentication: An **authentication** (2) mechanism that requires users to provide **credentials**, such as a login name and password, before they can gain access to one or more resources.

export: The process of creating an **installer package file** for a **conglomeration** or **partition** on a COMA server, so that it can be **imported** onto another server.

export attribute flow: The process of updating the **metaverse** attribute values of the current metaverse object during an export operation.

expression: (1) A combination of operators, symbols, constants, literal values, functions, names of fields or **columns** (2), controls, and properties that evaluates to a single value.

(2) A construct that serves two purposes: specifies the logical operator (AND/OR) to be used between 2 conditions of a **policy**; and specifies the index of the **expressions** that are parent to it. Taken together, **conditions** and **expressions** specify **policy** classification criteria.

(3) A combination of symbols (identifiers, literals, functions, and operators) that yields a single data value.

Extended Backus-Naur Form (EBNF): A modified version of Backus-Naur Form (BNF), which is commonly used to describe programming languages and formal languages. EBNF extends standard BNF to better enable the concise expression of such languages, as described in [ISO-14977](#).

extended payload: An arbitrary BLOB of data associated with a **Peer Name** and published by an application.

extended type library: A component that contains Automation standard descriptions of exposed objects, properties, and methods that are implemented by an **aggregatable server** and supplemented by another **Automation server**.

Extensible Application Markup Language (XAML): (1) A declarative XML-based language that is used to represent a tree of objects. XAML markup is stored in .xaml files or, for workflow schemas, .xoml files.

(2) An XML schema that defines the appearance and some aspects of the behavior of an application's user interface.

Extensible Message and Presence Protocol (XMPP): An application profile of **XML** that enables the near-real-time exchange of structured yet extensible data between any two or more network entities.

Extensible Stylesheet Language (XSL): An **XML** vocabulary that is used to transform XML data to another form, such as **HTML**, by means of a style sheet that defines presentation rules.

external content type: A type of **DataClass** object that is stored in a line-of-business (LOB) system and whose instances have a persistent EntityInstanceId. Also referred to as Entity.

external data: Data that is stored in a repository outside a workbook.

external group: A group whose membership is controlled by an external component, such as an AD DS domain group or a role that is managed by a role provider in **ASP.NET**.

external link: A reference to a cell, range, defined name, or other object in another worksheet or workbook.

external list: A container that is within a SharePoint site and that references a set of **EntityInstances** that are sourced from a line-of-business (LOB) system. It has a customizable schema that is composed of one or more **Fields** (4).

external security provider: An external object that manages permissions on a site.

external user: Any user who is located outside the enterprise network boundary, including **remote users** (1), federated users, and public instant messaging (IM) users.

8 F

FAI contents table: A table of **folder associated information (FAI)** Message objects that are stored in a Folder object.

failure response: An **HTTP** response where the value of the **Status-Code** element is 4xx or 5xx, as described in [\[RFC2616\]](#).

fallback data culture: A data culture that is selected through an algorithm as a substitute for a data culture that is not installed or is otherwise unavailable.

fallback UI culture: A user interface (UI) culture that is selected through an algorithm as a substitute for a UI culture that is not installed or is otherwise unavailable.

fallback URI: A **Uniform Resource Identifier (URI)**, as described in [\[RFC3986\]](#), that specifies the **user agent** address to which unretrieved **calls** are transferred.

fanout: The process of transmitting a message from a client device to a relay server for replication and distribution to multiple recipients.

farm: A group of computers that work together as a single system to help ensure that applications and resources are available. Also referred to as server farm.

FAT32 file system: A derivative of the **file allocation table (FAT)** file system. **FAT32** supports smaller cluster sizes and larger **volumes** than **FAT**, which results in more efficient space allocation on **FAT32 volumes**. **FAT32** uses 32-bit addressing.

fax message: (1) A **Message object** that contains a digital representation of content received from a fax machine.

(2) See **message**.

feature: A package of SharePoint elements that can be activated or deactivated for a specific feature scope.

feature identifier: A **GUID** that identifies a **feature**.

feature receiver: A server-side code routine that is called when a **feature** is activated, deactivated, installed, uninstalled, or upgraded on a computer, server farm, or server cluster.

feature scope: The scope at which a **feature** can be activated.

federated location: A source that returns search results for a search query. The source can be a local **search catalog** or an OpenSearch1.0/1.1-compliant search engine, as described in [\[OpenSearch1.1-Draft3\]](#).

federated partner: An enterprise that is trusted for **federation** (2).

federated user: An external user who possesses valid credentials with a federated partner and who therefore is treated as authenticated by a protocol server.

federation: (1) The ability to issue a query to multiple federated locations, which are described by federated location definitions, and to return the results in a single search results page.

(2) The ability of a server deployment to interoperate with other servers that were deployed by other enterprises.

(3) A collection of **security realms** that have established **trust**.

feed entity: An object that represents anything that can have a feed, such as a user, a document, or a site.

feed entry: The data contained in a posting to a feed.

field: (1) An element or **attribute** (1) in a data source that can contain data.

(2) A container for metadata within a SharePoint list and associated list items.

(3) A discrete unit of a record that has a name, a data type, and a value.

(4) The data elements that constitute an **Entity** in a line-of-business (LOB) system.

(5) An attribute or role of an **entity**.

field definition: The definition of a field in the **Collaborative Application Markup Language (CAML)**.

field identifier: A GUID that is used to identify a field.

field internal name: A string that uniquely identifies a field in a content type or a SharePoint list.

field link: A property that specifies a reference from a **content type** to a **field** (2) or **field definition**.

field type: A name that identifies the action or effect that a field has within a document. Examples of field types are Author, Page, Comments, and Date.

file: (1) A single, discrete unit of content.

(2) An entity of data in the **file system** that a user can access and manage. A **file** must have a unique name in its directory. It consists of one or more streams of bytes that hold a set of related data, plus a set of **attributes** (also called properties) that describe the **file** or the data within the **file**. The creation time of a **file** is an example of a file **attribute**.

(3) A unit of data in the **file system**. An encrypted file consists of encrypted data along with the metadata required for a user to **decrypt** the file. The file and its metadata are protected using **public key** cryptography such that an authorized user's **private key** is required to **decrypt** the file.

(4) A **file** is a typed data stream. A **file** does not imply storage of the data stream in any particular medium or with any particular organization, or, for example, in a file system (*italic is used when referring to traditional files*).

file allocation table (FAT): A data structure that the operating system creates when a volume is formatted by using **FAT** or **FAT32 file systems**. The operating system stores information about each **file** in the **FAT** so that it can retrieve the **file** later.

File Allocation Table (FAT): A file system that is used by MS-DOS and Windows operating systems to organize and manage files.

file data object: An object that represents a file that was inserted into a OneNote revision store file. It can be stored internally as a data stream in the revision store file, or externally in the onefiles folder.

file extension: The sequence of characters in a **file's** name between the end of the **file's** name and the last "." character. Vendors of applications choose such sequences for the applications

to uniquely identify **files** that were created by those applications. This allows file management software to determine which application should be used to open a **file**.

File Replication Service (FRS): One of the services offered by a **domain controller (DC)**, which is advertised through the Domain Controller Location protocol. The service being offered to **clients** is a replicated data storage **volume** that is associated with the default **naming context (NC)**. The running or paused state of the **FRS** on a **DC** is available through protocols documented in [MS-ADTS] section 6.3.

file system: (1) A system that enables applications to store and retrieve files on storage devices. Files are placed in a hierarchical structure. The file system specifies naming conventions for files and the format for specifying the path to a file in the tree structure. Each file system consists of one or more drivers and DLLs that define the data formats and features of the file system. File systems can exist on the following storage devices: diskettes, hard disks, jukeboxes, removable optical disks, and tape backup units.

(2) A system that enables applications to store and retrieve **files** on storage devices. Files are placed in a hierarchical structure. The **file system** specifies naming conventions for **files** and the format for specifying the path to a **file** in the tree structure. Each **file system** consists of one or more drivers and DLLs that define the data formats and features of the **file system**. File systems can exist on the following storage devices: diskettes, hard disks, jukeboxes, removable optical disks, and tape backup units.

(3) A set of data structures for naming, organizing, and storing files in a **volume**. **NTFS**, **FAT**, and **FAT32** are examples of **file system** types.

File Transfer Protocol (FTP): A member of the TCP/IP suite of protocols that is used to copy files between two computers on the Internet if both computers support their respective FTP roles. One computer is an FTP client and the other is an FTP server.

fill: A color, pattern, or other attribute that is used to format the background of a cell, shape, or chart element. See also **fill color** and **fill pattern**.

fill alignment: A setting that repeats a cell value to fill the horizontal space of a cell. If the cell value exceeds the horizontal width of the cell, the value is truncated.

fill color: A color that is used to fill the background of a cell, shape, or chart element.

fill pattern: A repetitive design that users can add to the background of a cell, shape, or chart element.

filter: (1) A mechanism by which a set of data is scoped to display only those entries that meet specified logical criteria.

(2) A setting that excludes subfolders (and their contents) or **files** from replication. There are two types of filters: **file** filters and folder filters.

(3) In the context of the **Lightweight Directory Access Protocol (LDAP)**, the **filter** is one of the parameters in a search request. The **filter** specifies matching constraints for the candidate objects.

(4) A configuration on a **network access server (NAS)** that specifies the types of traffic that are acceptable for IP local host traffic. **Filters** can block or allow traffic by IP address, IP protocol, TCP port, or **User Datagram Protocol (UDP)** port.

(5) A processing object in the **scan repository** identified by **scan documents** that is a unique **URI**. This object will perform a specific operation in a **PostScan job**. The operations

performed by each **filter** are governed by the **filter** dialect **URI** and **filter-specific instructions**.

(6) Type of driver that is layered between the kernel and a base file system (such as **FAT** or **NTFS**) that receives I/O request packets on their way to and from the base file system. The term **filter** can refer to legacy filters or minifilters.

(7) A set of criteria that controls the set of records that is returned as a result set.

filter date value: Any one of a set of possible date values that can be used to define the filter criteria for an **AutoFilter**.

filter value: Any one of a set of possible values that can be used to define the filter criteria for an **AutoFilter**.

FilterDescriptor: A type of **MetadataObject** that describes a normalized way of gathering input from users. A FilterDescriptor is defined by its type and the Method that contains it.

filtering control: A user interface element that contains the filter functions of a PivotTable report.

filtering state: A setting that indicates whether a filter value or filter date value is included as part of the criteria that is used to define the filter for an **AutoFilter**.

filter-specific instructions: A set of data elements that tell a specific **filter** how to process the **scan document(s)** that are part of a **PostScan job**. The definition of these data elements is specific to each **filter**.

final offer: An offer that is sent by a **caller** at the end of connectivity checks and carries the **local candidate** and the **remote candidate** that were selected for media flow.

final response: A Session Initiation Protocol (SIP) response that terminates an SIP transaction. All 2xx, 3xx, 4xx, 5xx, and 6xx responses are final.

Finder: A type of **MethodInstance** that can be called to return a collection of zero or more EntityInstances of a specific Entity. Finder input is defined by the FilterDescriptors that are contained in the Method that contains the Finder.

firewall rule: A group of settings that specify which connections are allowed into and out of a client computer.

first-party request: A **conference control request** that modifies the state of the sending participant only.

fit to page: A printing option that scales a document to print on a specified number of pages.

flags: A set of values used to configure or report options or settings.

floating-point number: A number that is represented by a mantissa and an exponent according to a given base. The mantissa is typically a value between "0" and "1". To find the value of a floating-point number, the base is raised to the power of the exponent, and the mantissa is multiplied by the result.

floor: An extension of the horizontal axis, or the area created by the inclusion of the z axis, in a 3-D chart to create a three-dimensional effect. See also **wall**.

flow: (1) The direction in which text in a cell is rendered.

(2) A TCP session or **User Datagram Protocol (UDP)** pseudosession, identified by a 5-tuple (source and destination IP and ports, and protocol). By extension, a request/response Internet Control Message protocol (ICMP) exchange (for example, ICMP echo) is also a **flow**.

focus: A single **user agent** that maintains a **dialog** and **Session Initiation Protocol (SIP)** signaling relationship with each **participant** (2), implements conference policies, and ensures that each participant receives the media that comprise the tightly coupled **conference**.

Focus Factory: A component that is responsible for creating, managing, and deleting conferences.

folder: (1) A file system construct. File systems organize data by providing a hierarchy of objects, which are referred to as folders or directories, that contain files and can also contain other folders.

(2) A **file system** construct. File systems organize a **volume's** data by providing a hierarchy of objects known as **folders** or directories, which contain **files**.

(3) A container for **files** and other folders. A folder may be encrypted. The semantics of encrypting a folder are implementation-dependent. In the Windows implementation, encrypting a folder does not directly cause any data to be encrypted. Encrypting a folder in Windows has the following consequences of EFSRPC Metadata is created and stored with the folder and an **NTFS** attribute is set on the folder to signify that it is encrypted. **NTFS** checks this attribute when any new **files** or folders are created in the folder. **NTFS** will automatically encrypt any **files** or folders created within a folder that has this attribute set.

folder associated information (FAI): A collection of **Message objects** that are stored in a Folder object and are typically hidden from view by email applications. An FAI Message object is used to store a variety of settings and auxiliary data, including forms, views, calendar options, favorites, and category lists.

Folder object: A messaging construct that is typically used to organize data into a hierarchy of objects containing Message objects and **folder associated information (FAI)** Message objects.

font: An object that defines the graphic design, or formatting, of a collection of numbers, symbols, and letters. A font specifies the style (such as bold and strikeout), size, family (a typeface such as Times New Roman), and other qualities to describe how the collection is drawn.

font face color: A property of a cell that specifies the color that is used to render a font.

font face decoration: Any of the set of font properties that specify how to render a font, such as italics and underline.

font face weight: A value that specifies the thickness of a font.

font family: A set of fonts that all have common stroke width and serif characteristics. For example, Times Roman and Times Roman Italic are members of the same font family.

font scaling: A process of resizing a proportionally-spaced font.

font scheme: A combination of complementary fonts in a **theme**.

footer: One or more lines of text in the bottom margin area of a page in a document or a slide in a presentation. A footer typically contains elements such as the page number and the name of the file.

footnote: A note that appears at the end of a page, section, chapter, or publication. It explains, comments on, or provides references for text in the main body of a document. A footnote consists of two linked parts, a reference mark within the main body of the document and the corresponding text of the note.

forecast: The process of projecting values forward or backward in a series, based on trends in existing data.

foreground color: A color that is used to display text, patterns, and other objects that appear in front of or on top of the **background color**.

forest: (1) One or more domains that share a common schema and trust each other transitively. An organization can have multiple forests. A forest establishes the security and administrative boundary for all objects that reside within the domains that belong to the forest. In contrast, a domain establishes the administrative boundary for managing objects, such as users, groups, and computers. In addition, each domain has individual security policies and trust relationships with other domains.

(2) In the **Active Directory** directory service, a forest is a set of **naming contexts (NCs)** consisting of one schema NC, one config NC, and one or more domain NCs. Because a set of NCs can be arranged into a tree structure, a forest is also a set of one or several trees of NCs.

(3) One or more **domains** that share a common **schema** and trust each other transitively. An organization can have multiple **forests**. A **forest** establishes the security and administrative boundary for all the **objects** that reside within the **domains** that belong to the **forest**. In contrast, a **domain** establishes the administrative boundary for managing **objects**, such as users, groups, and computers. In addition, each **domain** has individual security policies and trust relationships with other **domains**.

(4) In the **Active Directory** directory service, a **forest** is a set of **naming contexts (NCs)** consisting of one **schema NC**, one **config NC**, and one or more **domain NCs**. Because a set of **NCs** can be arranged into a tree structure, a **forest** is also a set of one or several trees of **NCs**.

(5) For **Active Directory Domain Services (AD DS)**, a set of **naming contexts (NCs)** consisting of one **schema naming context (schema NC)**, one **configuration naming context (config NC)**, one or more **domain naming contexts (domain NCs)**, and zero or more application naming contexts (application NCs). Because a set of **NCs** can be arranged into a tree structure, a **forest** is also a set containing one or several trees of **NCs**. For **AD LDS**, a set of **NCs** consisting of one **schema NC**, one **config NC**, and zero or more **application NCs**. (In Microsoft documentation, an **AD LDS forest** is called a "configuration set".)

form: (1) A structured document with controls and spaces that are reserved for entering and displaying information. Forms can contain special coding for actions such as submitting and querying data.

(2) A document with a set of controls into which users can enter information. Controls on a form can be bound to elements in the data source of the form, such as fields and groups. See also **bind**.

form definition (.xsf) file: An **XML** file with an .xsf file name extension. The file contains information about the files and components that are used within a form, including user interface customizations, **XML schemas**, views, **business logic** (1), **events** (2), and deployment settings.

form digest: An object that is inserted into a page and is used by a protocol server to validate client requests. The validation is specific to a user, site, and time period.

form digest validation: A type of security validation that helps prevent an attack wherein users are tricked into posting data to a server.

form file: An **XML** file that contains data that is entered into an InfoPath form by using a web browser or Microsoft InfoPath.

form library: A type of document library that is optimized for storing and displaying data in XML-based forms.

form security level: A setting that determines whether an InfoPath form can access data on other domains, or access files and settings on a user's computer. There are three security levels for forms: Restricted, Domain, and Full Trust.

form server: A server that can host XML-based electronic forms and that supports rendering those forms in a web browser.

form template: A file or set of files that defines the data structure, appearance, and behavior of a **form** (2).

form template (.xsn) file: A **cabinet (.cab) file** with an .xsn file name extension that contains the files that comprise a form template.

form view: A display setting that is saved with an InfoPath form template and specifies which controls and data appear on a form when the form is being filled out.

format: (1) To submit a command for a **volume** to write metadata to the disk, which is used by the **file system** to organize the data on the disk. A volume is **formatted** with a specific **file system**.

(2) A data structure that is used to define the encoding of audio and video data. The actual structures are opaque to [MS-RDPEV].

(3) A set of flags that encapsulates text layout information such as alignment, text direction, and trimming.

format string: A string that contains the number formatting information to apply to data, such as decimal position, percentage indicator, or currency symbol.

formatting run: A set of formatting properties that are applied to a **text run**.

forms authentication: An **authentication** (2) method in which protocol clients redirect unauthenticated requests to an **HTML** form by using **HTTP**. If the protocol client authenticates the request, the system issues a **cookie** that stores the credentials or a key for reacquiring the identity. In subsequent requests, the cookie is submitted in request headers and the requests are authenticated and authorized by an **ASP.NET** event handler that uses the validation method that is specified by the protocol client.

formula: A logical equation or function that produces a result in a spreadsheet application.

formula bar: A user interface element that appears at the top of a worksheet and is used to display and edit cell content.

forward error correction (FEC): A process in which a sender uses redundancy to enable a receiver to recover from packet loss.

forward link: A hyperlink between a referenced document and a referencing party. For example, if Document A contains a hyperlink to Document B, Document A has a forward link to Document B.

forward link attribute: An **attribute** whose values include **object** references (for example, an **attribute** of syntax Object(DS-DN)). The **forward link values** can be used to compute the values of a related **attribute**, a **back link attribute**, on other **objects**. If an **object** o refers to **object** r in **forward link attribute** f, and there exists a **back link attribute** b corresponding to f, then a **back link value** referring to o exists in **attribute** b on object r. The relationship between the forward and **back link attributes** is expressed using the **linkId attribute** on the attributeSchema **objects** representing the two **attributes**. The forward link's linkId is an even number, and the back link's linkId is the forward link's linkId plus one. A **forward link attribute** can exist with no corresponding **back link attribute**, but not vice-versa. For more information, see [\[MS-ADTS\]](#).

forward link value: The value of a **forward link attribute**.

forwarder: The **forwarder** is the kernel-mode component of the router that is responsible for forwarding data from one router **interface** to the others. The **forwarder** also decides whether a packet is destined for **local** delivery, whether it is destined to be forwarded out of another **interface**, or both. There are two kernel-mode **forwardersunicast** and **multicast**.

forwarders: A DNS server that is designated to facilitate forwarding of queries for other DNS servers.

foundation: A string that is a property associated with a **candidate**. The string is the same for candidates that are of the same type, protocol, and base IP addresses, and are obtained from the same STUN/TURN server for relayed and server reflexive candidates.

fragment: (1) A component of a **URI** that allows for indirect identification of a secondary resource by reference to a primary resource, as defined in [\[RFC3986\]](#) section 3.5.

(2) An independently downloadable unit of **media** that comprises one or more **samples**.

(3) The term "fragment" that is defined in XMD/2.

frame: (1) A space, displayed onscreen as a box, that contains a specific element of a publication.

(2) A rectangular section of a webpage that is a separate HTML document from the rest of the page. Webpages can have multiple frames, each of which is a separate document.

(3) A CIFS Browser Protocol message.

friendly name: A name for a user or object that can be read and understood easily by a human.

front-end web server: A server that hosts webpages, performs processing tasks, and accepts requests from protocol clients and sends them to the appropriate back-end server for further processing.

frozen: See **frozen panes**.

frozen panes: Portions of a worksheet that remain static and do not scroll when the worksheet is displayed in split pane view. See also **split pane**.

FRS: See **File Replication Service (FRS)**.

full: An Interactive Connectivity Establishment (ICE) implementation that adheres to the complete set of functionality described in [\[MS-ICE2\]](#).

full address book file: An **address book file** that contains a complete set of the **address book contacts** that existed when the file was generated by the user, contact, and groups objects in AD DS.

full crawl: A crawl process that indexes all of the items in a specified content source, regardless of whether the item was modified.

full URL: A string of characters in a standardized format that identifies a document or resource on the World Wide Web.

full-text index catalog: A collection of full-text index components and other files that are organized in a specific directory structure and contain the data that is needed to perform queries.

fully qualified class name: A class name that includes namespace information. Use of a fully qualified class name ensures that the class name is treated as unique.

fully qualified domain name (FQDN): (1) An unambiguous **domain name** (2) that gives an absolute location in the Domain Name System's (DNS) hierarchy tree, as defined in [\[RFC1035\]](#) section 3.1 and [\[RFC2181\]](#) section 11.

(2) In **Active Directory**, a **fully qualified domain name (FQDN)** (1) that identifies a **domain**.

(3) A fully qualified domain name (FQDN) (1) that does not include the "ldap/" prefix.

fully qualified URL: A URL that includes a protocol scheme name, a host name, optionally a port number, a path, optionally a search part, and optionally a fragment identifier, as described in [\[RFC2616\]](#).

function: A code module that takes a value as input, performs an operation, and returns the results to a worksheet.

function category: A group of worksheet functions that are part of the same broad usage area, such as Finance or Statistical. A function category can be built-in or user-defined.

future function: A function that can be written to but is not implemented in a file.

9 G

gallery: (1) A library that is used to store a collection of site resources, such as Web Parts, list templates, and site templates.

(2) A type of **ribbon** control that displays a set of items from which users can choose.

game: An application that uses a **DirectPlay** protocol to communicate between computers.

game session: The metadata associated with the collection of computers participating in a single **instance** of a computer **game**.

gamma correction: In digital imaging, the process of changing the brightness, contrast, or color balance of an image by assigning new values (different colors) to gray or color tones.

GC: See **global catalog (GC)**.

general alignment: A default formatting setting for the horizontal alignment of cell content in a worksheet. Text is positioned to the left and numbers are positioned to the right.

generic list: A SharePoint list whose **base type** value is "Generic List".

Generic Security Services (GSS): An Internet standard, as described in [RFC2743](#), for providing security services to applications. It consists of an application programming interface (GSS-API) set, as well as standards that describe the structure of the security data.

GenericInvoker: A type of **MethodInstance** that can be called to perform a specific task in a line-of-business (LOB) system. GenericInvoker input and output is specific to the Method.

geometry space: An arbitrarily defined coordinate system for shape geometry. Any coordinate references to a shape use this coordinate system. All connection sites, **adjust handles**, and vertices of a shape are defined in geometry space.

geometry text: A type of text that follows the geometry of the shape, rather than being contained within the **bounding rectangle** of the shape.

ghosted: (1) A property that is not deleted by the server if the element is not included in a Sync <Change> request message. By default, elements that are not included in a Sync <Change> request are deleted from the store.

(2) See **uncustomized**.

Global Address List (GAL): An **address list** that conceptually represents the default address list for an **address book**.

global assembly cache (GAC): A computer-wide code cache that stores .NET Framework **assemblies** that were installed specifically to be shared by multiple applications on a computer. Applications that are installed in the global assembly cache have a strong name, consisting of an assembly identity, strengthened by a public key and a digital signature.

global catalog (GC): A unified partial view of multiple **naming contexts (NCs)** in a distributed partitioned directory. The **Active Directory** directory service **GC** is implemented by **GC servers**. The definition of **global catalog** is specified in [MS-ADTS](#) section 3.1.1.1.8.

global catalog server (GC server): A **domain controller (DC)** that contains a naming context (NC) replica (one full, the rest partial) for each **domain naming context** in the **forest**.

global group: An **Active Directory group** that allows **user objects** from its own **domain** and **global groups** from its own **domain** as members. Universal groups can contain **global groups**. A **group object g** is a **global group** if and only if `GROUP_TYPE_ACCOUNT_GROUP` is present in `g!` `groupType`. A **global group** that is also a **security-enabled group** is valid for inclusion within ACLs anywhere in the **forest**. If a **domain** is in **mixed mode**, then a **global group** in that **domain** that is also a **security-enabled group** allows only **user object** as members. See also **domain local group**, **security-enabled group**.

global navigation menu: The navigation menu that appears horizontally at the top of the default **master page** and shows the set of **navigation nodes** from the site map provider's root node.

global partition: The default, required partition on a COMA server.

global version sequence number (GVSN): A pair of numbers that includes the **machine identifier** and the **version sequence number (VSN)**. While two machines might assign the same **VSN**, because they have different machine identifiers, the associated **GVSNs** differ. A **GVSN** is used to identify a unique version of a unique resource. In other words, no two different resources are ever assigned the same **GVSN**, and no two different updates to the same resource are ever assigned the same **GVSN**.

Global Version Sequence Numbers (GVSN): A GVSN is a pair: Machine identifier and **version sequence number (VSN)**. Although two machines might assign the same **VSN**, because they have different machine identifiers, the associated GVSNs differ. A GVSN is used to identify a unique version of a unique resource. In other words, no two different resources ever get assigned the same GVSN, and no two different updates to the same resource ever get assigned the same GVSN.

Globally Routable User Agent URI (GRUU): A **URI** that identifies a **user agent** and is globally routable. A URI possesses a GRUU property if it is useable by any **user agent client (UAC)** that is connected to the Internet, routable to a specific user agent instance, and long-lived.

globally unique identifier (GUID): A term used interchangeably with **universally unique identifier (UUID)** in Microsoft protocol technical documents (TDs). Interchanging the usage of these terms does not imply or require a specific algorithm or mechanism to generate the value. Specifically, the use of this term does not imply or require that the algorithms specified in [\[RFC4122\]](#) or [\[C706\]](#) must be used for generating the **GUID**. See also **universally unique identifier (UUID)**.

GOP: A group of pictures that starts with one **I-frame** and ends with the next I-frame, excluding the next I-frame, as described in [\[SMPT-VC-1\]](#).

gradient fill: A type of fill that applies gradient formatting to the background of a cell or an object.

gradient stop: A marker on a gradient spectrum that denotes where a specific color is introduced in gradient formatting.

gradient vector: A vector that indicates the direction of a gradient fill. The gradient vector is perpendicular to the bands of color.

grammar checker: An application that uses default or user-defined settings to search for grammatical errors in a document.

grand total: An aggregation of all of the field subtotals in a PivotTable report.

graph: A set of connected nodes.

graph maintenance: The process by which each **node** attempts to improve its connectivity within the **graph**.

graph object: An object that represents a chart and the datasheet that contains the data for that chart.

GraphicDropDown control: A type of DropDown control that can display custom graphics in a list of options.

Graphics Interchange Format (GIF): A compression format that supports device-independent transmission and interchange of bitmapped image data. The format uses a palette of up to 256 distinct colors from the 24-bit **RGB** color space. It also supports **animation** and a separate palette of 256 colors for each frame. The color limitation makes the GIF format unsuitable for reproducing color photographs and other images with gradients of color, but it is well-suited for simpler images such as graphics with solid areas of color.

gridline: A line that is drawn on a worksheet or table for use as a visual aid to distinguish between cells.

group: (1) An element that can contain fields and other groups in the data source for an InfoPath form. Controls that contain other controls, such as repeating tables and sections, are bound to groups.

(2) A named collection of users who share similar access permissions or roles.

(3) A named collection of quick links, colleagues, or memberships for the purpose of organization.

(4) A process of combining similar elements into a set in accordance with logical criteria. It is frequently used to combine sets of data from Online Analytical Processing (OLAP) databases or PivotTable reports.

(5) A collection of **objects** that can be treated as a whole.

(6) A collection of **players** within a **game session**. Typically, **players** are placed in a **group** when they serve a common purpose.

(7) A graph in which each node implements the group security model.

(8) A **cluster** group is a container for zero or more **cluster resources**, when referring to cluster groups. **Groups** enable **resources** to be combined into larger logical units and are owned by only one **node** in the **cluster** at a time.

(9) A **group object**.

group object: (1) A database object that represents a collection of user and group objects and has a **security identifier (SID)** value.

(2) In **Active Directory**, a group object has an object class group. A group has a forward link attribute member; the values of this **attribute** (2) either represent elements of the group (for example, objects of class user or computer) or subsets of the group (objects of class group). The back link attribute memberOf enables navigation from group members to the groups containing them. Some groups represent groups of security principals and some do not and are, for instance, used to represent email distribution lists.

(3) A database **object** that represents a collection of user and group **objects** and has a **security identifier (SID)** value.

(4) In **Active Directory**, a **group object** has an **object class** group. A **group** has a **forward link attribute** member; the values of this **attribute** either represent elements of the **group** (for example, **objects** of class user or computer) or subsets of the **group** (**objects** of class group). The representation of group subsets is called "nested group membership". The **back link attribute** memberOf enables navigation from **group** members to the **groups** containing them. Some **groups** represent **groups** of **security principals** and some do not and are, for instance, used to represent email distribution lists.

Group Policy Object (GPO): A collection of administrator-defined specifications of the policy settings that can be applied to groups of computers in a domain. Each GPO includes two elements: an object that resides in the **Active Directory** for the domain, and a corresponding file system subdirectory that resides on the sysvol DFS share of the Group Policy server for the domain.

group shape: A shape that contains a group of shapes.

group target application: A **target application** that stores credentials for a group of Secure Store Service (SSS) users. It references a set of **claims** (2) that represents the SSS users who can retrieve the credentials associated with it.

grow: The process of increasing the number of rows or **columns** (2) in a PivotTable report.

GUID: (1) A term used interchangeably with universally unique identifier (UUID) in Microsoft protocol technical documents (TDs). Interchanging the use of these terms does not imply or require a specific algorithm or mechanism to generate the value. Specifically, the use of this term does not imply or require that the algorithms described in [\[RFC4122\]](#) or [\[C706\]](#) need to be used to generate the GUID. See also **universally unique identifier (UUID)**.

(2) See **globally unique identifier (GUID)**.

GUID_NULL: A **GUID** that has the value "{00000000-0000-0000-0000-000000000000}".

GUIDString: A **GUID** in the form of an **ASCII** or **Unicode** string, consisting of one group of 8 hexadecimal digits, followed by three groups of 4 hexadecimal digits each, followed by one group of 12 hexadecimal digits. It is the standard representation of a GUID, as described in [\[RFC4122\]](#) section 3. For example, "6B29FC40-CA47-1067-B31D-00DD010662DA". Unlike a curly braced GUID string, a GUIDString is not enclosed in braces.

gutter: An area above a column heading and to the left of a row heading. A gutter typically displays outline symbols that are used to expand and collapse groups of cells.

10 H

handle: (1) Any token that can be used to identify and access an object such as a device, file, or a window.

(2) A 32-bit numerical ID that uniquely identifies a resource or a channel. Handles are allocated by the server and communicated to the client via resource or channel creation messages.

(3) A recipient of a message.

(4) A token that can be used to identify and access cursors, chapters, and bookmarks.

handout master slide: A slide that defines layout and positioning information for handout pages, which are pages that are optimized for printing a presentation.

hash: (1) A fixed-size result that is obtained by applying a one-way mathematical function, which is sometimes referred to as a hash algorithm, to an arbitrary amount of data. If the input data changes, the hash also changes. The hash can be used in many operations, including **authentication** (2) and digital signing.

(2) A hash, such as SHA-1, on the content or content block.

(3) A term that refers to either a hash function, the value computed by such a function, or the act of computing such a value.

hash code: See **hash**.

hash list: A list of **hashes** that include the **block hashes** and the **content hash**.

Hash-based Message Authentication Code (HMAC): A mechanism for message **authentication** (2) using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function (for example, **MD5** and **SHA-1**) in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function.

header: (1) A line, or lines, of content in the top margin area of a page in a document or a slide in a presentation. A header typically contains elements such as the title of the chapter, the title of the document, a page number, or the name of the author.

(2) A name-value pair that supplies structured data in an Internet email message or **MIME entity**.

(3) The structure at the beginning of a **compound file**.

header field: (1) A component of a Session Initiation Protocol (SIP) message header, as described in [\[RFC3261\]](#).

(2) As specified in section 4.2 of [\[RFC2616\]](#).

header row: (1) A row in a table, typically the first row, that contains labels for **columns** (2) in the table.

(2) A row at the beginning of a **category** (5) that does not represent data in the **Table object**, but provides information about a grouping.

health state: An abstract notion of the state of a machine that is used to indicate its compliance with network **policies**. Some examples of such state would include the state of the firewall on the machine, the version of the virus signature files for an antivirus application, and so on.

Help file: A file that contains the documentation for a specific product or technology.

Help topic identifier: A unique identifier for an article that contains Help content.

hidden: A condition of an object that prevents it from being displayed in rendered output.

hidden column: A **column** (2) that does not appear in a worksheet view because its width is set to 0 (zero). A column can be hidden if an outline is collapsed.

hidden protection: A cell protection property that prevents formulas, but not values, from appearing in a cell when a worksheet is **protected**.

hidden row: A row that does not appear in a worksheet view because its height is set to "0" (zero). A row can be hidden if the data is filtered or an outline is collapsed.

hierarchy: (1) A logical tree structure that organizes the members of a dimension such that each member has one parent member and zero or more child members.

(2) A logical tree structure that organizes a record such that each member has one parent member and zero or more child members.

(3) An arrangement of data items within the Master Data Services (MDS) system in a ranked or graduated series.

high-low lines: Supplemental lines that are added to a line chart and connect the maximum data points of one series with the minimum data points of another series for each **category** (3). High-low lines are typically used on stock charts.

historical version: Any version of a document or list item that is not one of the current versions. Depending on configuration settings, historical versions can be retained in a **back-end database server**, and might not be visible to specific users.

hit highlighted summary: A summary that appears on the search results page for each query result. It displays an excerpt from the item that contains the query text and applies highlight formatting to that query text.

HMAC-SHA1: See **SHA-1**.

home page: On the World Wide Web, a document that serves as a starting point for a set of webpages and other files in a website.

horizontal alignment: A formatting setting that specifies how content is positioned within the horizontal space of a cell, object, or page. Content can be aligned along the left or right edge, or distributed evenly across the horizontal space.

horizontal indent: An indent that is used in a cell to adjust cell content horizontally.

horizontal text: Text that is rendered horizontally in a cell.

host: (1) A general-purpose computer that is networking capable.

(2) In **DirectPlay**, the computer responsible for responding to **DirectPlay** game session enumeration requests and maintaining the master copy of all the **player** and group lists for the game. One computer is designated as the **host** of the **DirectPlay** game session. All other

participants in the **DirectPlay** game session are called **peers**. However, in peer-to-peer mode the name table entry representing the **host** of the session is also marked as a **peer**.

(3) A subcomponent of the naming **authority** in a **URI scheme**, as defined in [\[RFC3986\]](#) section 3.2.2.

(4) An interface between an application **runspace** and a user capable of responding to the host method calls specified in [\[MS-PSRP\]](#) section 2.2.3.17.

(5) The machine with the desktop or applications that are being **shared** with the other **participants**.

Host Candidate: A **candidate** that is obtained by binding to ports on the local interfaces of the host computer. The local interfaces include both physical interfaces and logical interfaces such as Virtual Private Networks (VPNs).

host data language: The **data culture** of a site.

host extender: An Automation type that is provided by a host application to extend the functionality of an **Automation server**.

host header: An Internet host and port number that identifies a network resource.

host hop: The process of traversing to a server with a different host name during a crawl.

host name: (1) The name of a physical server, as described in [\[RFC952\]](#).

(2) The name of a host on a network that is used for identification and access purposes by humans and other computers on the network.

hosted cache: A centralized cache comprised of **blocks** added by **peers**.

HRESULT: An integer value that indicates the result or status of an operation. A particular HRESULT can have different meanings depending on the protocol using it. See [\[MS-ERREF\]](#) section 2.1 and specific protocol documents for further details.

HTML fragment: Lines of text that adhere to HTML tag rules, as described in [\[HTML\]](#), but do not have processing instructions or any other type of header information.

HTTP GET: An **HTTP method** for retrieving a resource, as described in [\[RFC2616\]](#).

HTTP HEAD: An HTTP method for retrieving header information for a resource, as described in [\[RFC2616\]](#).

HTTP method: In an HTTP message, a token that specifies the method to be performed on the resource that is identified by the **Request-URI**, as described in [\[RFC2616\]](#).

HTTP OK: An **HTTP** response with status code 200, as described in [\[RFC2616\]](#) section 6.1.1.

HTTP OPTIONS: An HTTP method for determining the options and requirements that are associated with a resource, or the capabilities of a protocol server, as described in [\[RFC2616\]](#).

HTTP POST: An HTTP method, as described in [\[RFC2616\]](#).

HTTP proxy: An intermediary program that acts as both a server and a client for the purpose of making requests on behalf of other clients. For more information, see [\[RFC2616\]](#).

HTTP referer: A string in an HTTP request-header field that identifies the address of the resource that is making the current request, as described in [\[RFC2616\]](#).

hue-saturation-luminance (HSL): A color model that defines a color by using three dimensions: hue, the color itself; saturation, the purity of the color; and luminance, the amount of light that is either reflected or absorbed by the color. See also **color scheme** and **color space**.

hybrid compression: A type of data compression that uses a combination of **run length encoding** and bit-wise compression.

hyperlink: A relationship between two **anchors**, as described in [\[RFC1866\]](#).

hyperlink location: A portion of a hyperlink that specifies the location of a specific item, such as a **bookmark** (1), within a document, object, or other type of resource; for example “#bookmark” in the hyperlink location C:\Documents\Document.docx#bookmark.

Hypertext Markup Language (HTML): An application of the Standard Generalized Markup Language (SGML) that uses tags to mark elements in a document, as described in [\[HTML\]](#).

Hypertext Transfer Protocol (HTTP): An application-level protocol for distributed, collaborative, hypermedia information systems (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.

Hypertext Transfer Protocol 1.0 (HTTP/1.0): An application of the Standard Generalized Markup Language (SGML) that uses tags to mark elements in a document, as described in [\[HTML\]](#).

Hypertext Transfer Protocol 1.1 (HTTP/1.1): Version 1.1 of the Hypertext Transfer Protocol (HTTP), as described in [\[RFC2068\]](#).

Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS): An extension of **HTTP** that securely encrypts and decrypts webpage requests.

11 I

iCalendar: A standard content type for capturing calendar event information, as described in [\[RFC2445\]](#).

ICE keep-alive message: A message that is sent periodically to keep active the **NAT bindings** at **intermediate NATs** and allocations on the **TURN server**.

icon: A graphical image used to supplement alphanumeric text in the visual identification of an object on a computer monitor. Icons are typically small, relative to the size of the area on which they are displayed.

icon set: A collection of icons that can be used to comment and classify data into categories.

identifier: A string value that is used to uniquely identify a component of the **CSDL** and that is of type SimpleIdentifier.

Identifier: The **Field** (4) or **Fields** (4) that define the Identity of an EntityInstance. Also referred to as Key.

identity: (1) A digital persona that is associated with two key pairs, one for encrypting data and another for signing data.

(2) An account that represents a person (user account), an application (service account), and computers that participate in the domain (machine accounts). A password is used by the system as proof of an identity.

identity object: An entity that is a collection of one or more identity attributes. For example, an identity object could represent a user's account. An identity object is an abstraction over physical realizations such as **directory objects**.

identity provider (IP): A **security token service (STS)** that performs identity verification as part of its processing. For more information, see [\[WSFedPRP\]](#).

identity provider/security token service (IP/STS): An **STS** that may or may not be an **identity provider (IP)**. This term is used as shorthand to see both identity that verifies token services and general token services that do not verify identity. Note that the "/" symbol implies an "or" relationship.

identity URL: A string of characters that uniquely identifies an identity and conforms to the syntax of a URI, as described in [\[RFC3986\]](#).

identity-targeted message: A message that is destined for a specific resource handler and identity combination, regardless of the client device. The message address includes a resource URL, identity URL, and client device URL, where the client device URL is empty.

IdEnumerator: A type of **MethodInstance** that can be called to return the **Field** (4) values that represent the identity of EntityInstances of a specific Entity. IdEnumerator input is defined by the FilterDescriptors that are contained in the Method that contains the IdEnumerator.

IDispatch identifier (DispID): A 32-bit signed integer that is used in Automation interfaces to identify methods, properties, and arguments.

IDL: See **Interface Definition Language (IDL)**.

I-frame: A **video frame** that is encoded as a single image, such that it can be decoded without any dependencies on previous frames. Also referred to as Intra-Coded frame, Intra frame, and key frame.

IM MCU: A **Multipoint Control Unit (MCU)** that supports Instant Messaging (IM) conferencing.

image: A rectangular grid of pixels that has a definite height and a definite width and that can be displayed in a report.

Image Color Management (ICM): Technology that ensures that a color image, graphic, or text object is rendered as closely as possible to its original intent on any device despite differences in imaging technologies and color capabilities between devices.

IME: See **Input Method Editor (IME)**.

immediate conversion job: A **conversion job** that contains only one **conversion item** and is intended to be executed as a higher priority than a typical conversion job.

immediate translation job: A **translation job** that contains only one **translation item** and is executed as a higher priority than a typical translation job.

import: The process of creating a **conglomeration** or **partition** on a COMA server based on **modules** and configurations extracted from an **installer package file**.

import attribute flow: The process of updating the **metaverse** attribute values of the current metaverse object during an import operation.

in-band provisioning: A process in which a protocol client obtains configuration information from a protocol server.

inclusion list: A list of items to include in query results and to add to a search index the next time that a crawl occurs.

incremental crawl: A crawl process that includes logic to index only a subset of the items in a content source that is crawled based on item modifications.

indentation level: A measure of the distance between the position of content that is in a cell and the logical left side of the cell. An indentation level is equal to three spaces.

index column: A part of a search index that can be hosted by one server computer or virtual server. Each index column contains a unique set of indexed items.

index directory file: A file that is part of a **full-text index catalog**. It is used to store index keys from an associated content index file, which facilitates finding a specific content index record in the content index file.

index directory level: An array of **index directory pages** that contains **index keys** from an associated index and the positions of those keys in the index.

index directory page: A page that conforms to the index directory page structure that stores index directory records.

index identifier: An integer that uniquely identifies a full-text index component within a **full-text index catalog**.

index key: A key that references a record in a content index file or a scope index file. It consists of an index key string and a property identifier.

index key string: A sequence of bytes that specifies the value that is used to sort records in a content index file or a scope index file.

index partition: A part of an inverted index within a search system. In Search Server 2010 and Office SharePoint Server 2007 for Search, it is defined by a set of document distribution identifiers. In FAST Search Server 2010, it is defined by a search index within an **index column** and can be divided into additional index partitions.

index server: A server that is assigned the task of crawling.

index table file: A directory that is used to store an inventory of files in a **full-text index catalog**.

indexing: The process of extracting text and properties from files and storing the extracted values into the indexes (for text) and the property cache (for properties).

indexing service: (1) A service that traverses URL spaces and file systems to acquire items, including properties, to record in catalogs for those spaces and systems. The catalogs can then be used for tasks such as searching and auditing content.

(2) A service that creates **indexed catalogs** for the contents and properties of file systems. Applications can search the **catalogs** for information from the files on the **indexed** file system.

individual target application: A **target application** that stores credentials for Secure Store Service (SSS) users. It references an identity **claim** (2) that represents an SSS user who can retrieve the credentials that are associated with it.

inflectional form: A variant of a root token that has been modified according to the linguistic rules of a given language. For example, inflections of the verb "swim" in English include "swim," "swims," "swimming," and "swam."

Information Rights Management (IRM): A technology that provides persistent protection to digital data by using encryption, **certificates** (1), and **authentication** (2). Authorized recipients or users acquire a license to gain access to the protected files according to the rights or business rules that are set by the content owner.

initial offer: An offer that is sent by a **caller** and with the caller's **local candidates** when the caller initiates a media session with a **callee**.

ink: A process of entering text in handwritten form. Instead of converting handwritten text to typed text, ink is converted to an object and displayed exactly as it was written.

inner rectangle: In a cell that is formatted with a rectangular gradient, a rectangle that is formed by the leftmost, rightmost, topmost, and bottommost lines of pixels in which the initial color of the gradient is completely dissipated. See also **rectangular gradient**.

input cell: A cell in which each input value from a data table is substituted.

Input Method Editor (IME): An application that is used to enter characters in written Asian languages by using a standard 101-key keyboard. An IME consists of both an engine that converts keystrokes into phonetic and ideographic characters and a dictionary of commonly used ideographic words.

input source: A table, view, query, or schema diagram that is used as a data source for a query.

InputFilter: A **FilterDescriptor** type that is used while calling an operation for a line-of-business (LOB) system. An LOB system can use the value of an InputFilter as additional arguments for the operation.

InputOutputFilter: A **FilterDescriptor** type that is used while calling an operation for a line-of-business (LOB) system. An LOB system can use the value of an InputOutputFilter as additional arguments for the operation, and additional results of an operation that cannot be captured by ReturnPropertyDescriptor can be retrieved as a value of the InputOutputFilter.

insert row: A placeholder row at the bottom of a table. It is used to enter new records.

installer package file: A file that packages together **modules** and configuration states sufficient to create a **conglomeration** or **partition** on a server.

instance: (1) A unique publication of data for a **category** (4). It enables a **publisher** to publish data for the same category multiple times. An example is a publisher who uses two different **endpoints** (5) to publish data. These endpoints can publish the same category. However, each endpoint requires a different instance number to be considered a distinct publication by the **server** (2). An instance number is provided by the publishing client.

(2) A specific occurrence of a **game** running in a **game session**. A **game** application process or module may be created more than one time on a single computer system, or on separate computer systems. Each time a **game** application process or module is created, the occurrence is considered to be a separate **instance**.

Instant Message Delivery Notification (IMDN): A notification that is sent from a multipoint control unit (MCU) to the sender of a message. It contains details about any failures that occurred when forwarding the message to other participants in a conference.

Integrated Windows authentication: A configuration setting that enables negotiation of **authentication** (2) protocols in Internet Information Services (IIS). Integrated Windows authentication is more secure than Basic authentication, because the user name and password are hashed instead of plaintext.

Interactive Connectivity Establishment (ICE): A methodology that was established by the Internet Engineering Task Force (IETF) to facilitate the traversal of network address translation (NAT) by media.

interactive report: A visualization that has a presentation mode that provides sort, filter, and pivot capabilities for displaying different views of the data. The underlying data can be stored either in the workbook or in an external data source.

interface: (1) A specification in a **Component Object Model (COM)** server that describes how to access the methods of a class. For more information, see [\[MS-DCOM\]](#).

(2) A group of related function prototypes in a specific order, analogous to a C++ virtual interface. Multiple objects, of different object class, may implement the same interface. A derived interface may be created by adding methods after the end of an existing interface. In the Distributed Component Object Model (DCOM), all interfaces initially derive from IUnknown.

(3) This term is used exactly as specified in [\[C706\]](#) section "Introduction to the RPC API" in Part 2.

(4) A collection of messages used together. **Interfaces** support inheritance and extensibility through the Interface Query message as defined in [\[MS-RDPEXPS\]](#) section 1.3.2.1.1.

(5) Represents a network that can be reached over an **adapter**. Each **interface** has a unique **interface** identifier also known as an **interface** index. **Interfaces** that are active have an **adapter** that is providing connectivity to the network they represent. **Interfaces** that are inactive do not have an **adapter** providing connectivity unless an administrator disabled the **interface** after it already had an **adapter**. Routing a packet to a network represented by an **interface** will cause the router to allocate an **adapter** for that **interface**, and will establish a wide area network (WAN) connection to the remote network. Allocating an **adapter** to an **interface** is referred to as binding. In the case of a local area network (LAN) **interface**, the **interface** corresponds to an actual physical device in the computer, a LAN **adapter**. In the case of a WAN interface, the **interface** is mapped to a port at the time that a connection is established. The port could be a COM port, a parallel port, or a virtual port (for tunnels such as **PPTP** [RFC2637] and **L2TP** [RFC2661]). WAN interfaces have the additional quality that they typically receive a network address only at the time that a connection is established. For example, a WAN interface using PPP [RFC1661] receives its network layer address from the remote peer during the connection process. Receiving a network address as part of the connection process is sometimes referred to as late-binding.

Interface Definition Language (IDL): The International Standards Organization (ISO) standard language for specifying the **interface** for remote procedure calls. For more information, see [C706] section 4.

intermediate NAT: A network address translation (NAT) address that is present in the communication path of two **endpoints** (5).

internal identifier: (1) An integer that uniquely identifies any item in a **term store**.

(2) A Folder ID or Message ID, as described in [MS-OXCDATA].

internal version number: A number that increases monotonically and is used to identify conflicts when saving an item.

Internationalized Resource Identifier (IRI): A resource identifier that conforms to the rules for Internationalized Resource Identifiers, as defined in [RFC3987].

Internet Assigned Numbers Authority (IANA): A central repository for the protocol name and number registries that are used in many Internet protocols.

Internet Information Services (IIS): The services provided in Windows implementation that support web server functionality. **IIS** consists of a collection of standard **Internet protocol servers** such as HTTP and FTP in addition to common infrastructures that are used by other Microsoft **Internet protocol servers** such as SMTP, NNTP, and so on. **IIS** has been part of the Windows operating system in some versions and a separate install package in others. **IIS** version 5.0 shipped as part of Windows 2000, **IIS** version 5.1 as part of Windows XP, **IIS** version 6.0 as part of Windows Server 2003, and **IIS** version 7.0 as part of Windows Vista and Windows Server 2008.

Internet Key Exchange (IKE): The protocol that is used to negotiate and provide authenticated keying material for **security associations (SAs)** in a protected manner. For more information, see [RFC2409].

Internet message: A message, such as an email message, that conforms to the syntax that is described in [RFC2822].

Internet Protocol security (IPsec): A framework of open standards for ensuring private, secure communications over Internet Protocol (IP) networks through the use of cryptographic security services. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. The Microsoft

implementation of IPsec is based on standards developed by the Internet Engineering Task Force (IETF) IPsec working group.

Internet protocol server: A software program that implements the server host of a standard Internet protocol such as HTTP or FTP.

Internet Protocol version 4 (IPv4): An Internet protocol that has 32-bit source and destination addresses. IPv4 is the predecessor of IPv6.

Internet Protocol version 6 (IPv6): A revised version of the Internet Protocol (IP) designed to address growth on the Internet. Improvements include a 128-bit IP address size, expanded routing capabilities, and support for **authentication** (2) and privacy.

inverted index: (1) For each token that is encountered in a corpus of indexed items, a data structure that stores a list of postings that identify which documents matched and a list of occurrences that identify which position in each document.

(2) A persistent structure that contains the text content pulled out of files during **indexing**. The text in an inverted index maps from a word in a property to a list of the documents and locations within a document that contain that word.

INVITE: A **Session Initiation Protocol (SIP)** method that is used to invite a user or a service to participate in a session.

IP-PBX: A **PBX** that supports **Voice over IP (VoIP)**.

IPv4 address in string format: A string representation of an **IPv4** address in dotted-decimal notation, as described in [\[RFC1123\]](#) section 2.1.

IPv6 address in string format: A string representation of an **IPv6** address, as described in [\[RFC4291\]](#) section 2.2.

IRM protector: An application that converts a file to an encrypted format when a user downloads the file and to a nonencrypted format when a user uploads a rights-managed file. See also **Information Rights Management (IRM)**.

item: A unit of content that can be indexed and searched by a search application.

item identifier: (1) An integer that uniquely identifies an item in a SharePoint list.

(2) For tabular data, the identifier for a particular row.

iterative calculation: A **calculation mode** in which calculations are performed until a specific numeric condition is met or a maximum number of iterations is reached.

12 J

JavaScript Object Notation (JSON): A text-based, data interchange format that is used to transmit structured data, typically in **Asynchronous JavaScript + XML (AJAX)** web applications, as described in [\[RFC4627\]](#). The JSON format is based on the structure of ECMAScript (Jscript, JavaScript) objects.

jitter: A variation in a network delay that is perceived by the receiver of each packet.

job: (1) An inbound or outbound fax transmission that is awaiting transmission in the Fax Queue; the Fax Jobs are qualified as inbound or outbound based on this. The Fax Jobs are further qualified as follows: **queued** qualifies a Fax Job as awaiting transmission, and **active** qualifies a Fax Job as in process of being sent or received by the fax server.

(2) An object identifying an administrative action (for example, running a program) to be performed on specified **triggers** and **conditions** (for example, every day at a specific time).
Synonym for Task.

join: A combination of data from multiple sources that is based upon a common attribute or join condition.

Joint Photographic Experts Group (JPEG): A raster graphics file format for displaying high-resolution color graphics. JPEG graphics apply a user-specified compression scheme that can significantly reduce the file sizes of photo-realistic color graphics. A higher level of compression results in lower quality, whereas a lower level of compression results in higher quality. JPEG-format files have a .jpg or .jpeg file name extension.

justify distributed: A special, distributed-alignment setting that evenly distributes the last line of text in a cell. The setting is primarily used for East Asian languages. See also **distributed alignment**.

13 K

keepalive message: A protocol message that is sent between a protocol client and a protocol server to help ensure that a connection is considered active by all **endpoints** (5). Inactive connections are considered idle and are likely to be closed by either **endpoint** (5) to conserve resources.

Kerberos: (1) An **authentication** (2) system that enables two parties to exchange private information across an otherwise open network by assigning a unique key (called a **ticket**) to each user that logs on to the network and then embedding these tickets into messages sent by the users. For more information, see [\[MS-KILE\]](#).

(2) An **authentication** system that enables two parties to exchange private information across an otherwise open network by assigning a unique **key** (called a **ticket**) to each user that logs on to the network and then embedding these **tickets** into messages sent by the users. For more information, see [\[MS-KILE\]](#).

(3) An authentication access type as defined by [\[RFC1964\]](#).

Kerberos principal: A unique individual account known to the **Key Distribution Center (KDC)**. Often a user, but it can be a service offering a resource on the network.

key: (1) In the **registry**, a node in the logical tree of the data store.

(2) In cryptography, a generic term used to refer to cryptographic data that is used to initialize a cryptographic algorithm. **Keys** are also sometimes referred to as **keying material**.

(3) A 256-bit unsigned integer used internally by MC-DRT to identify a resource.

Key Distribution Center (KDC): The **Kerberos** service that implements the **authentication** and **ticket** granting services specified in the **Kerberos** protocol. The service runs on computers selected by the administrator of the **realm** or domain; it is not present on every machine on the network. It must have access to an **account** database for the **realm** that it serves. Windows **KDCs** are integrated into the **domain controller** role of a Windows Server acting as a Domain Controller. It is a network service that supplies **tickets** to **clients** for use in authenticating to services.

key performance indicator (KPI): A predefined measure that is used to track performance against a strategic goal, objective, plan, initiative, or business process. A visual cue is frequently used to communicate performance against the measure.

keying material: The data from which the **main mode (MM)** and **quick mode (QM) security association (SA) authentication** and **encryption keys** are generated.

KeyTip: A small, pop-up window that appears over commands on the **ribbon** when users press the ALT key. By pressing the key that is displayed in a KeyTip, users can execute the command that is associated with the KeyTip.

keyword: One or more words or phrases that site administrators identified as important for a search service application. A keyword provides a way to apply business rules to search results for queries that use the keyword.

keyword consumer: A site collection that uses a specific set of **keywords**, synonyms, and **best bets**.

keyword synonym: An alternate phrasing of a specific keyword. When users search for a keyword synonym, the search results include the same **best bet** results as for the keyword.

Knowledge Consistency Checker (KCC): An internal Windows component of the **Active Directory** replication that is used to create spanning trees for **domain controller** to **domain controller** replication and to translate those trees into settings of variables that implement the **replication** topology.

14 L

L2TP: Layer Two Tunneling Protocol, as defined in [\[RFC2661\]](#).

labeling policy: A policy that supports the addition of labels to a list item.

language code identifier (LCID): A 32-bit number that identifies the user interface human language dialect or variation that is supported by an application or a client computer.

LastIdFilter: A **FilterDescriptor** type that is used when querying a line-of-business (LOB) system in which data is to be returned in chunks. When requesting a new chunk, the filter can be populated with the EntityInstanceId of the last EntityInstance.

LDAP: (1) See **Lightweight Directory Access Protocol (LDAP)**.

(2) Lightweight Directory Access Protocol, which can be either version 2 [\[RFC1777\]](#), or version 3 [\[RFC3377\]](#).

LDAP Data Interchange Format (LDIF): A standard that defines how to import and export directory data between directory servers that use the **Lightweight Directory Access Protocol (LDAP)**, as described in [\[RFC2849\]](#).

LDAP Distinguished Name: A string representation of a **distinguished name (DN)** (4) used to access an object on a directory server via **Lightweight Directory Access Protocol (LDAP)**.

leader line: A line that connects a data label to its corresponding data point. The primary purpose of a leader line is to increase legibility.

leaf name: The segment of a URL that follows the last slash. If the resource is a directory, the leaf name can be an **empty string** (1).

left-to-right: A reading order in which characters in words are read from left to right, and words are read from left to right in sentences.

legal hold: A restriction that prevents a document from being modified or transactions from being entered for a record.

legend entry: An item in a chart legend that identifies a single series or **category** (3).

legend key: A symbol that is associated with a legend entry.

level: (1) A relative position in a hierarchy of data. A level is frequently used when describing how to navigate a hierarchy in an Online Analytical Processing (OLAP) database or a PivotTable report.

(2) The name of a set of members in a **dimension hierarchy**, such that all members of the set are at the same distance from the root of the hierarchy.

Library: (1) Part of the **Remoting Data Model**. A **Library** is a named unit that contains a collection of **Remoting Types**. For more information, see Library in [MS-NRTP] section 3.1.1.

(2) A storage device that contains one or more tape drives, a number of slots to hold tape cartridges, and an automated method for loading tapes.

library directory: A directory in which Microsoft Excel **add-ins** are installed.

license key: An array of bytes that enables access to a control according to the usage policies for that control.

Lightweight Directory Access Protocol (LDAP): The primary access protocol for **Active Directory**. Lightweight Directory Access Protocol (LDAP) is an industry-standard protocol, established by the Internet Engineering Task Force (IETF), which allows users to query and update information in a **directory service (DS)**, as described in [\[MS-ADTS\]](#).

LimitFilter: A **FilterDescriptor** type that is used when querying a line-of-business (LOB) system. Its value can be interpreted as a limit on the number of EntityInstances that are returned when the Method to which it belongs is called.

line chart: A type of chart in which data points in a series are connected by a line.

line style: A style, including width and dash type, that is applied to and alters the appearance of a line or **border**.

linear gradient: A type of gradient fill in which the color of a cell or other object gradually changes horizontally, vertically, or diagonally from one edge of the object to the other.

line-of-business (LOB) system: A software system that is used to store business data and can also contain business rules and **business logic** (2) that support business processes.

link: (1) An **attribute** (2) value that refers to a directory object and whose Attribute-Schema object specifies an even value for the linkId attribute. Also referred to as forward link.

(2) When the value of an attribute refers to a directory object, and the attribute's Attribute-Schema object has an even value for attribute linkId, then that attribute value is a link. Sometimes referred to as a forward link.

(3) A link is similar to an **association**, as specified in [\[MC-CSDL\]](#), but describes a unidirectional relationship between entity types instead of a bidirectional one. A link can be either a unidirectional relationship that occurs when two entity types are related via an association and only one of the entity types defines a NavigationProperty that is bound to the association or a reference to one direction of a bidirectional association between two entity types, as specified in [\[MC-CSDL\]](#).

(4) An **object** that refers to another item.

link fixup: A process that helps to ensure consistent paths to linked components.

linked object: (1) An object that is inserted into a document and continues to exist in a separate source file. If the object in the source file changes, the object in the document is updated automatically to reflect those changes.

(2) Application data that is referenced by documents from other applications.

list: (1) A container within a SharePoint site that stores list items. A list has a customizable schema that is composed of one or more fields.

(2) An organization of a region of cells into a tabular structure in a workbook.

(3) A **report item** on a report layout that displays data in a list format.

list form: A page that enables users to create, view, or edit an item in a list.

List Form Web Part: A type of **Web Part** that is used to display, edit, or view an item in a SharePoint list.

list identifier: A GUID that is used to identify a **list** (1) in a site collection.

list item: An individual entry within a SharePoint list. Each list item has a schema that maps to fields in the list that contains the item, depending on the content type of the item.

list item attachment: A file that is contained within a list item and is stored in a folder in the **list** (1) with the segment "Attachments".

list item identifier: See **item identifier**.

list schema: The **Collaborative Application Markup Language (CAML)** schema of a list.

list server template: A value that identifies the template that is used for a SharePoint list.

list template: An XML-based definition of list settings, including fields and views, and optionally list items. List templates are stored in .stp files in the content database.

list template identifier: A GUID that is used to identify a list template for a SharePoint list.

list view: A named collection of settings for querying and displaying items in a SharePoint list. There are two types of views: Personal, which can be used only by the user who created the view; and Public, which can be used by all users who have permission to access to the site.

list view page: A **Web Parts Page** that displays a view of a SharePoint list.

List View Web Part: A type of **Web Part** that generates HTML-based views of items in a SharePoint list.

Lite: An implementation that supports a minimal subset of Interactive Connectivity Establishment (ICE) functionality, as described in [\[MS-ICE2\]](#), to work with a Full ICE implementation. A Lite implementation responds to but does not send connectivity checks.

little-endian: Multiple-byte values that are byte-ordered with the least significant byte stored in the memory location with the lowest address.

lobby: A collection of objects that contains data about one or more participants who are waiting for the organizer or a presenter in a conference to admit participants to the conference.

LobSystem: A type of **MetadataObject** that represents a specific version of a line-of business (LOB) system. An LOB system can be a database or a web service.

LobSystemInstance: A type of **MetadataObject** that represents a specific deployed instance of a **line-of-business (LOB) system**, as represented by a **LobSystem**. LobSystemInstances are contained by LobSystems. LobSystemInstance Properties describe how to connect to an instance of the LobSystem that contains them by providing information such as the server name, connection string, and **authentication mode**.

local candidate: A **candidate** whose transport addresses are local transport addresses.

local LU: An LU 6.2 implementation ([\[MS-DTCLU\]](#) section 3.2) that uses the MSDTC Connection Manager: OleTx Transaction Protocol Logical Unit Mainframe Extension protocol [MS-DTCLU] to communicate with a **transaction manager**.

local name: (1) A defined name whose scope is limited to a specific sheet instead of the entire workbook.

(2) A string value that, together with an **XML namespace**, identifies **XML** element and attribute names. For more information, see [\[XMLNS-2ED\]](#).

local search scope: An administrator-defined **restriction** (1) that can optionally be added to a query to restrict the query results to items that are from a specific SharePoint site collection, site, or list.

local transport address: A transport address that is obtained by binding to a specific port from an IP address on the host computer. The IP address can be from physical interfaces or from logical interfaces such as Virtual Private Networks (VPNs).

locale: (1) A collection of rules and data that are specific to a language and a geographical area. A locale can include information about sorting rules, date and time formatting, numeric and monetary conventions, and character classification.

(2) An identifier, as specified in [\[MS-LCID\]](#), that specifies preferences related to language. These preferences indicate how dates and times are to be formatted, how items are to be sorted alphabetically, how strings are to be compared, and so on.

locale settings: (1) A collection of rules and data that are specific to a language and a geographic area. Locale settings include information about sorting rules, date and time formatting, numeric and monetary conventions, and character classification.

(2) A collection of system settings that specify the default code pages and associated bitmap font files for a computer. The default code pages and fonts enable a non-Unicode application written for one language version of a system to run correctly on another language version of a system.

localization: The process of adapting an application or documentation, including text and non-text elements, to meet the language, cultural, and political expectations and requirements of a specific geographic country or region.

localized name: The descriptive name of a **MetadataObject** for a specific locale.

location profile: A definition of an environment where local numbers can be resolved to identifiers that either route to unique enterprise users or form unique numbers in a public telephone network, as defined by the International Telecommunications Union (ITU) recommendation.

location profile description: An **XML document** that contains the name of a **location profile** and a set of **translation rules** that are associated with that profile.

locked: The condition of a cell, worksheet, or other object that restricts edits or modifications to it by users.

locked protection: A cell-protection property that restricts the editing of cell content when a worksheet is **protected**.

logical left: A position that is relative to the language orientation of a document. Logical left means left, except in a right-to-left language where it means right. Also referred to as leading edge.

logical palette: A **palette** that defines colors as device-independent values. Unlike the **system palette**, which has predefined, device-specific color definitions, a logical palette contains color values that can be defined entirely by an application. A logical palette entry must be mapped to the **system palette** entry in order for the custom colors to appear when the application is run.

logical right: A position that is relative to the language orientation of a document. Logical right means right, except in a right-to-left language where it means left. Also referred to as trailing edge.

logical top-left: A position that is relative to the language orientation of a document. Logical top-left is the upper-left corner of a range or object when in left-to-right mode. It is the upper-right corner when in right-to-left mode.

logical top-right: A position that is relative to the language orientation of a document. Logical top-right is the upper-right corner of a range or object when in left-to-right mode. It is the upper-left corner when in right-to-left mode.

logical unit (LU): An addressable network element in the Systems Network Architecture that serves as an access point to the network for programs and users, allowing them to access resources and communicate with other programs and users. For more information on logical units, see [\[SNA\]](#).

login name: A string that is used to identify a user or entity to an operating system, directory service, or distributed system. For example, in Windows-integrated authentication, a login name uses the form "DOMAIN\username".

long file name: A folder or file name that is longer than the 8.3 file name standard, which permits as many as eight characters followed by a period and a file name extension of three characters.

long-term credentials: A set of user-authentication credentials that consist of a user name and password, and are used by a protocol client to authenticate with a protocol server.

lookup field: A field of the Lookup type that enables users to select an item from another data source.

lossy network transports: A transport that cannot deliver a data payload reliably from a source to a destination.

LU Type 6.2 (LU 6.2): A type of **logical unit** designed to provide support for two or more distributed **application** programs cooperating to carry out some **work**. All communication provided by **LU 6.2** is program-to-program. For more information, see [\[LU62Peer\]](#).

15 M

machine identifier: A **GUID** that is unique for each machine.

macro: A set of instructions that are recorded or written, and then typically saved to a file. When a macro is run, all of the instructions are performed automatically.

macro sheet: A single, logical container that is used to store and run Excel 4.0 macro formulas.

Magazines: See Slots.

mail app: An **app for Office** that enhances an email or appointment item.

mail merge: The process of merging information into a document from a **data source** (1), such as an address book or database, to create customized documents, such as form letters or mailing labels.

mail merge data source: A file or **address book** that contains the information to be merged into a document during a mail merge operation.

mail merge header document: A file that contains the names of the **fields** (3) in a mail merge data source.

mailbox: A **message store** that contains email, calendar items, and other **Message objects** for a single recipient.

main data connection: The primary connection between an InfoPath form and a **data source** (2) that stores or provides data for the form. The main data connection defines the structure of the main data source of the form.

main data source: An **XML document** or **XML schema** that defines the collection of **fields** (1) and **groups** (1) that store data for an InfoPath form.

main master slide: A slide that defines the formatting and content that can be used by presentation slides. If a slide uses formatting and content from a main master slide, it is referred to as following a main master slide.

main mode (MM): The first phase of an **Internet Key Exchange (IKE)** negotiation that performs authentication and negotiates a **main mode security association (MM SA)** between the peers. For more information, see [\[RFC2409\]](#) section 5.

main mode security association (MM SA): A security association that is used to protect **Internet Key Exchange (IKE)** traffic between two peers. For more information, see [\[RFC2408\]](#) section 2.

major gridline: A horizontal or vertical line that is in the plot area of a chart and corresponds to the major scaling unit on an axis.

major scheme: A font scheme that is used for primary text elements, such as headings and titles, in a **theme**.

major tick mark: A **tick mark** that corresponds to a major scaling unit on an axis.

major version: An iteration of a software component, document, or list item that is ready for a larger group to see, or has changed significantly from the previous major version. For an item on a SharePoint site, the **minor version** is always "0" (zero) for a major version.

managed code: Code that is executed by the **common language runtime (CLR)** environment rather than directly by the operating system. Managed code applications gain CLR services, such as automatic garbage collection, runtime type checking, and security support. These services provide uniform behavior that is independent of platform and language.

managed property: A specific property that is part of a metadata schema. It can be exposed for use in search queries that are executed from the user interface.

management agent: A component that consists of properties, rules, and rules extensions that determine how an object is processed in the metadirectory. A single management agent can have one or more run profiles that determine the management agent's behavior, such as how or when the management agent runs.

management client: An application that uses the WSRM Protocol interfaces for the purpose of presenting a user interface that allows a user to perform the functions exposed by the WSRM Protocol.

management server: (1) A server application that is used to manage SharePoint Workspace and Groove identities and services.

(2) The server endpoint of the IPAM Management Protocol.

management service: An agent that implements the WSRM Protocol on a given computer by applying specified resource policies, returning requested **accounting** information, and storing the **accounting** data dumped by the other management services running on remote servers.

management state: A state switch with two values, running and stopped, that tells whether the **management service** can be active or inactive. "Running" means the service will perform all **resource management** and **accounting** functions according to its current policies. "Stopped" means that it will remain in an inactive state, doing nothing except making configuration changes that will take effect when the **management service** becomes active again; for example, import, export, creation, deletion, or modification of [resource allocation policy](#).

Mandarin phonetic symbols: A phonetic system for transcribing Chinese through the use of an alphabet that includes characters for all possible sounds in the spoken Mandarin language.

manifest: (1) A file that stores metadata about an expansion pack, such as the name of the expansion pack, the files and resources that are included in the expansion pack, and the dependencies that it has on other files and components.

(2) Metadata about the **presentation** that allows a client to make requests for **media**.

manual calculation mode: A **calculation mode** in which the formulas in a workbook are calculated only when specified by a user. See also **automatic calculation mode**.

manual filter: A filter that lets users select a set of individual data items or dimension hierarchies by using a user interface that displays levels from the hierarchies.

mapper: A **station** that initiates a **topology discovery test**.

marketplace license: The proof of an app purchase that defines the usage pattern that is allowed for the app.

marshal: To encode one or more data structures into an octet stream using a specific **remote procedure call (RPC)** transfer syntax (for example, marshaling a 32-bit integer).

marshaled server object: A server object that is created by a higher layer, and not in response to an incoming request (see **server-activated object (SAO)** for more information on the latter).

marshaled server object (MSO): (1) A **server object** that is created by a higher layer, and not in response to an incoming request. (See **server-activated object (SAO)** for more information on the latter.)

(2) A **Marshaled Server Object** is a **Server Object** that is created by a higher layer, and not in response to an incoming request. For more information on server objects, (see **Server-Activated Object (SAO)** for more information on the latter).. The .NET Remoting Lifetime Services Protocol [\[MS-NRSL\]](#) provides a mechanism for controlling the lifetimes of **marshaled server objects**.

master index component: A full-text index component that contains index keys that are extracted from a set of items. In a **full-text index catalog**, there is only one master index component. It is referenced by an `itMaster CIndexRecord`.

master key: A key that provides information for packet encryption and **authentication** (2) in **Secure Real-Time Transport Protocol (SRTP)** and **Scale Secure Real-Time Transport Protocol (SSRTP)** transactions.

master page: An **ASP.NET** file that has a predefined layout that can include static text, **HTML** elements, and server controls.

master secret: A key that is used to symmetrically encrypt and decrypt credentials and single sign-on (SSO) tickets.

master secret key: A symmetric encryption key that is used to encrypt and decrypt credentials and **Secure Store Service (SSS) tickets**.

master secret server: A protocol server that stores and can provide a master secret in response to a request from a protocol client.

master unit: A unit of linear measurement that is equal to 1/576 inch.

maximum transmission unit (MTU): The size, in bytes, of the largest packet that a given layer of a communications protocol can pass onward.

MCU-Conference-URI: A literal that specifies a URI that can be used to access conferencing services in the context of a **Multipoint Control Unit (MCU)**.

MCU-Type: A literal that identifies all of the media types, such as audio-video, that are supported by a **Multipoint Control Unit (MCU)**.

MD5: A one-way, 128-bit hashing scheme that was developed by RSA Data Security, Inc., as described in [\[RFC1321\]](#).

MD5 hash: A hashing algorithm, as described in [\[RFC1321\]](#), that was developed by RSA Data Security, Inc. An MD5 hash is used by the File Replication Service (FRS) to verify that a file on each replica member is identical.

MDX unique name: A unique identifier for a multidimensional expression (MDX) member or value in a given Online Analytical Processing (OLAP) cube, for example "[Customer].[Customer Geography].[Country].&[Australia]".

measure: In a cube, a set of values that are typically numeric and are based on a **column** (2) in the fact table of the cube. Measures are the central values that are aggregated and analyzed.

measure group: A collection of related **measures** in a **cube** that derive from a single fact table, typically in a data source view.

media: Compressed audio, video, and text data that is used by the client to play a **presentation**.

Media Access Control (MAC) address: A hardware address provided by the network interface vendor that uniquely identifies each interface on a physical network for communication with other interfaces, as specified in [\[IEEE802.3\]](#). It is used by the media access control sublayer of the data link layer of a network connection.

media data: The data for an audio or video **stream** in a **presentation**, encoded in a specific **format**.

Media Source ID (MSI): A 32-bit identifier that uniquely identifies an audio or video source in a conference.

meeting instance: A collection of data for a meeting that occurs only once or a single occurrence of a meeting that occurs multiple times. The data can be stored in a client application or on a website.

Meeting object: A **Calendar object** that has both an organizer and attendees.

Meeting Workspace: A website that is created by using the Meetings Web Services protocol, as described in [\[MS-MEETS\]](#). It can host documents, discussions, and other information about a meeting.

Meeting Workspace site: A SharePoint site that is based on a Meeting Workspace site template and has a template ID value of "2". A Meeting Workspace site is used for planning, posting, and working together on meeting materials.

member: (1) A user in the **Members group** of a site.

(2) An identity that belongs to a **shared space**.

(3) See **OLAP member**.

(4) A general term for a **tablix** member, data member, chart member, or gauge member.

(5) A single master data record that is stored in the Master Data Services (MDS) system.

(6) See **Class**.

member group: A group of users that is specific to a user profile service. Examples of types of member groups are distribution lists, security groups, and SharePoint sites. A member group contains metadata such as the group name, email address, URL, and a list of members.

member property: An **attribute** (1) on a data item within a specific dimension in an Online Analytical Processing (OLAP) database.

Members group: A default group of users on a SharePoint site. By default, the Members group is assigned the Contribute permission level.

membership: The state or status of being a member of a member group. A membership contains additional metadata such as the privacy level that is associated with the membership.

membership group: See **group** (2).

menu toolbar: A type of toolbar that is displayed in an application window, typically at the top, and provides a set of menu controls from which the user can select. Activating a control on the toolbar displays a list of commands in that menu, and the menu remains open until the user closes it or chooses a menu command.

merged cell: A single cell that is created by combining two or more **adjacent cells**.

merged range: A **range** that contains one or more merged cells.

merged term: A single **term** that is the combination of and has the semantic meaning of two, previously distinct terms.

mesh: (1) A network of nodes that are all identified with the same **mesh name**.

(2) The covering of the surface of an object by triangular shapes without gaps or overlaps.

mesh name: A set of nodes that establish connections to each other to form a **mesh**.

message: (1) A data structure representing a unit of data transfer between distributed applications. A message has **message properties**, which may include message header properties, a **message body** property, and message trailer properties.

(2) See **message tag (MTAG)**.

(3) A fax that a fax server has completely received or transmitted, and **archived** to the Fax Archive Folder described in [MS-FAX] section 3.1.1.

(4) An atomic unit in the OMA-DM protocol.

Message Authentication Code (MAC): A message authenticator computed through the use of a symmetric key. A **MAC** algorithm accepts a secret key and a data buffer, and outputs a **MAC**. The data and **MAC** can then be sent to another party, which can verify the integrity and authenticity of the data by using the same secret key and the same **MAC** algorithm.

Message Bar notification: A message that appears in the area below the **ribbon** in an application window. It can be a security **alert** (2), or information about a workflow task, the active document, or a policy.

message body: (1) The content within an HTTP message, as described in [\[RFC2616\]](#).

(2) The main message text of an email message. A few properties of a **Message object** represent its message body, with one property containing the text itself and others defining its **code page** and its relationship to alternative body formats.

(3) A distinguished **message property** that represents the application payload.

(4) As specified in [\[RFC2616\]](#) section 4.3.

message identifier: (1) A string that uniquely identifies an email message.

(2) An index into a message table. A message table is a collection of localizable strings. For Windows implementations, the message table is stored in the resource section of a dynamic link library.

Message object: A set of properties that represents an email message, appointment, contact, or other type of personal-information-management object. In addition to its own properties, a

Message object contains recipient properties that represent the addressees to which it is addressed, and an **attachments table** that represents any files and other Message objects that are attached to it.

message property: A data structure that contains a **property identifier** and a value, and that is associated with a **message**.

message queue: A data structure containing an ordered list of zero or more **messages**. A **queue** has a head and a tail and supports a first in, first out (FIFO) access pattern. **Messages** are appended to the tail through a write operation (Send) that appends the **message** and increments the tail pointer. **Messages** are consumed from the head through a destructive read operation (Receive) that deletes the **message** and increments the head pointer. A **message** at the head may also be read through a nondestructive read operation (Peek).

message store: A unit of containment for a single hierarchy of Folder objects, such as a mailbox or public folders.

message tag (MTAG): (1) A message that is sent between participants in the context of connections.

(2) A 4-byte integer value that describes the message type and its interpretation.

Messaging Application Programming Interface (MAPI): (1) A messaging architecture that enables multiple applications to interact with multiple messaging systems across a variety of hardware platforms.

(2) A Windows programming interface that enables email to be sent from within a Windows application.

metadata: (1) XML-formatted data that defines the characteristics of an **update**, including its title, description, rules for determining whether the **update** is applicable to a **client computer**, and instructions for installing the **update** content.

(2) A generic term for a **hash** or **hash list**.

metadata index: A data structure that is stored on a **back-end database server**. It stores properties that are associated with each item, and the **attributes** (1) of those properties.

metadata schema: A schema that is used to manage information about an item.

metadata store: A database that is stored on a **back-end database server** and contains all stored procedures and storage for the **MetadataObject** types.

MetadataCatalog: A **MetadataObject** that represents a Metadata partition.

MetadataModel: A collection of **MetadataObjects** that describes a line-of-business (LOB) system. It provides a framework for converting operations that are requested by a protocol client into requests that are specific to a given LOB system.

MetadataObject: An abstract data structure that consists of a set of **attributes** (1) that represent a LobSystem, LobSystemInstance, DataClass, Entity, Method, MethodInstance, Parameter, TypeDescriptor, Identifier, FilterDescriptor, **Action**, **ActionParameter**, or **Association**.

MetadataObjectId: An **attribute** (1) that uniquely identifies a **MetadataObject** that is stored in a metadata store.

metadict: A **dictionary** that has strongly typed values.

metafile: (1) A file that stores an image as graphical objects, such as lines, circles, and polygons, instead of pixels. A metafile preserves an image more accurately than pixels when an image is resized.

(2) A sequence of record structures that store an image in an application-independent format. Metafile records contain drawing commands, object definitions, and configuration settings. When a metafile is processed, the stored image can be rendered on a display, output to a printer or plotter, stored in memory, or saved to a file or stream.

metakey: A string in a **metadict** that is mapped to a strongly-typed value.

metaverse: A storage area that contains the aggregated information from multiple connected data sources, providing a single global, integrated view of all combined objects.

Method: A type of **MetadataObject** that represents a piece of executable **business logic** (2) in a line-of-business (LOB) system. Methods are contained by DataClasses and they contain Parameters.

MethodInstance: A type of **MetadataObject** that associates a normalized or stereotypical semantic with a Method that represents a native API in a line-of-business (LOB) system. MethodInstances identify which part of the data that is returned by a Method is relevant for the semantic by defining a **ReturnPropertyDescriptor**. MethodInstances are contained by Methods.

Microsoft Message Queuing (MSMQ): A communications service that provides asynchronous and reliable **message** passing between distributed **applications**. In **Message Queuing**, **applications** send **messages** to **queues** and consume **messages** from **queues**. The **queues** provide persistence of the **messages**, enabling the sending and receiving **applications** to operate asynchronously from one another.

Microsoft Terminal Services (TS): A component that allows a user to access applications or data stored on a remote computer over a network connection.

MIME Encapsulation of Aggregate HTML Documents (MHTML): A MIME-encapsulated HTML document, as described in [\[RFC2557\]](#).

MIME entity: An entity that is as described in [\[RFC2045\]](#), [\[RFC2046\]](#), and [\[RFC2047\]](#).

MIME type: A method that is used by protocol clients to associate files of a certain type with applications that can open or access files of that type.

minimal save: A process that saves only critical workbook data to disk when errors are detected during a file save operation.

minor gridline: A horizontal or vertical line that is in the plot area of a chart and corresponds to the minor scaling unit on an axis.

minor scheme: A font scheme that is used for secondary text elements, such as body text, in a **theme**.

minor tick mark: A **tick mark** that corresponds to a minor scaling unit on an axis.

minor version: An iteration of a software component, document, or list item that is in progress or has changed only slightly from the previous version. For an item on a SharePoint site, the minor version number is never "0" (zero) and is incremented for each new version of an item, unless a **major version** is explicitly published. When minor versioning is disabled on a

SharePoint site, only major version numbers are incremented, and the minor version is always "0" (zero).

mixed mode: A state of an **Active Directory domain** that supports **domain controllers (DCs)** running Windows NT Server 4.0. Mixed mode does not allow organizations to take advantage of new **Active Directory** features such as universal groups, nested group membership, and interdomain group membership. See also **native mode**.

mixer: (1) An intermediate system that receives a set of media **streams** (2) of the same type, combines the media in a type-specific manner, and redistributes the result to each **participant** (2).

(2) An intermediate system that receives **RTP packets** from one or more sources, possibly changes the data format, combines the packets in some manner and then forwards a new **RTP packet**. Because the timing among multiple input sources will not generally be synchronized, the mixer will make timing adjustments among the **streams** and generate its own timing for the combined **stream**. Thus, all data packets originating from a mixer will be identified as having the mixer as their **synchronization source**. See [\[RFC3550\]](#) section 3.

mobile device: A small computing device that is easily portable and can be used in various environments.

Model: A **MetadataObject** that defines a set of references to a logically related set of Entities. Models are typically used to facilitate easy transfer into and out of Metadata stores.

moderated list: See **moderated object**.

moderated object: An object for which a moderator reviews and either approves or rejects additions or changes to that object or to objects that are contained by that object. New objects and changes to existing objects can be seen by other users only after they have been approved by the moderator.

moderation status: A content approval status that indicates whether a list item was approved by a moderator.

Modified Alleged Rivest Cipher 4 (MARC4) algorithm: A variable, key-length, symmetric encryption algorithm that discards the first 256 bytes of a keystream.

module: (1) A collection of routines and data structures that performs a specific task or implements a specific abstract data type. Modules usually consist of two parts, a module header and a module body. A module header is a set of name/value attribute pairs that specify the linguistic characteristics of the module. A module body is the VBA source code, a set of declarations followed by procedures. VBA supports two types of modules, **procedural modules** and class modules.

(2) A file used by a server to register and instantiate one or more components. It contains either implementations of the components or metadata that a server can use to find implementations.

(3) A BLOB in the Desired State Configuration Pull Model Protocol [MS-DSCPM]. The protocol does not process the content of the BLOB, and it is passed as it is to the higher layer.

moniker: An object that stores information that uniquely identifies a Component Object Model (COM) object and allows that object to be located and activated.

motion path: A set of related coordinates, typically in pixels, that define how to render an object, such as a curve or line, or an **animation**. Also referred to as path.

Mount: To move **physical media** from a **library slot** to a **drive**.

moving average: A type of trendline that is calculated based on the most recent period of data points in a series.

ms-diagnostics header: A header that is added to a **Session Initiation Protocol (SIP)** response, BYE request, or CANCEL request to convey troubleshooting information.

ms-diagnostics-public header: A header that is added to a **Session Initiation Protocol (SIP)** response, BYE request, or CANCEL request to convey troubleshooting information. Unlike the **ms-diagnostics header**, the ms-diagnostics-public header does not contain a "source" parameter.

MSMQ: See **Microsoft Message Queuing (MSMQ)**.

MSMQ Directory Service: A network directory service that provides directory information, including key distribution, to **MSMQ**. It initially shipped in the Windows NT 4.0 Option Pack as part of **MSMQ**. This directory service predates and is superseded by **Active Directory (AD)**.

MSMQ object: Any one of the objects stored by **MSMQ** in its directory service. An object has a class name and a set of properties.

MSMQ queue manager: An **MSMQ** service hosted on a machine that provides **queued** messaging services. **Queue managers** manage **queues** deployed on the local computer and provide asynchronous transfer of **messages** to **queues** located on other computers. A **queue manager** is identified by a **globally unique identifier (GUID)**.

MSMQ routing server: A role played by an **MSMQ queue manager**. An MSMQ routing server implements store and forward messaging. A routing server may provide connectivity between different **connected networks** within a **site** or may provide session concentration between **sites**.

MSMQ site: A network of computers, typically physically collocated, that have high connectivity as measured in terms of latency (low) and throughput (high). A site is represented by a site object in the directory service. An MSMQ site maps one-to-one with an **Active Directory** site when **Active Directory** provides directory services to **MSMQ**.

MSMQ site gate: An **MSMQ routing server** through which all intersite messaging traffic flows.

multibyte character set (MBCS): An alternative to **Unicode** for supporting character sets, like Japanese and Chinese, that cannot be represented in a single byte. Under **MBCS**, characters are encoded in either one or two bytes. In two-byte characters, the first byte, or "lead" byte, signals that both it and the following byte are to be interpreted as one character. The first byte comes from a range of codes reserved for use as lead bytes. Which ranges of bytes can be lead bytes depends on the **code page** in use. For example, Japanese **code page** 932 uses the range 0x81 through 0x9F as lead bytes, but Korean **code page** 949 uses a different range.

multicast: (1) A content delivery method in which a single stream is transmitted from a media server to multiple clients. The clients have no connection with the server. Instead, the server sends a single copy of the stream across the network to multicast-enabled routers, which replicate the data. Clients can then receive the stream by monitoring a specific multicast IP address and port.

(2) A style of resource location or a data transmission in which a client makes a request to specific parties on a network simultaneously.

(3) Allows a host to send data to only those destinations that specifically request to receive the data. In this way, **multicasting** differs from sending broadcast data, because broadcast data is sent to all hosts. **multicasting** saves network bandwidth because **multicast** data is received only by those hosts that request the data, and the data travels over any link only once. **multicasting** saves server bandwidth because a server has to send only one **multicast** message per network instead of one **unicast** message per receiver.

(4) The ability of a transport protocol, such as User Datagram Protocol (UDP), to deliver messages to a group of recipients simultaneously without duplication of message unless the link to recipients is split.

(5) The delivery of data from one source to multiple destinations over a network. Copies of the data are made only when it needs to be transmitted on different branches containing the destinations. A minimal spanning tree-based communication where the source sits at the root of the tree, the destinations are on the other nodes, and packets travel down replicated only when necessary.

multicasting: The process by which data is transmitted over a network to multiple recipients simultaneously.

multidimensional expression (MDX): A syntax that is used for defining multidimensional objects, and for querying and manipulating multidimensional data.

multimedia session: A set of concurrent **RTP sessions** among a common group of **participants** (2). For example, a video **conference** (1) (which is a multimedia session) may contain an audio **RTP session** and a video **RTP session**. See [\[RFC3550\]](#) section 3.

Multipoint Control Unit (MCU): A server **endpoint** (5) that offers mixing services for multiparty, multiuser conferencing. An MCU typically supports one or more media types, such as audio, video, and data.

Multipurpose Internet Mail Extensions (MIME): A set of extensions that redefines and expands support for various types of content in email messages, as described in [\[RFC2045\]](#), [\[RFC2046\]](#), and [\[RFC2047\]](#).

multivalue property: A property that can contain multiple values of the same type.

multi-valued claim: See the definition of **claim**.

16 N

name record: The **NetBIOS name-to-IPv4** address mapping.

name table: The list of systems participating in a **DXDiag**, **DirectPlay 4**, or **DirectPlay 8** session, as well as any application-created groups.

named object: A **list** (2), PivotTable report, chart, or range that can be referenced by name. A sheet is not a type of named object.

named object view: A mode in which only named objects are rendered.

named pipe: A named, one-way, or duplex pipe for communication between a pipe server and one or more pipe clients.

named property: A property that is identified by both a GUID and either a string name or a 32-bit identifier.

named range: See **defined name**.

named set: A grouping of dimension members or items from a data source or a set expression that is named and treated as a single unit and that can be referenced or reused multiple times.

namespace: (1) A name that is defined on the **schema** (2) and that is subsequently used to prefix **identifiers** to form the **namespace qualified name** of a structural type.

(2) An abstract container that provides context for the items (names, technical terms, or words) that it holds and allows disambiguation of items that have the same name (residing in different **namespaces**).

(3) The entire **collection** (as specified in [\[RFC4918\]](#) section 5.2) of items under a request **URI**.

namespace qualified name: A qualified name that refers to a structural type by using the name of the **namespace** (1), followed by a period, followed by the name of the structural type.

naming context (NC): An **NC** is a set of objects organized as a tree. It is referenced by a **DSName**. The **DN** of the **DSName** is the distinguishedName **attribute** of the tree root. The **GUID** of the **DSName** is the objectGUID **attribute** of the tree root. The **security identifier (SID)** of the **DSName**, if present, is the objectSid **attribute** of the tree root; for **Active Directory Domain Services (AD DS)**, the **SID** is present if and only if the **NC** is a **domain naming context (domain NC)**. **Active Directory** supports organizing several **NCs** into a tree structure.

NAP: See **Network Access Protection (NAP)**.

narrow katakana: A non-cursive **character set** (1) that is used to write non-Japanese words phonetically in Japanese. Narrow katakana characters are represented with a single byte. Also referred to as half-width katakana.

NAT binding: The string representation of the protocol sequence, NetworkAddress, and optionally the endpoint. Also referred to as "string binding." For more information, see [\[C706\]](#) section "String Bindings."

native mode: A state of an **Active Directory** domain in which all current and future **domain controllers (DCs)** use AD style domains. Native mode allows organizations to take advantage of the new **Active Directory** features such as universal groups, nested group membership, and interdomain group membership.

native PivotTable: A PivotTable report that is populated with data from a worksheet in the same workbook.

natural language query: (1) Query text that contains words and does not contain any property **restrictions** (1).

(2) A query constructed using human language instead of query syntax. The generic search service (GSS) is free to interpret the query in order to determine the best results. The interpretation is explicitly not specified in order to allow improvements over time.

navigation node: An element in the navigational structure of a site. The element is a link or a series of links to a specific page in the site.

navigation node element identifier: An integer that identifies a navigation node. This value is unique for every navigation node in the navigational structure of a SharePoint site.

navigation structure: A hierarchical organization of links between related content on a site.

NC: See **naming context (NC)**.

NC replica: A variable containing a tree of **objects** whose root **object** is identified by some **naming context (NC)**.

NetBIOS: A particular network transport that is part of the LAN Manager protocol suite.

NetBIOS uses a broadcast communication style that was applicable to early segmented local area networks. The LAN Manager protocols were the default in Windows NT environments prior to Windows 2000. A protocol family including name resolution, datagram, and connection services. For more information, see [\[RFC1001\]](#) and [\[RFC1002\]](#).

NetBIOS name: A 16-byte address that is used to identify a **NetBIOS** resource on the network. For more information, see [\[RFC1001\]](#) and [\[RFC1002\]](#).

NetBIOS Name Server (NBNS): A server that stores NetBIOS name-to-IPv4 address mappings and that resolves NetBIOS names for NBT-enabled hosts. A server running the Windows Internet Name Service (WINS) is the Microsoft implementation of an NBNS.

network access client (NAC): An endpoint that establishes a call session to a **NAS** in order to perform network access.

Network Access Protection (NAP): A feature of an operating system that provides a platform for system health-validated access to private networks. **NAP** provides a way of detecting the health state of a network client that is attempting to connect to or communicate on a network, and limiting the access of the network client until the health policy requirements have been met. **NAP** is implemented through quarantines and health checks, as specified in [\[TNC-IF-TNCCSPBSoh\]](#).

network access server (NAS): A computer server that provides an access service for a user who is trying to access a network. A **NAS** operates as a client of **RADIUS**. The **RADIUS client** is responsible for passing user information to designated **RADIUS servers** and then acting on the response returned by the **RADIUS server**. Examples of a NAS include: a VPN server, Wireless Access Point, 802.1x-enabled switch, or **Network Access Protection (NAP)** server.

network address translation (NAT): The process of converting between IP addresses used within an intranet, or other private network, and Internet IP addresses.

network byte order: The order in which the bytes of a multiple-byte number are transmitted on a network, most significant byte first (in **big-endian** storage). This may or may not match the order in which numbers are normally stored in memory for a particular processor.

new form: A form that enables users to create a list item.

new workbook session: A **session** (2) that is not based on an existing workbook file.

next hop: The next router on the path toward a **destination**. Packets from a source are forwarded to a **destination** on a hop-by-hop basis.

next hops: Routes have one or more **next hops** associated with them. If the **destination** is not on a directly connected network, the **next hop** is the address of the next router (or network) on the outgoing network that can **best route** data to the **destination**. Each **next hop** is uniquely identified by the address of the **next hop** and the **interface** index used to reach the **next hop**. If the **next hop** itself is not directly connected, it is marked as a "remote" **next hop**. In this case, the **forwarder** must perform another lookup using the next hop's network address. This lookup is necessary to find the "local" **next hop** used to reach the remote **next hop** and the **destination**.

ninched: A condition in which a group of selected cells or objects do not share a specific property. For example, if a selection has three cells and only two of the cells share the same color formatting, the color formatting of the selection is in a ninched state.

NLCheck: An API that is implemented by **grammar checkers** that were developed by Microsoft Corporation.

node: (1) A location in a diagram that can have links to other locations.

(2) A computer system that is configured as a member of a **cluster**. That is, the computer has the necessary software installed and configured to participate in the **cluster**, and the **cluster** configuration includes this computer as a member.

(3) An instance of the Peer-to-Peer Graphing Protocol.

(4) An entry identified by name in a DNS **zone**. A **node** contains all of the DNS records sets associated with the name.

(5) An **endpoint** in the computer network that can receive, send, or process a SOAP message, as specified in [\[SOAP1.2-2/2007\]](#).

(6) An instance of PNRP running on a machine.

(7) An instance of DRT running on a machine.

(8) An instance of a channel **endpoint** participating in the **mesh** that implements the Peer Channel Protocol.

node ID: A statistically unique 64-bit identifier for a **node** in a **graph**. A **node ID** must be unique within a **graph**.

noise word: (1) See **stop word**.

(2) A word that is ignored by the Windows Search service (WSS) when present in the restrictions specified for the search query, because it has little discriminatory value. English

examples include "a," "and," and "the." Implementers of a generic search service (GSS) MAY choose to follow this guideline.

nominated: A **candidate pair** for which the nominated flag is set.

nonce: A number that is used only once. This is typically implemented as a random number large enough that the probability of number reuse is extremely small. A nonce is used in authentication protocols to prevent replay attacks. For more information, see [RFC2617].

non-contiguous range: A selected **range** that includes non-adjacent cells.

Normal view: A document view that displays text formatting and a simplified page layout of a document. The Normal view hides some layout elements such as the header and footer. Referred to as Draft view in Office Word 2007 and Word 2010.

notes slide: A slide that contains presentation notes or other information that is not displayed during a slide show. The formatting and content of a notes slide can derive from a notes master slide.

notification: (1) A process in which a subscribing **Session Initiation Protocol (SIP)** client is notified of the state of a subscribed resource by sending a NOTIFY message to the subscriber.

(2) A typed buffer of data sent by a **print server** to a **print client** as a result of an event on the server.

(3) The act of a notifier sending a **NOTIFY** message to a subscriber to inform the subscriber of the state of a resource.

NOTIFY: A method that is used to notify a **Session Initiation Protocol (SIP)** client that an event requested by an earlier SUBSCRIBE method has occurred. The notification optionally provides details about the event.

novice: The side of a **Remote Assistance connection** that shares its screen with the other computer in order to receive help.

NT File System (NTFS): The native file system for Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2. For more information, see [\[MSFT-NTFS\]](#).

NT LAN Manager (NTLM) Authentication Protocol: A protocol using a challenge-response mechanism for **authentication** (2) in which clients are able to verify their identities without sending a password to the server. It consists of three messages, commonly referred to as Type 1 (negotiation), Type 2 (challenge) and Type 3 (authentication). For more information, see [\[MS-NLMP\]](#).

nTDSDSA object: An **object of class** nTDSDSA that is always located in the **configuration naming context (config NC)**. This **object** represents a **domain controller (DC)** in the **forest**. See [\[MS-ADTS\]](#) section 6.1.1.2.2.1.2.1.1.

NTFS: See **NT File System (NTFS)**.

NULL cipher: A cipher that does not modify a **Real-Time Transport Protocol (RTP)** payload and is defined in the **Secure Real-Time Transport Protocol (SRTP)** protocol. It is used when **RTP packet** encryption is not necessary, but packet **authentication** (1) is necessary.

NULL GUID: A **GUID** of all zeros.

number format: A property of a cell or other type of object that determines how numerical data is displayed or interpreted. For example, a currency number format affixes the proper currency symbol to the number.

obfuscation key: A secret shared key combined with a cryptographic hash function that is intended to prevent a reversal of an encoding process. See also **XOR obfuscation**.

object: (1) A set of **attributes** (1), each with its associated values. Two attributes of an object have special significance: an identifying attribute and a parent-identifying attribute. An identifying attribute is a designated single-valued attribute that appears on every object; the value of this attribute identifies the object. For the set of objects in a replica, the values of the identifying attribute are distinct. A parent-identifying attribute is a designated single-valued attribute that appears on every object; the value of this attribute identifies the object's parent. That is, this attribute contains the value of the parent's identifying attribute, or a reserved value identifying no object. For the set of objects in a replica, the values of this parent-identifying attribute define a tree with objects as vertices and child-parent references as directed edges with the **child** as an edge's tail and the parent as an edge's head. Note that an object is a value, not a variable; a replica is a variable. The process of adding, modifying, or deleting an object in a replica replaces the entire value of the replica with a new value. As the word replica suggests, it is often the case that two replicas contain "the same objects". In this usage, objects in two replicas are considered the same if they have the same value of the identifying attribute and if there is a process in place (replication) to converge the values of the remaining attributes. When the members of a set of replicas are considered to be the same, it is common to say "an object" as shorthand referring to the set of corresponding objects in the replicas.

(2) In **Active Directory**, an **entity** consisting of a set of attributes, each attribute with a set of associated values. For more information, see [\[MS-ADTS\]](#).

(3) In **COM**, a software entity that implements the IUnknown interface and zero or more additional interfaces that may be obtained from each other using the IUnknown interface. A COM object can be exposed to remote clients via the DCOM protocol, in which case it is also a DCOM object.

(4) In the DCOM protocol, a software entity that implements one or more object remote protocol (ORPC) interfaces and which is uniquely identified, within the scope of an object exporter, by an **object identifier (OID)** (1). For more information, see [\[MS-DCOM\]](#).

(5) A set of attributes, each with its associated values. For more information on objects, see [\[MS-ADTS\]](#) section 1 or [\[MS-DRSR\]](#) section 1.

(6) In Active Directory, an entity consisting of a set of attributes, each attribute with a set of associated values. For more information, see [\[MS-ADTS\]](#). See also **directory object**.

(7) In **COM**, a software entity that implements the IUnknown interface and zero or more additional interfaces that may be obtained from each other using the IUnknown interface. A **COM object** can be exposed to remote clients via the DCOM protocol, in which case it is also a **DCOM object** (4).

(8) In the **DCOM** protocol, a software entity that implements one or more object remote protocol (ORPC) interfaces and which is uniquely identified, within the scope of an **object exporter**, by an **object identifier (OID)** (1). For more information, see [\[MS-DCOM\]](#).

(9) In COM, an instance of an object class. Each object implements one or more interfaces that may be obtained from each other by using the IUnknown interface.

(10) The root of the type hierarchy. For more information, see [\[ECMA-335\]](#).

(11) A file, email, email attachment, contact, calendar appointment or any other self-contained item that can be **indexed** and searched for by the **GSS**.

object class: (1) A predicate defined on **objects** (1) that constrains their **attributes** (1). Also an identifier for such a predicate.

(2) A set of restrictions on the construction and update of objects. An object class can specify a set of must-have attributes (every object of the class must have at least one value of each) and may-have attributes (every object of the class may have a value of each). An object class can also specify the allowable classes for the parent object of an object in the class. An object class can be defined by single-inheritance; an object whose class is defined in this way is a member of all object classes used to derive its most specific class. An object class is defined in a classSchema object.

(3) In **COM**, a category of **objects** (3) identified by a CLSID, members of which can be obtained through activation of the CLSID.

(4) In the DCOM protocol, a category of **objects** (4) identified by a CLSID, members of which can be obtained through activation of the CLSID. An object class is typically associated with a common set of interfaces that are implemented by all objects in the object class.

(5) A predicate defined on objects that constrains their attributes. Also an identifier for such a predicate.

(6) A set of restrictions on the construction and update of objects. An **object class** can specify a set of must-have attributes (every object of the class must have at least one value of each) and may-have attributes (every object of the class may have a value of each). An **object class** can also specify the allowable classes for the parent object of an object in the class. An **object class** can be defined by single inheritance; an object whose class is defined in this way is a member of all **object classes** used to derive its most specific class. An **object class** is defined in a classSchema object. See section 1 of [MS-ADTS] and section 1 of [MS-DRSR].

(7) In **COM**, a category of **objects** (3) identified by a **CLSID**, members of which can be obtained through **activation** of the **CLSID**.

(8) In the **DCOM** protocol, a category of **objects** (4) identified by a **CLSID**, members of which can be obtained through **activation** of the **CLSID**. An **object class** is typically associated with a common set of interfaces that are implemented by all **objects** in the **object class**.

object exporter: An object container (for example, process, machine, thread) in an object server. **Object exporters** are callable using RPC interfaces, and they are responsible for dispatching calls to the objects they contain.

object identifier (OID): (1) In the context of an object server, a 64-bit number that uniquely identifies an object.

(2) In the context of a directory service, a number identifying an object class or **attribute** (2). Object identifiers are issued by the ITU and form a hierarchy. An OID is represented as a dotted decimal string (for example, "1.2.3.4"). For more information on OIDs, see [\[X660\]](#) and [\[RFC3280\]](#) Appendix A. OIDs are used to uniquely identify certificate templates available to the **certification authority (CA)** (1). Within a **certificate** (1), OIDs are used to identify standard extensions, as described in [\[RFC3280\]](#) section 4.2.1.x, as well as non-standard extensions.

(3) In the Lightweight Directory Access Protocol (LDAP), a sequence of numbers in a format described by [\[RFC1778\]](#). In many LDAP directory implementations, an OID is the standard internal representation of an attribute. In the directory model used in this specification, the more familiar `ldapDisplayName` represents an attribute.

(4) In the context of **ASN.1**, an object identifier, as described in [\[ITUX680\]](#).

(5) A variable-length identifier from a namespace administered by the ITU. Objects, protocols, and so on that make use of **ASN.1** or Basic Encoding Rules (BER), **Distinguished Encoding Rules (DER)**, or Canonical Encoding Rules (CER) encoding format leverage identities from the ITU. For more information, see [\[ITUX680\]](#).

(6) In the context of a directory service, a number identifying an object class or attribute. Object identifiers are issued by the ITU and form a hierarchy. An OID is represented as a dotted decimal string (for example, "1.2.3.4"). For more information on OIDs, see [\[X660\]](#) and Appendix A of [\[RFC3280\]](#). **OIDs** are used to uniquely identify certificate templates available to the **certificate authority (CA)**. Within a certificate, **OIDs** are used to identify standard extensions as covered in [\[RFC3280\]](#) section 4.2.1.x, as well as non-standard extensions.

(7) In the Lightweight Directory Access Protocol (LDAP), a sequence of numbers in a format specified by [\[RFC1778\]](#). In many LDAP directory implementations, an **OID** is the standard internal representation of an attribute. In the directory model used in [MS-ADTS], the more familiar `ldapDisplayName` represents an attribute.

(8) In the context of **Abstract Syntax Notation One (ASN.1)**, an object identifier, as specified in [\[ITUX680\]](#).

(9) A variable-length identifier from a namespace administered by the ITU. Objects, protocols, and so on that make use of ASN.1 or Basic Encoding Rules (BER), Distinguished Encoding Rules (DER), or Canonical Encoding Rules (CER) encoding format leverage identities from the ITU. For more information, see [\[ITUX680\]](#).

Object Linking and Embedding (OLE): A technology for transferring and sharing information between applications by inserting a file or part of a file into a compound document. The inserted file can be either embedded or linked. See also **embedded object** and **linked object**.

object model: A collection of object-oriented APIs that represent data structures and are designed to promote software interoperability.

object of class x (or x object): An object *o* such that one of the values of its `objectClass` attributes is *x*. For instance, if `objectClass` contains the value `user`, *o* is an object of class `user`. This is often contracted to "user object".

object reference: (1) An attribute value that references an **object**. Reading a reference gives the **distinguished name (DN)** of the **object**.

(2) In the **DCOM** protocol, a reference to an **object** (4), represented on the wire as an **OBJREF**. An **object reference** enables the **object** to be reached by entities outside the **object's object exporter**.

(3) An **attribute** value that references an **object**; reading a reference gives the **distinguished name (DN)** or full **dsname** of the **object**.

OBJREF: The **marshaled** form of an object reference.

OCXDropDown control: A type of DropDown control that displays a list of the ActiveX controls that are available within that application.

ODBC: See **Open Database Connectivity (ODBC)**.

offer: A message that is sent by an offerer.

Office data connection (ODC) file: A file that stores information about a connection to a data source, such as an Access database, worksheet, or text file. This file facilitates data source administration.

Office Web Extension: See **app for Office**.

offline: (1) The condition of not being connected to or not being on a network or the Internet. Offline can also refer to a device, such as a printer that is not connected to a computer, and files that are stored on a computer that is not connected to or not on a network or the Internet.

(2) An operational state applicable to **volumes** and disks. In the offline state, the **volume** or disk is unavailable for data input/output (I/O) or configuration.

OLAP: See **Online Analytical Processing (OLAP)**.

OLAP All level: An optional level at the top of a hierarchy. It typically contains an **OLAP All member** that represents an aggregation of all of the lower-level members of that hierarchy.

OLAP All member: A multidimensional expression (MDX) that evaluates a hierarchy and returns a set that contains all of the members of the specified hierarchy.

OLAP allocation: An operation in which the values for members at lower levels in an **OLAP hierarchy** are changed based on changes to values for members at higher levels in that hierarchy.

OLAP calculated member: An **OLAP member** whose value is calculated at run time.

OLAP cube: A data structure that aggregates **Online Analytical Processing (OLAP)** measures by **OLAP levels** and **OLAP hierarchies**. An OLAP cube combines several OLAP hierarchies, such as time, geography, and product lines, with OLAP measures, such as sales or inventory figures.

OLAP hierarchy: An **attribute hierarchy** or a user-defined hierarchy in a data structure. By default, each dimension **attribute** (1) has an attribute hierarchy. A user-defined hierarchy is a set of related attribute hierarchies that is used to facilitate browsing an **OLAP cube**.

OLAP KPI: See **key performance indicator (KPI)**.

OLAP level: Within an **OLAP hierarchy**, a set of data that is organized into a lower or higher level of detail, such as Year, Quarter, Month, and Day levels in a Time hierarchy.

OLAP measure: A set of numeric values in an **OLAP cube** that is used in aggregation and analysis.

OLAP measure group: A collection of related **OLAP measures** in an **OLAP cube**. An OLAP cube can contain multiple measure groups.

OLAP member: An item that is in an **OLAP level**. For example, a Canada member in a Country level of a Geography hierarchy.

OLAP member property: A relationship between two **OLAP hierarchies**, such as a Population member property of a Country member.

OLAP named set: A collection of **OLAP tuples** that have the same dimensionality. Also referred to as OLAP set.

OLAP subselect: The ability to execute multiple SELECT commands in a FROM clause that is inside a multidimensional expression (MDX) statement.

OLAP tuple: An ordered collection of members that are from different dimensions of an **OLAP cube**. A single member is a special case of a tuple.

OLAP weight expression: A multidimensional expression (MDX) that is used to apply and allocate modified values to an **Online Analytical Processing (OLAP)** provider. It typically returns a decimal value between "0" and "1".

OLE compound file: A form of structured storage, as described in [\[MS-CFB\]](#). A compound file allows independent storages and streams to exist within a single file.

OLE control: A reusable software component that is designed to work in containers that support **Object Linking and Embedding (OLE)** 2.0.

OLE DB: A set of interfaces that are based on the Component Object Model (COM) programming model and expose data from a variety of sources. These interfaces support the amount of Database Management System (DBMS) functionality that is appropriate for a data store and they enable a data store to share data.

OLE link: A connection between an **Object Linking and Embedding (OLE)** object and its OLE server. See also **DDE link**.

OLE object: An object that supports the **Object Linking and Embedding (OLE)** protocol.

OLE server: An application or DLL that supplies a linked or embedded OLE object to another application.

OLE1: See **Object Linking and Embedding (OLE)**.

OLE2: See **Object Linking and Embedding (OLE)**.

OleTx: A comprehensive distributed transaction manager processing protocol that uses the protocols specified in the following document(s): [\[MS-CMPO\]](#), [\[MS-CMP\]](#), [\[MS-DTCLU\]](#), [\[MS-DTCM\]](#), [\[MS-DTCO\]](#), [\[MC-DTCXA\]](#), [\[MS-TIPP\]](#), and [\[MS-CMOM\]](#).

onefiles folder: A folder that stores file data objects for a OneNote revision store file. It is located in the same directory as the revision store file and the folder name maps to the name of the revision store file. For example, if the revision store file is named "section.one" the onefiles folder is named "section_onefiles".

one-variable data table: A data table that consists of only one input cell, which is either a row input cell or a column input cell.

One-Way Method: A **Remote Method** that has no application response sent from the implementation of the **Remote Method** back to the caller. This pattern is sometimes referred to as "fire and forget".

Online Analytical Processing (OLAP): A technology that uses multidimensional structures to provide access to data for analysis. The source data for OLAP is stored in data warehouses in a relational database. See also **cube**.

Open Data Protocol (OData): A web protocol for querying and updating data specified in [\[MS-ODATA\]](#).

Open Database Connectivity (ODBC): A standard software API method for accessing data that is stored in a variety of proprietary personal computer, minicomputer, and mainframe databases. It is an implementation of [\[ISO/IEC9075-3:2008\]](#) and provides extensions to that standard.

Open Item permission: An authorization that enables users to retrieve an entire file.

opnum: An operation number or numeric identifier that is used to identify a specific **remote procedure call (RPC)** method or a method in an interface. For more information, see [\[C706\]](#) section 12.5.2.12 or [\[MS-RPCE\]](#).

optional feature: A non-default behavior that modifies the **Active Directory** state model. An **optional feature** is enabled or disabled in a specific scope, such as a **forest** or a **domain**. For more information, refer to [\[MS-ADTS\]](#) section 3.1.1.9.

orbit: A number that uniquely identifies a parked **call** and enables a **user agent** to retrieve that call. The number is assigned automatically by a **call park service (CPS)** and is sent to the user agent who parked the call.

organization: (1) A security group that contains additional **fields** (1) for describing hierarchical relationships between organizations.

(2) A collection of forests, including the current forest, whose TRUST_ATTRIBUTE_CROSS_ORGANIZATION bit of the Trust attribute ([\[MS-ADTS\]](#) section 6.1.6.7.9) of the trusted domain object (TDO) is not set.

organizational unit: An AD DS container object that is used within domains. An organizational unit is a logical container into which users, groups, computers, and other organizational units are placed. It can contain objects only from its parent domain. An organizational unit is the smallest scope to which a Group Policy object (GPO) can be linked, or over which administrative authority can be delegated.

organizer: The owner or creator of a conference or event.

originating update: An update that is performed to an **NC replica** via any protocol except replication. An **originating update** to an attribute or link value generates a new **stamp** for the attribute or link value.

originating video source (OVS): An entity that locally produces a video stream and sends the video stream to another party or to a **Multipoint Control Unit (MCU)**. For example, a protocol client that is configured with a video camera.

orphaned term: A **term** whose source term was deleted.

outbound: Network traffic flowing from the server to the client.

outbound proxy: (1) A network node that acts as a proxy for outbound traffic between a protocol client and a protocol server.

(2) A network node that acts as an RPC over HTTP proxy for outbound traffic between an RPC client and an RPC server.

outcome: One of the three possible results (Commit, Abort, In Doubt) reachable at the end of a life cycle for an **atomic transaction**.

outline: A nested grouping of rows or **columns** (2) that are in a worksheet.

outline collapse: A process in which rows or **columns** (2) of an **outline** are made invisible.

outline effect: A formatting effect in which a line is placed around the edge of a shape or around each character in a text string.

outline expand: A process in which rows or **columns** (2) of an **outline** are made visible.

outline level: (1) The number of levels that a task is indented from the top level of an outline; the order associated with an outline.

(2) A type of paragraph formatting that can be used to assign a hierarchical level, Level 1 through Level 9, to paragraphs in a document. After outline levels are assigned, an outline of a document can be viewed by using Outline view, the document map, or the navigation pane.

outline state: A setting that specifies whether an outline is currently outline expanded or outline collapsed.

out-of-memory: A state of a computer or application when it halts because all of the available volatile memory has been allocated and none is currently available for reallocation.

OutputFilter: A **FilterDescriptor** type that is used while calling an operation for a line-of-business (LOB) system. Additional results of an operation that cannot be captured by a **ReturnPropertyDescriptor** can be retrieved as a value of an **OutputFilter**.

owner: A **security principal** (2) who has the requisite permission to manage a security group.

18 P

package file: (1) A file that is in a deployment package and is not a manifest file.

(2) A file that contains a collection of tasks that form a workflow that is executed in the order that is defined within the package, with possible conditional branching.

Packed Encoding Rules (PER): A set of encoding rules for **ASN.1** notation, specified in [\[ITUX691\]](#). These rules enable the identification, extraction, and decoding of data structures.

padding: Bytes that are inserted in a data stream to maintain alignment of the protocol requests on natural boundaries.

page: (1) A file that consists of HTML and can include references to graphics, scripts, or dynamic content such as Web Parts.

(2) Represents the layout settings for page-oriented report rendering formats.

page break: (1) The point at which one page ends and another begins, in the context of printing.

(2) A divider that breaks a worksheet into separate pages for printing. Page breaks are inserted automatically based on the paper size, margin settings, scaling options, and the positions of any page breaks that are inserted manually.

Page Break Preview view: A worksheet view that displays the areas to be printed and the locations of page breaks.

page description language (PDL): The language for describing the layout and contents of a printed page. Common examples are PostScript and **Printer Control Language (PCL)**.

page field parameter: A PivotTable page field that is also a **workbook parameter**.

page hop: The process of traversing from one item to another during a crawl. See also **site hop**.

page impression: An identifier for unique **query text**.

page layout: A dynamic web template that is stored as a document. It contains content placeholders that bind to **fields** (3) of a publishing page. A page layout has an associated content type that determines which publishing pages it can be bound to.

Page Layout view: A sheet view that displays a sheet as it would appear on a printed page, including margins, header and footer elements, and pagination.

page margin: The white space at the top, bottom, and sides of a document when a document is printed.

paged view: A view that supports one or more visual pages. A paged view is used to break large sets of data into smaller sets for increased performance and manageability.

PageNumberFilter: A **FilterDescriptor** type that is used when querying a line-of-business (LOB) system. Its value can be the sequence number of the batch to return, if the LOB system can return data in batches.

palette: An array of values, each element of which contains the definition of a color. The color elements in a palette are often indexed so that clients can refer to the colors, each of which can occupy 24 bits or more, by a number that requires less storage space.

pane: A portion of a software window that has a distinct function and is bounded by and separated from other portions of the window by vertical or horizontal bars.

Pane control: A type of toolbar control that hosts a window within itself. The hosted window is not constrained by the layout and control type options of a **basic toolbar** or a **menu toolbar**.

Parameter: A type of **MetadataObject** that represents the formal parameters of a piece of **business logic** (2) in a line-of-business (LOB) system. Parameters have a single root **TypeDescriptor** that defines the structure of the Parameter. They also have a **Direction** and a **TypeReflector**. Parameters are contained by **Methods**.

parameterized query: (1) A query that contains parameters. It applies to Open Database Connectivity (ODBC) and web queries. For example, a web query that retrieves stock quotes from a webpage can prompt users for a parameter, such as a stock symbol.

(2) A query that contains placeholders for values to be bound at query execution.

parent: A data item within the MDS system that can contain childmembers.

parent list: A **list** (1) that contains a list item or list folder.

parent site: The site that is above the current site in the hierarchy of the site collection.

park: A process in which an active **call** is moved to a **parking lot**, without terminating that call. The call can then be retrieved by the same or another **user agent**. See also **call park service (CPS)**.

parkee: A **user agent** whose **call** is parked by another user agent, by using a **call park service (CPS)**. The parkee's call is not terminated and can be retrieved by the user agent who parked the call or a different user agent.

parker: A **user agent** who uses a **call park service (CPS)** to park a **call**. The call can then be retrieved by the same or a different user agent.

parking lot: A collection of one or more orbits that were configured by a **call park service (CPS)**. Each parked **call** is uniquely identified by the **orbit** that is assigned to it.

participant: (1) An **actor** in an **activity flow**. A participant can be either an initiator or a target.

(2) A user who is participating in a **conference** or peer-to-peer **call**, or the object that is used to represent that user.

(3) Any of the parties that are involved in an **atomic transaction** and that have a stake in the operations that are performed under the **transaction** or in the **outcome** of the **transaction** ([\[WSAT10\]](#), [\[WSAT11\]](#)).

(4) A user who is participating in a **conference** or peer-to-peer call. May also be used in reference to the object that is used to represent this participant on the implementation.

(5) A machine that is accessing the desktop content **shared** by the **host**.

partition: (1) An area within a shared services database, such as an area that isolates different tenants within a service, or the process of creating such an area in a shared services database.

(2) A storage block that contains the content in binary files or metadata about file content.

(3) In the context of hard disks, a logical region of a hard disk. A hard disk may be subdivided into one or more **partitions**.

(4) In the context of **directory services**, a synonym for **directory partition** and naming context (NC) replica.

(5) A container for a specific configuration of a COM+ **object class**.

(6) A container for **conglomerations**. Every COMA server has at least one partition--the **Global Partition**--and may have additional partitions. A partition is identified by a **partition identifier**.

(7) One of the storage containers for data and aggregations of a cube. Every cube contains one or more partitions. For a cube with multiple partitions, each partition can be stored separately in a different physical location. Each partition can be based on a different data source. Partitions are not visible to users; the cube appears to be a single object.

partition identifier: A GUID that identifies a **partition** (1).

partner: (1) A computer connected to a local computer through either inbound or outbound connections.

(2) A participant in the MSDTC Connection Manager: OleTx Transports Protocol. Each **partner** has its own **contact identifier (CID)**, and uses the IXnRemote interface to invoke and receive **remote procedure calls (RPCs)**. The IXnRemote interface is described within the full **Interface Definition Language (IDL)** for [MS-CMPO] in section 6.

(3) A computer that is participating in **DFS-R** file replication.

(4) In the context of [MS-PASS], an organization in a business relationship with the **Authentication Service (AS)**. A **partner** needs to be able to access the **token** issued by the **AS**. Typically, a **partner** site is the actual service or site a consumer visits and, in the process, is **authenticated** by the **AS**. Examples of **partners** are the MSN Money and MSN Messenger sites.

P-Asserted-Identity (PAI): A Session Initiation Protocol (SIP) header field, as described in [\[RFC3325\]](#), that is used by trusted entities to carry the identity of the user who is sending an SIP message as it was verified by **authentication** (2).

PasswordCredentialFilter: A **FilterDescriptor** type that is used when querying a line-of-business (LOB) system and can hold the password of an account that is defined in that system. When it is used in conjunction with a UsernameCredentialFilter, an LOB system can use the PasswordCredentialFilter value to restrict access to data for an account.

path: (1) When referring to a file path on a file system, a hierarchical sequence of folders. When referring to a connection to a storage device, a connection through which a machine can communicate with the storage device.

(2) A graphics object that is a container for a series of line and curve segments, and **regions** (2) in an image.

(3) An ordered list of **roles** to follow to reach a specific **entity**.

path component: Data that identifies a resource within the scope of a scheme and authority in a **URI**, as described in [\[RFC3986\]](#).

path segment: A portion of a **URI**, as described in [\[RFC3986\]](#). See also **path component**.

pattern color: The color of the background pattern that is specified for a cell.

pattern fill: A state of a cell in which a background pattern is specified.

pattern mask: Any of the set of patterns that specify a design for the background of a cell.

patterned overlay mask: See **pattern mask**.

peer: (1) An additional **endpoint** (5) that is associated with an endpoint in a session. An example of a peer is the **callee** endpoint for a **caller** endpoint.

(2) The entity being authenticated by the authenticator.

(3) In **DirectPlay**, a player within a DirectPlay game session that has an established connection with every other peer in the game session, and which is not performing game session management duties. The participant that is managing the game session is called the host.

(4) An instance of the Retrieval Protocol for the Peer Content Caching and Retrieval Framework running on a host. A peer can be both a client and a server in the Retrieval Protocol operations.

(5) A node participating in the content caching and retrieval system. A peer is a node that both accesses the content and serves the content it caches for other peers.

(6) The entity on either end of an established SMP session.

(7) A single device or node in a **peer-to-peer** networking system.

(8) When used in context with the IETF standard Layering 2 Tunnel Protocol (L2TP), as specified in [\[MS-L2TP\]](#), peer refers to either the LAC or LNS. LNS is a peer to LAC and vice versa.

(9) When used in context with [\[MS-PTPT\]](#), **peer** refers to either the **PAC** or **PNS**. A PAC's **peer** is a **PNS** and vice versa.

peer name: A string composed of an **authority** and a **classifier**. This is the string used by applications to resolve to a list of **endpoints** and/or an **extended payload**. A **peer name** is not required to be unique. For example, several **nodes** that provide the same service may register the same **Peer Name**.

peer-derived candidate: A **candidate** whose **transport addresses** are new mapping addresses, typically allocated by **NATs**, that are discovered during **connectivity checks**.

peer-derived transport address: A derived transport address that is obtained from a connectivity check that is sent to a peer **endpoint** (5).

peer-to-peer: A server-less networking technology that allows several participating network devices to share resources and communicate directly with each other.

permission: A rule that is associated with an object and that regulates which users can gain access to the object and in what manner. See also **rights**.

permission level: A set of permissions that can be granted to principals or SharePoint groups on an entity such as a site, list, folder, item, or document.

persist: The process of storing data in a memory medium that does not require electricity to maintain the data that it stores. Examples of such mediums are hard disks, CDs, non-volatile RAM, and memory sticks.

personal site: A type of SharePoint site that is used by an individual user for personal productivity. The site appears to the user as My Site.

personal view: A view of a list that is created by a user for personal use. The view is unavailable to other users.

personal Web Part: A **Web Part** that was added to the personal view of a Web Parts Page and is available only to the user who added it.

personalization data: Customized data that is stored for a set of **Web Parts**. The data can be shared by all users or be specific to an individual user.

P-frame: A predicative video frame that references a previous frame. Also referred to as inter-coded frame or inter-frame.

phonetic guide: A set of supplemental phonetic symbols that appears above text in Japanese and other East Asian languages. A phonetic guide is displayed automatically and can be edited by the user.

phonetic information: A series of characters that appear above text in a cell and provide information that helps users pronounce the text.

phonetic string: A series of characters that appear above a string and provide information that helps users pronounce the string. Phonetic strings are typically used in East Asian languages.

phonetic text run: A series of characters that are within a **phonetic string**.

physical left: A leftward position that is not relative to the language orientation of document content. See also **logical left**.

Physical Media: The tangible media that are inserted into and removed from **libraries** and **mounted** in **drives**.

physical right: A rightward position that is not relative to the language orientation of document content. See also **logical right**.

picture library: A type of **document library** that is optimized for storing digital pictures or graphics.

pinned term: A term in a **term set** that cannot be directly moved or deleted.

pipeline: An ordered collection of commands, with the output of one command passed as input to the next.

PivotChart: See **PivotChart report**.

PivotChart filter pane: A user interface element that displays a list of active fields in a PivotChart view and is used to apply filters to those fields.

PivotChart report: A chart that uses a PivotCache for source data and inherits filtering and sorting functionality from a PivotTable report.

PivotTable: An interactive table that summarizes large amounts of data from various sources by using format and calculation methods. Row and column headings can be rotated to view different summaries of the source data, filter the data, or display detail data for specific areas.

PivotTable area: A logical zone that is used to organize data in a PivotTable report.

PivotTable data field: A PivotTable field that is contained in the PivotTable area where data values are shown.

PivotTable field: An element in a PivotTable report that represents a logical collection of data. A PivotTable field can represent a dimension hierarchy or actual data values.

PivotTable field list: A user interface element that displays a list of all of the fields in a PivotTable report. It can be used to populate a PivotTable report and to manipulate the fields.

PivotTable filter parameter: The value that a filter on a PivotTable report is set to, which indicates that matching values are included in the result set.

PivotTable member: An individual data item within a specific dimension as it is displayed in a PivotTable report. For example, a member in the Geography dimension might be North America.

PivotTable page field: A filter in a PivotTable report that applies to all of the data in the report, including any hierarchies.

pixel: A discrete unit of display on a computer display device.

placeholder: A character or symbol that is used in place of an actual value, text, or object. The actual value that the placeholder represents is unknown or unavailable at the current time, or is not displayed for security reasons.

plaintext: In cryptography, ordinary readable text before it is encrypted into **ciphertext**, or after it has been decrypted.

player: A person who is playing a computer game. There may be multiple players on a computer participating in any given game session. See also **name table**.

playlist: One or more **content** items that are **streamed** sequentially.

plot area: A portion of a chart area that contains the plotted data and axes.

pluggable security authentication: The ability to support alternate mechanisms for determining the identity of another entity.

point: A unit of measurement for fonts and spacing. A point is equal to 1/72 of an inch.

policy: (1) A set of rules that governs all interactions with an object such as a document or item.

(2) The set of rules that govern the interaction between a subject and an object or resource.

(3) A collection of settings that contains global settings, profile settings, firewall rules, and connection security rules. Together these settings specify how the host firewall and **Internet Protocol security (IPsec)** behave on the client computer.

(4) The description of actions permitted for a specified set of **content**, and restrictions placed on those actions. Restrictions are described in the license associated with the **content**.

(5) A set of **conditions** and actions. The **conditions** provide a mechanism for classifying DHCP Clients. Classification is based on the **conditions** and **expressions** configured by the user as part of the **policy**. **DHCP Client** requests received by the server are evaluated as per the classification specified in the **policy**. The actions can have an associated IP address range and/or option values. If a **DHCP Client** request matches **policy** conditions, the client is given an IP address from the IP address range of the **policy**. The client will also be given options configured for the matched **policy**. A **policy** can be configured at the **scope** or server level. Multiple policies can be configured at both the **scope** and server levels.

policy application: The protocol exchange by which a client obtains all of the **Group Policy Object (GPO)** and thus all applicable Group Policy settings for a particular policy target from the server, as specified in [\[MS-GPOL\]](#). Policy application can operate in two modes, user policy and computer policy.

polling SUBSCRIBE: A **SUBSCRIBE** request that is used to obtain a one-time snapshot of presence information for a **presentity**. It has a value of "0" (zero) in the Expires header field and does not have any tag in the To header field.

Popup control: A built-in or custom control on a menu bar or toolbar that displays a menu of related commands when clicked.

port: (1) A TCP/IP numbered connection point that is used to transfer data.

(2) A logical name that represents a connection to a **device**. A **port** can represent a network address (for example, a TCP/IP address) or a local connection (for example, a **USB port**).

(3) A subcomponent of the naming **authority** in a **URI scheme** ([\[RFC3986\]](#) section 3.2.3).

(4) The abstraction that transport protocols use to distinguish among multiple destinations within a given host computer. TCP/IP protocols identify ports by using small positive integers. The transport selectors (TSEL) used by the OSI transport layer are equivalent to ports. **RTP** depends upon the lower-layer protocol to provide some mechanism such as ports to multiplex the **RTP** and **RTCP packets** of a session. For more information, see [\[RFC3550\]](#) section 3.

(5) A place to add or remove **physical media** from a **library**.

(6) The logical endpoint of a remote access connection on the client or server.

Portable Network Graphics (PNG): A bitmap graphics file format that uses lossless data compression and supports variable transparency of images (alpha channels) and control of image brightness on different computers (gamma correction). PNG-format files have a .png file name extension.

portal content project: A primary **search catalog** that contains all of the **content sources** and settings for an administrator-defined crawl.

portal site: A type of SharePoint site that can act as an umbrella to other sites and can be used by a large organization.

portal site map provider: A **site map provider** that uses the location of objects, such as pages, in the file system as its source data for constructing a site map.

postback: A process in which a webpage sends data back to the server that hosts the page.

post-query suggestions: An alternative search query that is related to the search query that was executed.

PostScan job: A unit of work within the **scan repository**.

PostScan process: The entity that contains a **scan ticket** used by a **scan device** and the PostScan instructions used by a **scan repository server** when processing image data sent by a **scan device**.

PPTP: Point-to-Point Tunneling Protocol (PPTP) Profile, as defined in [MS-PTPT].

PPTP Access Concentrator (PAC): A node that acts as one side of a PPTP tunnel endpoint and is a **peer** to the **PPTP Network Server (PNS)**. **PAC** refers to the **server** that terminates the PPTP tunnel and provides VPN connectivity to a remote **client**.

PPTP Network Server (PNS): A node that acts as one side of a PPTP tunnel endpoint and is a **peer** to the **PPTP Access Concentrator (PAC)**. **PNS** refers to the remote **client** that requests to establish a VPN connectivity using PPTP tunnel.

precision as displayed: A calculation setting that permanently changes stored values in cells from full precision (15 digits) to the currently displayed format, including the number of decimal places.

preferred approval line: An **approval line** that is associated with a **content type**. Every time the content type is used, the associated approval line is also used.

prefix length: An integer that represents the number of identical bytes at the beginning of the current and previous index key strings. See also **suffix length**.

pre-query suggestions: A search query that is related to the search query that the user is typing.

presence: (1) A status indicator on a client device that is transmitted by using the Wide Area Network Device Presence Protocol (WAN DPP).

(2) A setting for the User field that determines whether instant-messaging status information appears with user names in that field.

presence information: A set of metadata for a client device, including IP address, port, and connection status.

Presence Information Data Format (PIDF): A common data format defined in [RFC3863](#) to exchange presence information.

presence server: A protocol server that uses Wide Area Network Device Presence Protocol (WAN DPP) to communicate presence information for client devices and to process both publish and subscribe messages from client devices.

presentation: (1) A collection of slides that are intended to be viewed by an audience.

(2) A set of audio and video data **streams** and related metadata that are synchronized for playback on a client.

presentation broadcast: A feature that enables users to run a presentation over the web. The presentation is saved in HTML format and can contain audio and video. It can also be recorded and saved for viewing later.

presentation slide: A slide that contains the content that can be displayed during a slide show. A presentation slide can derive formatting and content from a main master slide or a title master slide.

presentity: An entity that provides presence information to a presence service.

primary key: A field or set of fields that uniquely identifies each record in a table. A primary key cannot contain a null value.

primary lookup field: A lookup field that returns all of the information that is needed to support lookup operations from one list to another. See also **dependent lookup field**.

primary pie: The main chart in a bar of pie or pie of pie chart. A primary pie chart has one pie slice (data point) that is a grouping of data points.

primary shortcut key: The default combination of keys that are pressed simultaneously to execute a command. See also **secondary shortcut key**.

principal: (1) An authenticated **entity** that initiates a message or channel in a distributed system.

(2) An **identifier** of such an entity.

(3) In **Kerberos**, a **Kerberos principal**.

(4) An authenticated entity that initiates a message or channel in a distributed system.

(5) An ID of such an entity.

(6) In Kerberos, a Kerberos principal.

(7) A unique entity identifiable by a **security identifier (SID)** that is typically the requester of access to securable **objects** or resources. It often corresponds to a human user but can also be a computer or service. It is sometimes referred to as a **security principal**.

(8) A unique, individual account known to the **KDC**. Often a user, but it can be a **service** offering a resource on the network.

print area: A collection of one or more ranges of cells that are designated to be printed. If a worksheet includes a print area, only the content inside the print area is printed.

print client: The application or user that is trying to apply an operation on the print system either by printing a job or by managing the data structures or devices maintained by the print system.

print job: The rendered **page description language (PDL)** output data sent to a print device for a particular application or user request.

print server: A machine that hosts the print system and all its different components.

print settings: The settings that specify how a file is printed in a specific print job, such as duplex or landscape orientation. Printer settings are settings that can differ from printer to printer but apply to every print job of a given printer. Print settings are values that typically vary between print jobs.

print titles: The rows or **columns** (2) that appear on each page when a page is printed. Print titles are typically used to print column headers above tabular data that spans several printed pages.

print view: A document view that displays a document as it will appear on a printed page.

Printer Control Language (PCL): A **page description language (PDL)** developed by Hewlett Packard for its laser and ink-jet printers.

private branch exchange (PBX): A server-based telephony solution that services a specific organization or office.

private key: One of a pair of keys used in public-key cryptography. The private key is kept secret and is used to decrypt data that has been encrypted with the corresponding public key. For an introduction to this concept, see [\[CRYPTO\]](#) section 1.8 and [\[IEEE1363\]](#) section 3.1.

privilege attribute certificate (PAC): A Microsoft-specific authorization data present in the authorization data field of a ticket. The **PAC** contains several logical components, including group membership data for authorization, alternate credentials for non-Kerberos authentication protocols, and policy control information for supporting interactive logon.

procedural module: A collection of subroutines and functions.

process matching criteria (PMC): A resource policy object that selects a subset of currently executing processes. Since processes are dynamically created and terminated by the operating system in the course of running workloads, the WSRM Protocol uses PMCs as a means of identifying processes for **resource management** purposes. PMCs specify partial or full values to be matched against process property fields. Each PMC includes a name and a nonempty set of matching values and can also include a nonempty set of exclusion values. All running processes under management whose path and the associated user name match the values provided in a PMC are selected by that PMC, provided that they are not already selected by another PMC and do not match the exclusion values. Processes selected by a PMC specification at any given time are said to match, or be in, the PMC. A process can be selected by only one PMC at a time. The term "resource group" and PMC are used interchangeably.

profile page: An **ASP.NET** webpage that includes Web Part controls that display data from a line-of-business (LOB) system. By default, it contains a single **Web Part** that displays the details of a single, primary EntityInstance. If the primary Entity has associated Entities and is the source of an **Association**, the profile page also contains a related Web Part for each associated Entity, and each related Web Part displays EntityInstances that are associated with the primary EntityInstance.

profile site: A page that can display detailed information about a user by using a URL prefix that can be concatenated with a login name, email address, or GUID that identifies the user.

ProgID: An identifier that is used by the Windows registry to uniquely identify an object and is in the form OLEServerName.ObjectName, for example, "Excel.Sheet" or "PowerPoint.Slide."

promotion: A search setting that can be associated with a set of **keywords** and that specifies the same query boost value for all of those keywords.

Property: A typed name/value pair that is associated with a **MetadataObject**. Properties enable consumers of a protocol client to annotate or decorate the MetadataObject with consumer-specific extensions. A MetadataObject can contain multiple Properties.

property bag: (1) A container that stores data but is not defined in the schema for a SharePoint list. Instead of interpreting data in a property bag, the server only passes the data in response to requests. See also **metadict**.

(2) A name/value pair that stores a property of a control or object, typically by using the IPropertyBag interface.

property ID: A 16-bit numeric identifier of a specific **attribute** (1). A property ID does not include any **property type** information.

property identifier: (1) A unique integer or a 16-bit, numeric identifier that is used to identify a specific **attribute** (1) or property.

(2) A numerical value that uniquely identifies a property in a property set.

(3) A DWORD value associated with an **MSMQ object** property that defines the property type and its semantic meaning.

property set: (1) A set of **attributes** (1), identified by a **GUID**. Granting access to a property set grants access to all the attributes in the set.

(2) A set of attributes, identified by a **GUID**. Granting access to a property set grants access to all the attributes in the set.

(3) A set of properties, along with an FMTID, identifying the property set format and an associated class identifier (CLSID). The CLSID is used to identify the application or component that created the property set.

property tag: A 32-bit value that contains a property type and a property ID. The low-order 16 bits represent the property type. The high-order 16 bits represent the property ID.

property type: A 16-bit quantity that specifies the data type of a property value.

protected: A property that is applied manually to a file or a portion of a file, with or without a password, and that helps prevent users from accidentally or deliberately changing, moving, or deleting data.

protected content: (1) Any content or information, such as a file, Internet message, or other object type, to which a rights-management usage policy is assigned and is encrypted according to that policy. See also **Information Rights Management (IRM)**.

(2) **Content** for which usage is governed by policies specified in a license.

(3) Any media content that has a DRM usage policy assigned to it, and is encrypted according to that policy.

(4) Any content or information (file, email) that has an RMS usage policy assigned to it, and is encrypted according to that policy. Also known as "Protected Information".

protection: A mechanism that helps restrict users from making unwanted changes to the data or structure of a workbook.

protocol data units (PDUs): Information that is delivered as a unit among peer entities of a network and that may contain control information, address information, or data. For more information on remote procedure call (RPC)-specific PDUs, see [C706-Ch12RPC_PDU_Encode].

protocol stream: A continuous stream of records flowing in one direction.

provisional answer: An optional message that carries **local candidates** for a **callee** and can be sent by the callee in response to a **caller's** initial offer.

provisioned: A condition of an object that was created and deployed successfully.

proxy: (1) A computer, or the software that runs on it, that acts as a barrier between a network and the Internet by presenting only a single network address to external sites. By acting as a

go-between that represents all internal computers, the proxy helps protect network identities while also providing access to the Internet.

(2) A network node that accepts network traffic originating from one network agent and transmits it to another network agent.

(3) Part of the **Remoting Data Model**. A **Proxy** forwards the invocations of **Remote Methods** from the client to the **Server Object** for execution. The **Proxy** contains the **Request URI** of the **Server Object**. For more information, see [MS-NRTP] section 3.1.1.

(4) Used as described in [RFC2616] section 1.3

(5) An entity that can receive logging messages from both a client and a proxy, or from a server that is streaming on behalf of another server.

PSOM channel: A packet, datagram, octet stream connection, or sequence of logical connections that exists between **endpoints** (5) that are not unique. The channel defines a unique identity for each **endpoint** (5) and helps secure communications between them. It uses a **root distributed object** to enable both logical connections between child **distributed objects** and the exchange of messages between peers. A single PSOM connection can contain multiple PSOM channels.

public address: (1) An IPv4 or IPv6 address that is on the Internet.

(2) An external global address used by a **network address translation (NAT)**.

public IM connectivity: The ability of a protocol server deployment to interoperate with a public instant messaging (IM) provider.

public key: One of a pair of keys used in public-key cryptography. The public key is distributed freely and published as part of a **digital certificate**. For an introduction to this concept, see [CRYPTO] section 1.8 and [IEEE1363] section 3.1.

public key infrastructure (PKI): The laws, policies, standards, and software that regulate or manipulate certificates and public and private keys. In practice, it is a system of **digital certificates**, **certificate authorities (CAs)**, and other registration authorities that verify and authenticate the validity of each party involved in an electronic **transaction** (3). For more information, see [X509] section 6.

public queue: An application-defined **message queue** that is registered in the **MSMQ Directory Service**. A public queue may be deployed at any **queue manager**.

public switched telephone network (PSTN): Public switched telephone network is the voice-oriented public switched telephone network. It is circuit-switched, as opposed to the packet-switched networks.

public view: A view of a list that is available to all users who have permission to access that list.

publish: (1) The process of making an InfoPath form template available for people to fill out by using Microsoft InfoPath or a web browser.

(2) The process of posting **presence** (1) information from a client device to a presence server by using the Wide Area Network Device Presence Protocol (WAN DPP).

(3) A SERVICE request that specifies which **category** (4) instances to publish for a **presentity**.

(4) To register a **Peer Name** by using an encrypted Remote Assistance Connection String that is associated as the payload.

(5) An operation that makes **business rules** available for use within the Master Data Services (MDS) system.

published: A condition of portions of a workbook that are marked as being available to the user when that workbook is processed by a protocol server.

published item: A specific named object that is in a published workbook.

published items snapshot: A snapshot that contains only the published items or published sheets from a workbook. If no published items are defined, a snapshot contains an entire workbook.

published range: A specific type of published item that represents a range of cells.

published sheet: A **sheet** (2) that is published.

published version: The version of a list item that is approved and can be seen by all users. The user interface (UI) version number for a published version is incremented to the next positive major version number and the minor version is "0" (zero). See also **major version** and **minor version**.

publisher: (1) A **SIP protocol client** that is making a publish request.

(2) An application that needs to publish historical data that may be of interest to other applications.

(3) The side of a **Remote Assistance connection** that registers a **Peer Name**. It is the same as the **novice** role.

(4) A set of resources that are contained in the same **workspace**.

(5) In the context of events: The source of event generation. An application or component that writes to one or more **event logs**. An application that publishes events.

publisher-subscriber framework: An application framework that allows applications to expose historical data to other applications that might receive this data.

publishing level: An integer that is assigned to a document to indicate the publishing status of that version of the document.

publishing page: A document that binds to a page layout to generate an HTML page for display to a reader. Publishing pages have specific fields that contain the content that is displayed in an HTML page.

19 Q

QoE Monitoring Agent: A service running on a front-end server that collects and processes **Quality of Experience (QoE)** reports from clients in the form of a **SIP message**, sends a **202 Accepted** or an error response to the client, and sends the QoE metrics to the **QoE Monitoring Server**.

QoE Monitoring Server: A server that collects and processes **Quality of Experience (QoE)** metrics.

Quality of Experience (QoE): A subjective measure of a user's experiences with a media service.

query: (1) A formalized instruction to a data source to either extract data or perform a specified action. A query can be in the form of a query expression, a method-based query, or a combination of the two. The data source can be in different forms, such as a relational database, **XML document**, or in-memory object. See also **search query**.

(2) A context-dependent term commonly overloaded with three meanings, defined as follows: The act of requesting **records** from a set of **records** or the request itself. The particular string defining the criteria for which **records** are to be returned. This string can either be an XPath, as specified in [\[XPath\]](#), (for more information, see [MS-EVEN6] section 2.2.15) or a **structured XML query**, as specified in [\[XML10\]](#), (for more information, see [MS-EVEN6] section 2.2.16).

(3) Contains nonhierarchical data used to identify a resource within the scope of a **URI scheme** and naming **authority**, as defined in [\[RFC3986\]](#) section 3.4.

(4) A dataset query instance.

(5) A semantic query, as defined in [MS-SMDL].

query component: (1) A portion of a **URL** that follows a question mark (?), as described in [\[RFC3986\]](#).

(2) A search component that contains and manages an index partition, which contains all or a subset of the data that is collected by a **crawl component**. A query component can also process requests for that data.

query context: A component of a **promotion** that specifies the contexts in which a promotion is applied. Examples include the site where the query originates and a user's role or location.

query expansion: A process in which one or more tokens are added to a search query. Typically, the additional tokens are selected based on similarity to existing tokens in a search query, such as inflectional forms, synonyms, and phonetic similarity.

query processing: In a search service application, a series of operations, such as applying synonym and stemming expansion rules to the query text, that are performed before a search query is executed against a search index.

query refinement: A process that is used to drill into query results by using aggregated statistical data, such as the distribution of managed property values in query results.

query result: A result that is returned for a query. It contains the title and URL of the item, and can also contain other managed properties and a hit-highlighted summary.

query rule: A setting that consists of a keyword condition and an action performed to provide the most relevant search results.

query server: A server that has been assigned the task of fulfilling search queries.

query table: A two-dimensional table that presents data from an external data source.

query text: The textual, string portion of a query.

queryable expression: A syntax that is used by protocol clients to retrieve a set of **CSOM Objects** that meet a specific set of criteria, based on state data that is stored on a protocol server.

queue: An object that holds **messages** passed between applications or **messages** passed between **Message Queuing** and applications. In general, applications can send **messages** to queues and read **messages** from queues.

queue manager: A message queuing service that manages **queues** deployed on a computer. A queue manager may also provide asynchronous transfer of **messages** to **queues** deployed on other queue managers.

Quick Access Toolbar: A set of controls that represents tasks or commands within an application. By default, it provides access to frequently used commands on the **ribbon**. Users can customize it by adding or removing commands.

quick discovery: The process of discovering **responders** on a network.

Quick Launch: A collection of links to lists and pages in a SharePoint site. By default, it appears on the side of all pages, except site administration pages, in the site.

quick mode (QM): The second phase of an **Internet Key Exchange (IKE)** negotiation, during which the peers negotiate quick mode security associations ([quick mode security association \(QM SA\)](#)). For more information, see [\[RFC2409\]](#) section 5.5.

qWave-WD: The Quality Windows Audio/Video Experience (qWave): Wireless Diagnostics Protocol.

20 R

R1C1: A **reference style** in which each row and each **column** (2) has a numeric heading that is numbered sequentially from top to bottom and left to right, respectively. "R" stands for row and "C" stands for column.

R1C1 notation: A notation that is used to specify a row and **column** (2) of cells in a workbook, as described in [\[ECMA-376\]](#) and [\[ISO/IEC-29500:2008\]](#).

RADIUS client: A client that is responsible for passing user information to designated RADIUS servers, and then acting on the response that is returned.

RADIUS server: A server that is responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user. A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

range: (1) An addressable region that is in a workbook. A range typically consists of zero or more cells and represents a single, contiguous rectangle of cells on a single sheet.

(2) A set of continuous item identifiers to which the same clock vector applies. A range is represented by a starting point, an ending point, and a clock vector that applies to all IDs that are in between.

RangeFilter: A **FilterDescriptor** type that is used when querying a line-of-business (LOB) system. An LOB system can compare its minimum and maximum value with the value of a specific field of the set of EntityInstances and only those EntityInstances where field values that lie between the minimum and maximum are returned.

range-level protection: A mechanism that permits users to change only specific parts of a protected document while restricting access to all other parts of the document. See also **range-level protection bookmark**.

range-level protection bookmark: An entity in a document that is used to denote a range of content that is an exception to a document-level protection setting.

rank: An integer that represents the relevance of a specific item for a search query. It can be a combination of static rank and dynamic rank. See also **static rank** and **dynamic rank**.

ranking: A process in which an integer that represents the relevance of a specific item for a search query is assigned to that item. It can be a combination of **static rank** and **dynamic rank**.

ranking model: In a search query, a set of weights and numerical parameters that are used to compute a ranking score for each item. All items share the same ranking model for a specific set of search results. See also **rank**.

RAW format: A **data type** consisting of **PDL** data that can be sent to a **device** without further processing.

RC4: A variable key-length symmetric encryption algorithm. For more information, see [\[SCHNEIER\]](#) section 17.1.

Reading Layout view: A document view that displays a document as it will appear on a printed page and is optimized for reading a document on a computer screen. Two pages are displayed simultaneously, side-by-side.

reading order: The positioning of characters in words and the positioning of words in sentences. This can be left-to-right or right-to-left.

read-only mode: An **attribute** (1) that indicates that an object cannot be changed or deleted. The object can only be accessed or displayed.

read-only recommended: A file sharing property that displays an alert when a file is being opened. The text of the alert recommends that the user open the file with read-only permission.

Really Simple Syndication (RSS): An XML-based syndication format for content, as described in [\[RSS2.0\]](#).

realm: (1) An administrative boundary that uses one set of authentication servers to manage and deploy a single set of unique identifiers. A realm is a unique logon space.

(2) A collection of key distribution centers (KDCs) with a common set of principals, as described in [\[RFC4120\]](#) section 1.2.

(3) A collection of **users**, **partners**, and **authentication servers** bound by a common **authentication** policy.

real-time data (RTD): Data that is pushed into a worksheet from an **RTD server** and is updated continually. Real-time data is frequently used to track stock prices or inventory levels in real time.

Real-Time Transport Control Protocol (RTCP): A network transport protocol that enables monitoring of Real-Time Transport Protocol (RTP) data delivery and provides minimal control and identification functionality, as described in [\[RFC3550\]](#).

Real-Time Transport Protocol (RTP): A network transport protocol that provides end-to-end transport functions that are suitable for applications that transmit real-time data, such as audio and video, as described in [\[RFC3550\]](#).

recipient: (1) An entity that can receive email messages.

(2) An entity that is in an **address list**, can receive email messages, and contains a set of **attributes** (1). Each attribute has a set of associated values.

(3) The **recipient** of a **fax message**.

record: (1) A group of related **fields** (3), which are sometimes referred to as columns, of information that are treated as a unit. Also referred to as row.

(2) The fundamental unit of information in the .NET Binary Format: XML Data Structure encoded as a variable length series of bytes. [MC-NBFX] section 2 specifies the format for each type of **record**.

(3) A variable-length sequence of bytes with a predefined structure.

(4) A sequence of octets.

(5) The data structure that contains an **event** that is currently represented in an **event log**.

(6) A piece of data that is published by a **node** to the **graph**. **Records** are the primary mechanism of communication in a **graph**.

rectangular gradient: A type of gradient fill in which the color of a cell or other object gradually changes with each successive inner rectangle of pixels.

Recycle Bin: (1) The location where deleted files are stored until they are either restored, if they were deleted erroneously, or destroyed permanently.

(2) An **optional feature** that modifies the state model of object deletions and undeletions, making undeletion of **deleted-objects** possible without loss of the object's attribute values. For more information, see [\[MS-ADTS\]](#) section 3.1.1.9.1.

recycled-object: An **object** that has been deleted, but remains in storage until a configured amount of time (the **tombstone lifetime**) has passed, after which the **object** is permanently removed from storage. Unlike a **deleted-object**, most of the state of the **object** has been removed, and the **object** may no longer be undeleted without loss of information. By keeping the **recycled-object** in existence for the **tombstone lifetime**, the deleted state of the **object** is able to replicate. **Recycled-objects** exist only when the **Recycle Bin optional feature** is enabled.

red-green-blue (RGB): A color model that describes color information in terms of the red (R), green (G), and blue (B) intensities in a color.

red-green-blue-alpha (RGBA): A color model that describes color information in terms of the red (R), green (G), blue (B), and alpha (A) intensities that comprise a color.

reference: (1) A link in a project to another project, a .NET Framework **assembly**, or a compatible Component Object Model (COM) library. Adding a reference to a project enables use of the referenced item in a project, but does not copy it to the current project folder.

(2) A means of accessing a variable, such as an element in an array or a field in a record.

(3) A means by which cells, objects, and chart elements can be referenced in a formula.

reference style: A system that is used in formulas to specify cells or ranges of cells. A reference style specifies a cell in a two-dimensional table by identifying the row and **column** (2) that contain that cell or range of cells.

refinement bin: A set of data that is returned with query results and represents a statistical distribution of those results. The data is based on values of the managed property with which a refiner is associated.

refiner: A configuration that is used for **query refinement** and is associated with one managed property.

reflexive transport address: A **transport address** that is given to a protocol client and identifies the public address of that client as seen by a protocol server. The address is communicated to the protocol client through the XOR MAPPED ADDRESS **attribute** (1) in an allocate response message.

refresh: A process that retrieves values from a data source and populates a workbook with those values.

region: (1) See **disk extent**.

(2) A graphics object that is nonrectilinear in shape and is defined by an array of scanlines.

(3) A geographic location or area information. Region names are stored in a region file.

regional settings: See **locale settings** (1).

REGISTER: A **Session Initiation Protocol (SIP)** method that is used by an SIP client to register the client address with an SIP server.

registry: A local system-defined database in which applications and system components store and retrieve configuration data. It is a hierarchical data store with lightly typed elements that are logically stored in tree format. Applications use the registry API to retrieve, modify, or delete registry data. The data stored in the registry varies according to the version of Windows.

Regular Nomination: The process of selecting a valid **candidate pair** for media flow by validating the candidate pairs with Simple Traversal of UDP through NAT (STUN) binding requests, and then selecting a valid candidate pair by sending STUN binding requests with a flag indicating that the candidate pair was nominated.

relationship lookup field: A **lookup field** in a **back-end database server** that defines a relationship between two SharePoint lists.

relative distinguished name (RDN): (1) An attribute-value pair used in the distinguished name of an object. For more information, see [\[RFC2251\]](#).

(2) In the **Active Directory** directory service, the unique name of a child element relative to its parent in Active Directory. The RDN of a child element combined with the **fully qualified domain name (FQDN)** (2) of the parent forms the FQDN of the child.

(3) The name of an **object** relative to its parent. This is the leftmost attribute-value pair in the **distinguished name (DN)** of an **object**. For example, in the **DN** "cn=Peter Houston, ou=NTDEV, dc=microsoft, dc=com", the **RDN** is "cn=Peter Houston". For more information, see [\[RFC2251\]](#).

(4) In the **Active Directory** directory service, the unique name of a child element relative to its parent in Active Directory. The RDN of a child element combined with the fully qualified distinguished name (FQDN) of the parent forms the FQDN of the child.

(5) As specified in [\[X500\]](#), the portion of a distinguished name that is unique to an organization unit but might not be unique inside a domain.

relative identifier (RID): The last item in the series of **SubAuthority** values in a SID (as specified in [\[SIDD\]](#)). It distinguishes one account or group from all other accounts and groups in the domain. No two accounts or groups in any domain share the same relative identifier.

relative path: (1) A path that is implied by the active working directory or is calculated based on a specified directory. If users enter a command that refers to a file and the full path is not entered, the active working directory is the relative path of the referenced file.

(2) A path that is implied by the current working directory or is calculated based on a specified directory. When a user enters a command that refers to a file, and the full path is not entered, the current working directory becomes the relative path of the referenced file.

(3) A string that specifies a folder path or a web directory (such as "/details") relative to either the current report directory (such as "/salesreports") or the current URL for the **report server** (such as "http://reportserver").

relative reference: A reference to a location on a sheet that is relative to the cell that contains the reference. A relative reference can be stored as a cell reference or as an offset.

relative security descriptor: A security descriptor that contains all associated security information in a contiguous block of memory.

relay server: A server application that provides message transmission services for **Simple Symmetric Transport Protocol (SSTP)** messages.

relay URL: A string of characters that uniquely identifies a relay server and conforms to the syntax of a URI, as described in [\[RFC3986\]](#).

Relayed Candidate: A **candidate** that is allocated on the Traversal Using Relay NAT (TURN) server by sending an Allocate Request to the TURN server.

reliable messaging destination (RMD): An endpoint that receives a message. For more information, see [\[WSRM1-0\]](#), [\[WSRM1-1\]](#), and [\[WSRM1-2\]](#).

reliable messaging source (RMS): An endpoint that sends a message. For more information, see [\[WSRM1-0\]](#), [\[WSRM1-1\]](#), and [\[WSRM1-2\]](#).

relying party (RP): (1) The entity (person or computer) using information from a certificate in order to make a security decision. Typically, the RP is responsible for guarding some resource and applying access control policies based on information learned from a certificate.

(2) A web application or service that consumes **security tokens** issued by an **security token service (STS)**.

Remote Administration Protocol (RAP): A synchronous request/response protocol, used prior to the development of the remote procedure call (RPC) protocol, for marshaling and unmarshaling procedure call input and output arguments into messages and for reliably transporting messages to and from clients and servers.

remote application: An application running on a remote server.

Remote Assistance (RA): A feature of the operating system that allows screen, keyboard, and mouse sharing so that a computer user can be assisted by a remote helper.

Remote Assistance connection: A communication framework that is established between two computers that facilitates **Remote Assistance**.

Remote Authentication Dial-In User Service (RADIUS): A protocol for carrying authentication, authorization, and configuration information between a **network access server (NAS)** that prefers to authenticate connection requests from endpoints and a shared server that performs authentication, authorization, and accounting.

remote candidate: A **candidate** that belongs to a remote **endpoint** (5) in a session.

Remote Desktop Protocol (RDP): A multi-channel protocol that allows a user to connect to a computer running **Microsoft Terminal Services (TS)**. RDP enables the exchange of client and server settings and also enables negotiation of common settings to use for the duration of the connection, so that input, graphics, and other data can be exchanged and processed between client and server.

remote differential compression (RDC): Any of a class of compression algorithms that are designed to compare two files residing on different machines without requiring one of the files to be transmitted in its entirety to the other machine. For more information, see [\[MS-RDC\]](#).

remote endpoint: See **peer**.

Remote Method: Part of the **Remoting Data Model**. A **Remote Method** is a remotely callable operation. A **Remote Method** can either be One-Way or **Two-Way**. In the case of a **One-**

Way Method, there is no reply from the implementation. For more information, see [MS-NRTP] section 3.1.1

remote procedure call (RPC): A context-dependent term commonly overloaded with three meanings. Note that much of the industry literature concerning RPC technologies uses this term interchangeably for any of the three meanings. Following are the three definitions: The runtime environment providing remote procedure call facilities. The preferred usage for this meaning is "RPC runtime". The pattern of request and response message exchange between two parties (typically, a client and a server). The preferred usage for this meaning is "RPC exchange". A single message from an exchange as defined in the previous definition. The preferred usage for this term is "RPC message". For more information, see [\[C706\]](#).

remote user: (1) A user who has a persistent identity within an enterprise and is connected from outside the enterprise network boundary.

(2) An **Address Book object** known to be from a foreign or remote messaging system.

Remoting Data Model: A model that is used to represent higher-layer-defined data structures and values, and to represent a **Remote Method** invocation and the **Return Value** or error information from that invocation. A protocol, such as [\[MS-NRSL\]](#), that is built on top of this protocol can be defined by using the **Remoting Data Model**, and can be agnostic to the **serialization format**. For more information, see Abstract Data Model (section 3.1.1).

Remoting Type: Part of the **Remoting Data Model**. **Class**, **Array**, **Enum**, and Primitive are different kinds of **Remoting Types**. All **Remoting Types** are identified by a name that is case sensitive. For more information, see [MS-NRTP] section 3.1.1

repeating group: A group that can occur more than once in the data source for an InfoPath form. Controls such as repeating sections and repeating tables can be bound to repeating groups. See also **bind**.

replica: (1) A server that hosts an instance of a message item in a folder.

(2) A copy of the data that is in a user's **mailbox** at a specific point in time.

(3) A variable containing a set of objects.

(4) A particular repository of file and directory information to be synchronized, and the metadata store that represents that repository.

(5) **NBNS** database **name records** (name-to-**IPv4** address mapping) replicated from other **NBNS servers**.

(6) A set of data together with associated synchronization metadata.

Replica Tree Root: The folder whose "children" (that is, **files** and folders) are replicated.

replicated update: An update performed to a naming context (NC) replica by the **replication** system, to propagate the effect of an **originating update** at another **NC replica**. The **stamp** assigned during the **originating update** to attribute values or a link value is preserved by **replication**.

replication: (1) The process of propagating the effects of all originating writes to any replica of a **naming context (NC)**, to all replicas of the **NC**. If originating writes cease and replication continues, all replicas converge to a common application-visible state.

(2) An administration scenario in which a **replication client application** automatically copies multiple **conglomerations** from a **replication source** to one or more **replication targets**.

replication client application: A client application that provides automatic copying of **conglomerations** between COMA servers, typically using COMA **export** and **import** functionality.

replication source: A COMA server whose **catalog** contains **conglomerations** to be copied.

replication target: A COMA server whose **catalog** is to contain the copied **conglomerations** after **replication** is performed.

report: (1) A database object that provides a static representation of a set of data and can be used to group, sort, summarize, and aggregate data. The data in a report cannot be edited.

(2) An object that is a combination of three kinds of information: data or other kinds of information about how to obtain the data (queries) as well as the structure of the data; layout or formatting information that describes how the data is presented; and properties of the report, such as author of the report, report parameters, and images included in the report.

report item: An object that exists on a report layout.

report server: A location on the network to which clients can connect by using SOAP over HTTP or SOAP over HTTPS to publish, manage, and execute reports.

report view: An object that is used to display data in a **dashboard**. It can be coordinated with other report views by using filters. Examples of report views include analytic grids and charts, PivotTable reports, strategy maps, trend charts, and webpages.

reporting endpoint: A protocol client that sends **Quality of Experience (QoE)** metrics to a **QoE Monitoring Server**.

Representational State Transfer (REST): (1) A class of **web services** that is used to transfer domain-specific data by using **HTTP**, without additional messaging layers or session tracking, and returns textual data, such as **XML**.

(2) A software architecture implementation for distributed hypermedia systems, such as the World Wide Web.

request: (1) A **SOAP** message with additional constraints as specified in [MS-WSRVCR] section 2.2.1.

(2) A message from a **client** to an OSCP **responder**. The message requests the **revocation** status of an X.509 **certificate** (see [RFC2560]).

(3) An HTTP message sent from the client to the server, as defined in [RFC2616].

request identifier: A **GUID** that is used to identify a specific action or procedure that is sent to a protocol server or a protocol client.

request message: (1) A **Traversal Using Relay NAT (TURN)** message that is sent from a protocol client to a protocol server.

(2) A **SOAP** message with additional constraints as specified in Request Message (section 2.2.1).

Request URI: A **URI** that provides an address of a **Server Object**. The **Request URI** has two major components: a component that is used by the underlying transport to route the

message to an appropriate transport endpoint ([Channel URI](#)); and another component to map the message to a **Server Object** within a server ([Server Object URI](#)).

Request-URI: A **URI** in an **HTTP** request message, as described in [\[RFC2616\]](#).

resource: (1) Any component that a computer can access where data can be read, written, or processed. This resource could be an internal component such as a disk drive, or another computer on a network that is used to access a file.

(2) A logical entity or unit of data whose state changes in accordance with the **outcome** of an **atomic transaction**. **Resources** are either durable or volatile.

(3) Any physical or logical component that can be managed by a **cluster**. A resource is owned by a single **node** at any one time.

(4) An endpoint that represents a distinct type of management operation or value. A client exposes one or more resources and some resources can have more than one instance. For example, the Win32_LogicalDisk class represents a resource and Win32_LogicalDisk="C:\" is a specific instance of the resource.

(5) A network-accessible data object or service that is identified by an **IRI**, as defined in [\[RFC2616\]](#).

(6) An object that a **client** is requesting access to, typically referenced by a Uniform Resource Locator (**URL**) or Uniform Resource Identifier (**URI**), as specified in [\[RFC3986\]](#).

(7) An object created and retained by the composition engine running on the client, on behalf of the server. Resources are referenced in the protocol via handles. Resource handles are scoped to the channel on which they are created. The server may create multiple resources per channel.

(8) An **entity** that can be identified by a URI. This term is used as specified in [\[RFC2616\]](#) section 1.3.

(9) In WS-Transfer, resources are entities that have an XML representation and can be addressed by an **endpoint** reference [\[WXFR\]](#).

resource folder: A folder that contains images, templates, and other resource files for a **content type**.

resource management: A method of allocating the hardware resources of a computer to tasks being performed on that computer. It includes a system of **accounting** for hardware resources by task. The purpose of the WSRM Protocol is to control the resource management of a computer.

resource manager (RM): The participant that is responsible for coordinating the state of a resource with the outcome of atomic transactions. For a specified transaction, a resource manager enlists with exactly one transaction manager to vote on that transaction outcome and to obtain the final outcome. A resource manager is either durable or volatile, depending on its resource.

responder: (1) The computer that responds to request messages.

(2) The party that responds to the first message of an AuthIP exchange.

(3) The party that responds to the first message of an IKE exchange.

(4) An OCSP Extensions server that provides OCSP **responses** (see [\[RFC2560\]](#)).

(5) An LLTD-capable **station** to which **mappers** and **enumerators** send LLTD commands.

response: (1) A **SOAP** message with additional constraints as specified in [MS-WSRVCR] section 2.2.2.

(2) A message from an OSCP **responder**. The message specifies the status of an X.509 **certificate** (see [RFC2560]).

(3) An HTTP message sent from the server to the client, as defined in [RFC2616].

(4) A typed buffer of data sent by the client to the server in response to a **notification**.

response message: (1) A Traversal Using Relay NAT (TURN) message that is sent from a protocol server to a protocol client in response to a request message. It is sent when the request message is handled successfully by the protocol server.

(2) A **SOAP** message with additional constraints as specified in Response Message (section 2.2.2).

restriction: (1) A set of conditions that an item meets to be included in the search results that are returned by a query server in response to a search query.

(2) A filter used to map some domain into a subset of itself, by passing only those items from the domain that match the filter. Restrictions can be used to filter existing **Table objects** or to define new ones, such as **search folder** (2) or rule criteria.

(3) A set of conditions that a file must meet to be included in the search results returned by the Generic Search Service (GSS) in response to a search query. A restriction narrows the focus of a search query, limiting the files that the Generic Search Service (GSS) will include in the search results only to those files matching the conditions.

(4) A set of conditions that a file must meet to be included in the search results returned by the indexing service in response to a search query. A restriction narrows the focus of a search query, limiting the files that the indexing service includes in the search results only to those files matching the conditions.

result provider: A component or application that serves a query to a **search provider** and translates the resulting data into a result set.

result set: (1) A list of records that results from running a stored procedure or query, or applying a filter. The structure and content of the data in a result set varies according to the implementation.

(2) A set of data streams that represents the result of a query.

(3) A set of **records** that are selected by a **query**.

result source: A local or remote **search catalog**, a remote Exchange search endpoint or an OpenSearch1.0/1.1-compliant search engine that may include a list of attributes that defines a set of search results for a search query.

retention action: An action that occurs on an object, such as a document or site, in response to an event defined by a retention formula in a larger retention policy. Examples of retention actions are delete, move to a different location, and delete previous versions.

retention formula: A logical equation or function that is used to calculate when a **retention action** occurs on an object, such as a document or content type, as defined by a larger retention policy that applies to that object.

return code: A code that is used to report the outcome of a procedure or to influence subsequent events when a routine or process terminates (returns) and passes control of the system to another routine. For example, a return code can indicate whether an operation was successful.

Return Value: A **Data Value** that is returned as part of the results of a **Remote Method** invocation. For more information, see **Remote Method** in Abstract Data Model (section 3.1.1).

ReturnTypeDescriptor: An **attribute** (1) of a **MethodInstance**. It is the TypeDescriptor that identifies the portion of a Method's return or output Parameters to extract and return as the result of executing the MethodInstance. It defines the View of the EntityInstances returned, with its child TypeDescriptors denoting the Fields of the View.

revision: (1) A change in a document, file, or other object.

(2) A specific version of an **update** that is identified by a combination of an UpdateID **GUID** and a 32-bit revision number.

revision history: A list of data that describes document updates, such as when and by whom a document was modified.

revision record: Any of the records in the revision stream of a **shared workbook** that stores user edits to the workbook and other tracked information.

revocation: The process of invalidating a certificate. For more details, see [\[RFC3280\]](#) section 3.3.

ribbon: A set of controls that represents tasks or commands within an application. The tasks and commands are organized into tabs. The ribbon appears at the top of an application window and is part of the Microsoft Office Fluent user interface, which replaces the previous system of layered menus, toolbars, and task panes.

rich text: Text that is formatted in the Rich Text Format, as described in [\[MSFT-RTF\]](#).

rights: Tasks that a user is permitted to perform on a computer, site, domain, or other system resource. See also **permission**.

right-to-left: A reading and display order that is optimized for right-to-left languages.

Rivest-Shamir-Adleman (RSA): A system for public key cryptography. **RSA** is specified in [\[PKCS1\]](#) and [\[RFC3447\]](#).

RMD: See **reliable messaging destination (RMD)**.

RMS: See **reliable messaging source (RMS)**.

role: (1) A symbolic name that defines a class of users for a set of components. A role defines which users can call interfaces on a component.

(2) The domain role quantifies the relationship between a computer and a domain. Domain roles include the following: Joined: Linked to a domain for purposes of policy and security. Standalone: Not associated with any domain. Domain controller: Linked to a domain, and hosting that domain.

(3) A set of **role members** that represents authorization for a set of operations that is supported by a **conglomeration**. A role is identified by a **role name**.

(4) An association between a pair of **entities**. One entity is the source or origin of the role and the other entity is the target or destination of the role. The role specifically describes how the target entity is related to the source entity. For each role there is a naturally occurring corresponding role called the related role, where the source entity of the related role is the target entity of the role and the target entity of the related role is the source entity of the role. The association repeats for each subsequent pair of entities, so that the target of one role becomes the source of the next role. In this way, entities in an information model may be associated through chains of roles that extend from one entity to the next throughout the information model.

role assignment: An association between a principal or a site group and a role definition.

role definition: A named set of permissions for a SharePoint site. See also **permission level**.

role identifier: An integer that uniquely identifies a role definition within a SharePoint site.

role member: A predicate indicating that a particular user account belongs to a **role**.

role name: A string that identifies a **role** within a **conglomeration**.

rollup: A type of calculated value that is derived from the aggregated scores of child or descendant key performance indicators (KPIs) in a **scorecard**.

root certificate: A self-signed **certificate** (1) that identifies the **public key** of a root **certification authority (CA)** (1) and has been trusted to terminate a **certificate chain**.

root distributed object: The top-level **distributed object** to which a protocol client or protocol **server** (2) connects immediately after a channel is created. After a connection is established with a root distributed object, all other distributed objects on the same channel are connected.

root element: The top-level element in an **XML document**. It contains all other elements and is not contained by any other element, as described in [\[XML\]](#).

root folder: The folder at the top of a hierarchy of folders in a list.

root TypeDescriptor: A **TypeDescriptor** that is contained by a Parameter and has no parent TypeDescriptor. A Parameter can contain only one root TypeDescriptor.

routing link cost: A value that models the relative cost of direct communication between two **MSMQ sites**.

routing slip: Information that specifies how a document is to be distributed from a document originator and processed by one or more recipients. It also specifies subject and message body text that is associated with the document routing process and routing status or workflow information.

routing table: (1) A table that consists of destinations, routes, and **next hops**. These entries define a route to a **destination** network.

(2) A table maintained by each **MSMQ site gate** for inter-site routing. For each **MSMQ site** in an **enterprise**, the table specifies the **MSMQ site** to which a **message** should be forwarded in order to minimize the total **routing link cost** for that **message**.

row: (1) A collection of **columns** (1) that contains property values that describe a single item in a set of items that match the **restriction** (1) specified in a query.

(2) A single set of data that is displayed horizontally in a worksheet or a table.

(3) The collection of columns containing the property values that describe a single result from the set of objects that matched the restrictions specified in the search query submitted to the Generic Search Service (GSS).

(4) The collection of columns that contains the property values that describe a single file from the set of files that matched the restriction specified in the search query submitted to the indexing service

row banding: A table formatting option that applies **background colors** to alternating rows to increase legibility.

row field: A PivotTable field that is contained in the PivotTable area where row values are shown.

RPC transport: The underlying network services used by the remote procedure call (RPC) runtime for communications between network nodes. For more information, see [\[C706\]](#) section 2.

RSA: RSA Data Security, Inc., a major developer and publisher of **public key** cryptography standards (PKCS).

RSS channel: An RSS channel, as described in [\[RSS2.0\]](#).

RSS item: An item element in an RSS feed, as described in [\[RSS2.0\]](#).

RTCP packet: A control packet consisting of a fixed header part similar to that of **RTP packets**, followed by structured elements that vary depending upon the RTCP packet type. Typically, multiple RTCP packets are sent together as a compound RTCP packet in a single packet of the underlying protocol; this is enabled by the length field in the fixed header of each RTCP packet. See [\[RFC3550\]](#) section 3.

RTD server: A Component Object Model (COM) **Automation server** that is used by the real-time data (RTD) function to retrieve data in real time. The RTD server can exist as an ActiveX DLL or as an executable (.exe) file that runs on the same local computer or on a remote server.

RTP packet: A data packet consisting of the fixed RTP header, a possibly empty list of contributing sources, and the payload data. Some underlying protocols may require an encapsulation of the RTP packet to be defined. Typically one packet of the underlying protocol contains a single RTP packet, but several RTP packets can be contained if permitted by the encapsulation method. See [\[RFC3550\]](#) section 3.

RTP payload: The data transported by **RTP** in a packet, for example audio samples or compressed video data. For more information, see [\[RFC3550\]](#) section 3.

RTP profile: A collection that contains payload type codes and mappings to payload formats, such as media encodings. It can also define extensions or modifications to the **Real-Time Transport Protocol (RTP)** that are specific to a particular class of applications. Typically, an application operates under only one profile.

RTP session: An association among a set of **participants** (2) who are communicating by using the **Real-Time Transport Protocol (RTP)**, as described in [\[RFC3550\]](#). Each RTP session maintains a full, separate space of **Synchronization Source (SSRC)** identifiers.

RTVC1: A Microsoft proprietary implementation of the VC1 codec for real-time transmission purposes, as described in [\[SMPTE-VC-1\]](#). Microsoft extensions to VC1 are based on **cached frame** and **SP-frame**, as described in [\[MS-RTVPF\]](#).

RTVideo: A video **stream** (2) that carries an **RTVC1** bit stream.

RTVideo frame: A video frame that is encoded by using an **RTVC1** codec.

Ruby: A text layout setting that displays annotative characters above or to the right of the text to which it applies. It is typically used in East Asian documents to indicate pronunciation or to provide a brief annotation.

rule: (1) A condition or action, or a set of conditions or actions, that performs tasks automatically based on events and values.

(2) A set of qualifiers, such as enumeration values, and quantifiers, such as numeric arguments, that are specified as usage guidelines for a set of objects or data.

(3) A mapping of a file type to a location in a document repository.

(4) An item that defines a **condition** and an action. The condition is evaluated for each **Message object** as it is delivered, and the action is executed if the new Message object matches the condition.

ruler: A user interface element that enables users to adjust page margins and to measure and align objects in a document.

rules extension: A .NET assembly that is located on the server in the synchronization engine's "extensions" folder and implements the IMASynchronization interface.

run length encoding: A lossless compression method that replaces a contiguous series (run) of identical values in a data stream with a pair of values that represent the length of the series and the value itself. For example, a data stream that contains 57 consecutive entries with the value "10" could replace them all with the shorter pair of values "57", "10".

runspace: An entity capable of running one (and only one) **pipeline** of **commands**.

21 S

safe load: A process of loading a file in which additional error checking is performed and various corruption patterns in the file are detected and repaired.

salt: An additional random quantity, specified as input to an encryption function that is used to increase the strength of the encryption.

sample: (1) A unit of **media data** sent from the server to the client.

(2) The smallest fundamental unit (such as a frame) in which **media** is stored and processed.

sandboxed solution: A custom solution that can be deployed to a site by a site collection administrator, without approval from the server farm administrator.

SASL: The Simple Authentication and Security Layer, as described in [\[RFC2222\]](#). This is an **authentication** (2) mechanism used by the **Lightweight Directory Access Protocol (LDAP)**.

Scalar: A type of **MethodInstance** that can be called to return a scalar value.

Scale Secure Real-Time Transport Protocol (SSRTP): A Microsoft proprietary extension to the **Secure Real-Time Transport Protocol (SRTP)**, as described in [\[RFC3711\]](#).

scan device: A scanner, copier, or multifunction peripheral that supports the Devices Profile for Web Services [\[DPWS\]](#).

scan document: A single image file created by a **scan device** and transferred to the **scan repository server** during the processing of a **PostScan job**.

scan repository: A service that supports processing **PostScan jobs** based on data and instructions in a **PostScan process**.

scan ticket: An element that communicates the appropriate settings that should be used by a **scan device** when creating a **scan document**.

scatter chart: A chart that displays values on both the x and y axes to represent two variables as a single data point.

scenario: A named set of input values (changing cells) that can be substituted in a worksheet model.

Scenario Manager: A process for creating and managing different sets of input values for calculation models in a worksheet.

scene: An independent part of a **tour** that has a beginning and end, and a specific time duration in which a particular data visualization on the map occurs.

Schedule: The frequency at which **FRS** replicates data under **replica tree root**.

schema: (1) The set of **attributes** and **object classes** that govern the creation and update of **objects**.

(2) A container that defines a **namespace** that describes the scope of EDM types. All EDM types are contained within some **namespace**.

schema naming context (schema NC): A specific type of **naming context (NC)** or an instance of that type. A **forest** has a single **schema NC**, which is replicated to each **domain**

controller (DC) in the **forest**. No other **NC replicas** can contain these **objects**. Each **attribute** and class in the **forest's** schema is represented as a corresponding **object** in the **forest's schema NC**.

schema object: An object that defines an **attribute** (1) or an object class. Schema objects are contained in the schema naming context (schema NC).

schema version: An integer value that represents the version number of the schema for a deployment package.

scheme: The name of a specification to refer to when assigning identifiers within a particular **URI scheme**, as defined in [\[RFC3986\]](#) section 3.1.

scope: (1) A range of IP addresses and associated configuration options that are allocated to **DHCP clients** in a specific subnet.

(2) The term "Scope" that is defined in [\[WS-Discovery1.1\]](#).

(3) An item that represents a hierarchy in a **report**. There are explicit scopes (such as **data region**, **dataset**, group) and implicit scopes (such as report scope). At any level in the hierarchy, there can be only one ancestor scope (except for the top-level report scope and the **page** scope) but an unlimited number of descendants as well as peer scopes.

scope identifier: A GUID that uniquely identifies a scope within a site collection.

scope index key: A **basic scope index key** or a compound scope index key that references a scope index record.

scorecard: A report that depicts organizational and business performance by displaying a collection of **key performance indicators (KPIs)** with performance targets for those KPIs. Each KPI compares actual performance to goals for an area. A scorecard can be organized hierarchically and typically contains visualization tools such as trend charts and conditional formatting.

SDP answer: A **Session Description Protocol (SDP)** message that is sent by an answerer in response to an offer that is received from an offerer.

SDP offer: A **Session Description Protocol (SDP)** message that is sent by an offerer.

sealed content type: A named and uniquely identifiable collection of settings and fields that cannot be changed. A seal can be removed only by a site collection administrator. See also **content type**.

search alert: An **Internet message** that is sent to subscribers automatically for a specific query. It notifies subscribers when one or more new results exist, or an existing result was modified.

search application: A unique group of search settings that is associated, one-to-one, with a shared service provider.

search catalog: All of the crawl data that is associated with a specific search application. A search catalog provides information that is used to generate query results.

search down: A process of searching for information by ascending row and column numbers.

search folder: (1) A collection of related items to be crawled by a search service.

(2) A **Folder object** that provides a means of querying for items that match certain criteria. The search folder includes the **search folder definition message** and the **search folder container**.

search folder container: A **Folder object** that is created according to the specifications in the definition message. It is in the Finder folder of the message database.

search folder definition message: A **folder associated information (FAI)** message that persists all the information that defines a search folder. It is in the associated contents table of the **Common Views folder** in the message database.

search index: A set of data structures that facilitates query evaluation by a search service application. The primary part of a search index is an **inverted index** of terms.

search provider: A component or application that provides data in response to a query. See also **result provider**.

search query: A complete set of conditions that are used to generate search results, including query text, sort order, and ranking parameters.

search scope: A list of attributes that define a collection of items.

search scope compilation: The process of updating a **full-text index catalog** to reflect unincorporated changes to the definitions of search scopes.

search scope consumer: A site collection that uses a specific search scope display group.

search scope rule: An attribute that specifies which items are included in a search scope.

search security descriptor: (1) A Windows security descriptor.

(2) A custom security descriptor that is in an arbitrary format and is handled by alternate authentication providers in pluggable security **authentication** (2).

search service account: A user account under which a search service runs.

search service application: A shared service application that provides indexing and querying capabilities.

search setting context: An administrative setting that is used to specify when a search setting for a keyword is applied to a search query, based on the query context.

search up: A process of searching for information by descending row and column numbers.

secondary bar/pie: A secondary chart in a bar or pie or pie of pie chart that displays the detailed data of the grouped data point in the primary pie chart. The secondary bar/pie chart takes the form of a stacked bar chart or a pie chart that is connected to the primary pie chart with series lines.

secondary data connection: Any auxiliary connection between an InfoPath form and a data source that stores or provides data for the form.

secondary data source: An **XML** data file, a database, or a **web service** that is used to populate controls or provide values in an InfoPath form.

secondary shortcut key: A user-defined combination of keys that are pressed simultaneously to execute a command. See also **primary shortcut key**.

secret key: A symmetric encryption key shared by two entities, such as between a user and the **domain controller (DC)**, with a long lifetime. A password is a common example of a secret key. When used in a context that implies **Kerberos** only, a principal's secret key.

section: (1) A collection of user profile properties that appear together on a profile site.

(2) A portion of a document that is terminated by a section break or the end of the document. A section can store unique, page-level formatting, such as page size and orientation, and other formatting features such as headers and footers.

(3) A part of a form or report, such as a header or footer, that appears at each instance of a specific level in that form or report. It can be shown or hidden independently of other sections.

(4) Specifies the layout and structure information of a **report**. A report section is comprised of a body, a header, and a footer. A section is specified by the Section element.

securable object: An object that can have unique security permissions associated with it.

secure audio video profile (SAVP): A protocol that extends the audio-video profile specification to include the Secure Real-Time Transport Protocol, as described in [\[RFC3711\]](#).

Secure Real-Time Transport Protocol (SRTP): A profile of **Real-Time Transport Protocol (RTP)** that provides encryption, message **authentication** (2), and replay protection to the RTP data, as described in [\[RFC3711\]](#).

Secure Sockets Layer (SSL): A security protocol that supports confidentiality and integrity of messages in client and server applications that communicate over open networks. SSL uses two keys to encrypt data—a **public key** known to everyone and a private or **secret key** known only to the recipient of the message. SSL supports server and, optionally, client **authentication** (2) using **X.509 certificates** (2). For more information, see [\[X509\]](#). The SSL protocol is precursor to **Transport Layer Security (TLS)**. The TLS version 1.0 specification is based on SSL version 3.0.

Secure Store Service (SSS): A service that is used to store credentials for a user or a group of users. It enables applications, typically on behalf of a user, to authenticate and gain access to resources. Users can retrieve only their own credentials from the secure store.

Secure Store Service (SSS) store: A persistent store that provides storage for **target application** definitions and credentials.

Secure Store Service (SSS) ticket: A token that contains the encrypted identity of a Secure Store Service (SSS) user in the form of a **claim** (2) and a nonce.

Secure Store Service (SSS) user: A **security principal** (2) that interacts with a Secure Store Service (SSS) implementation.

Security Account Manager (SAM): A centrally managed service, such as AD DS, that enables a server to establish a trust relationship with other authorized servers. The SAM also maintains information about domains and **security principals** (2), and provides client-to-server information by using several available standards for access control lists (ACLs).

Security Assertion Markup Language (SAML): The set of specifications that describe security assertions encoded in **XML**, profiles for attaching assertions to protocols and frameworks, request/response protocols used to obtain assertions, and the protocol bindings to transfer protocols, such as **SOAP** and HTTP.

security association (SA): A simplex "connection" that provides security services to the traffic carried by it. See [\[RFC4301\]](#) for more information.

security context: (1) An abstract data structure that contains authorization information for a particular **security principal** in the form of a Token/Authorization Context (see [\[MS-DTYP\]](#) section 2.5.2). A server uses the authorization information in a **security context** to check access to requested resources. A **security context** also contains a **key** identifier that associates mutually established cryptographic **keys**, along with other information needed to perform secure communication with another security principal.

(2) The result of a TSIG [\[RFC2845\]](#) security negotiation between the server and a client machine.

(3) A data structure containing **authorization** information for a particular **security principal** in the form of a collection of **security identifiers (SIDs)**. One **SID** identifies the **principal** specifically, whereas others may represent other capabilities. A server uses the **authorization** information in a **security context** to check access to requested resources.

security descriptor: A data structure containing the security information associated with a securable **object**. A **security descriptor** identifies an **object's** owner by its **security identifier (SID)**. If access control is configured for the **object**, its **security descriptor** contains a **discretionary access control list (DACL)** with **SIDs** for the **security principals** who are allowed or denied access. Applications use this structure to set and query an **object's** security status. The **security descriptor** is used to guard access to an **object** as well as to control which type of auditing takes place when the **object** is accessed. The **security descriptor** format is specified in [\[MS-DTYP\]](#) section 2.4.6; a string representation of **security descriptors**, called SDDL, is specified in [\[MS-DTYP\]](#) section 2.5.1.

security group: A named group of principals on a SharePoint site.

security group identifier: An integer that is used to uniquely identify a security group, distinguishing it from all other **security principals** (2) and site groups within the same site collection.

security identifier (SID): An identifier for **security principals** in Windows that is used to identify an account or a group. Conceptually, the **SID** is composed of an account authority portion (typically a **domain**) and a smaller integer representing an identity relative to the account authority, termed the **relative identifier (RID)**. The **SID** format is specified in [\[MS-DTYP\]](#) section 2.4.2; a string representation of **SIDs** is specified in [\[MS-DTYP\]](#) section 2.4.2 and [\[MS-AZOD\]](#) section 1.1.1.2.

security policy: In the form of a collection of security policy settings, the policy itself is an expression of administrative intent regarding how computers and resources on their network should be secured.

security principal: (1) A unique entity that is identifiable through cryptographic means by at least one key. It frequently corresponds to a human user, but also can be a service that offers a resource to other security principals. Also referred to as principal.

(2) An identity that can be used to regulate access to resources. A security principal can be a user, a computer, or a group that represents a set of users.

(3) A unique entity identifiable through cryptographic means by at least one **key**. A **security principal** often corresponds to a human user but can also be a service offering a resource to other **security principals**. Sometimes referred to simply as a "principal".

(4) An identity that can be used to regulate access to resources, as specified in [MS-AUTHSOD] section 1.1.1.1. A **security principal** can be a user, a computer, or a group that represents a set of users.

(5) A unique entity, also referred to as a principal, that can be authenticated by **Active Directory**. It frequently corresponds to a human user, but also can be a service that offers a resource to other security principals. Other security principals might be a group, which is a set of principals. Groups are supported by **Active Directory**.

(6) An entity that is associated with a human user or a program that can be authenticated. At a minimum, it has two basic attributes, a name and an identifier, that uniquely identifies it and makes it meaningful to the system, administrators, and users. A security principal is also known as a principal or an account.

security principal identifier: A value that is used to uniquely identify a **security principal** (2). In Windows-based systems, it is a **security identifier (SID)**. In other types of systems, it can be a user identifier or other type of information that is associated with a **security principal** (2).

security principal name (SPN): The name that identifies a security principal (for example, machinename\$@domainname for a machine joined to a domain or username@domainname for a user). Domainname is resolved using the **Domain Name System (DNS)**.

security principal object: An **object** that corresponds to a **security principal**. A **security principal object** contains an identifier, used by the system and applications to name the principal, and a secret that is shared only by the principal. In **Active Directory**, a **security principal object** has the objectSid **attribute**. In **Active Directory**, the user, computer, and group **object classes** are examples of **security principal object classes** (though not every **group object** is a **security principal object**). In **AD LDS**, any **object** containing the msDS-BindableObject **auxiliary class** is a **security principal**. See also **computer object**, **group object**, and **user object**.

security protocol: A protocol that performs **authentication** and possibly additional security services on a network.

security provider: (1) A Component Object Model (COM) object that provides methods that return custom information about the security of a site.

(2) A pluggable security module that is specified by the protocol layer above the **remote procedure call (RPC)** layer, and will cause the RPC layer to use this module to secure messages in a communication session with the server. The security provider is sometimes referred to as an authentication service.

(3) A pluggable security module that is specified by the protocol layer above **remote procedure call (RPC)**, and will cause **RPC** to use this module to secure messages in a communication session with the server. Sometimes referred to as an **authentication** service. For more information, see [\[C706\]](#) and [\[MS-RPCE\]](#).

security realm or security domain: Represents a single unit of security administration or **trust** (for example, a Kerberos realm, for more information, see [\[RFC4120\]](#); or a Windows Domain, for more information, see [\[MSFT-ADC\]](#)).

security role: A defined set of access privileges. The security role that is assigned to a user determines the tasks that a user can perform and which parts of the user interface a user can view.

security scope: A tree structure of objects in which every object has the same security settings as the root.

security support provider (SSP): A dynamic-link library (DLL) that implements the **Security Support Provider Interface (SSPI)** by making one or more security packages available to applications. Each security package provides mappings between an application's **SSPI** function calls and an actual security model's functions. Security packages support **security protocols** such as **Kerberos** authentication and NTLM.

Security Support Provider Interface (SSPI): A Windows-specific API implementation that provides the means for connected applications to call one of several security providers to establish authenticated connections and to exchange data securely over those connections. This is the Windows equivalent of Generic Security Services (GSS)-API, and the two families of APIs are on-the-wire compatible.

security token: (1) An opaque message or data packet produced by a **Generic Security Services (GSS)**-style **authentication** package and carried by the application protocol. The application has no visibility into the contents of the **token**.

(2) A collection of one or more **claims**. Specifically in the case of mobile devices, a **security token** represents a previously authenticated user as defined in the Mobile Device Enrollment Protocol [\[MS-MDE\]](#).

security token service (STS): (1) A web service that issues **claims** (2) and packages them in encrypted security tokens.

(2) A web service that issues **security tokens**. That is, it makes assertions based on evidence that it **trusts**; these assertions are for consumption by whoever trusts it. For more information, see [\[WSFedPRP\]](#) sections 1.4 and 2 and [\[WSTrust\]](#) section 2.4. For [\[MS-ADFSP\]](#), [\[MS-ADFSWAP\]](#), and [\[MS-MWBF\]](#), **STS** refers to services that support (either directly or via a front end) the protocol defined in each of those specifications.

(3) To communicate trust, a service requires proof, such as a **signature** to prove knowledge of a **security token** or set of **security tokens**. A service itself can generate tokens or it can rely on a separate **STS** to issue a **security token** with its own trust statement. (Note that for some **security token** formats, this can be just a re-issuance or co-**signature**.) This forms the basis of trust brokering.

(4) A special type of server defined in WS-Trust [\[WSTrust1.3\]](#).

security trimmer: A filter that is used to limit search results to only those resources that a user can view, based on the user's permission level and the access control list (ACL) for a resource. A security trimmer helps to ensure that search results display only those resources that a user has permission to view.

security zone: A setting that determines whether a resource, such as a website, can access data on other domains, or access files and settings on a user's computer. There are four security zones: Internet, Local intranet, Trusted sites, and Restricted sites. The zone to which a resource is assigned specifies the security settings that are used for that resource. See also **form security level**.

security-enabled group: A **group object** with GROUP_TYPE_SECURITY_ENABLED present in its groupType **attribute**. Only **security-enabled groups** are added to a **security context**. See also **group object**.

segment: (1) A subdivision of content. In version 1.0 Content Information, each segment has a size of 32 megabytes, except the last segment which can be smaller if the content size is not a

multiple of the standard segment sizes. In version 2.0 Content Information, segments can vary in size.

(2) A set of stations that see each other's link-layer frames without being changed by any device in the middle, such as a switch.

(3) A unit of content for discovery purposes. A segment is identified on the network by its public identifier, also known as segment ID or HoHoDk. A segment does not belong to any particular content; it can be shared by many content items if all those content items have an identical segment-sized portion at some offset.

selected: The condition of a set of items that has focus in a workbook.

selection: An item or set of items, such as cells, shapes, objects, and chart elements, that has focus in a document.

self SUBSCRIBE: A **SUBSCRIBE** request that is used by a **publisher** to be notified of changes to its own data. It is possible to subscribe to three different sets of data: **categories** (4), **containers**, and **subscribers**.

self subscriber: A **SIP protocol client** that is making a subscribe request for self-published **category** (4) information.

self-signed certificate: A **certificate** (1) that is signed by its creator and verified using the **public key** contained in it. Such certificates are also termed **root certificates**.

sequence: (1) A unique identifier for a delta that includes the user identifier for the **endpoint** (3) that created the delta.

(2) The set of message packets sent over a session that represent a message **sequence**. A message is associated with a **sequence** number that corresponds to its position within the **sequence**. **Sequence** numbers begin with 1 and increment by 1 with each subsequent message.

(3) A one-way, uniquely identifiable batch of messages between an **RMS** and an **RMD**.

sequence header: A set of encoding and display parameters that are placed before a group of pictures, as described in [\[SMPTE-VC-1\]](#). See also **entry point header**.

Serialization Format: The structure of the serialized message content, which can be either binary or **SOAP**. Binary serialization format is specified in [\[MS-NRBF\]](#). SOAP serialization format is specified in [\[MS-NRTP\]](#).

series line: A supplemental line on a stacked column, stacked bar, pie of pie, or bar of pie chart that connects each data point in a series with the next data point to increase legibility.

server: (1) A computer on which the **remote procedure call (RPC)** server is executing.

(2) A replicating machine that sends replicated files to a partner (client). The term "server" refers to the machine acting in response to requests from partners that want to receive replicated files.

(3) A **DirectPlay** system application that is hosting a **DirectPlay** game session. In the context of **DirectPlay 8**, the term is reserved for **hosts** using **client/server mode**.

(4) For the Peer Content Caching and Retrieval Framework, a server is a server-role peer; that is, a peer that listens for incoming block-range requests from client-role peers and responds to the requests.

- (5) Used as a synonym for domain controller. See [\[MS-DISO\]](#).
- (6) Refers to the Group Policy server that is involved in a policy application sequence. See [\[MS-GPOL\]](#).
- (7) The entity that responds to the HTTP connection. See [\[MS-TSWP\]](#).
- (8) A server capable of issuing OMA-DM commands to a client and responding to OMA-DM commands issued by a client. See [\[MS-MDM\]](#).
- (9) Used to identify the system that implements WMI services, provides management services, and accepts DCOM ([\[MS-DCOM\]](#)) calls from WMI clients.
- (10) A domain controller. Used as a synonym for domain controller. See [\[MS-ADOD\]](#).
- (11) An entity that transfers content to a client through streaming. A server might be able to do streaming on behalf of another server; thus, a server can also be a proxy. See [\[MS-WMLOG\]](#).
- (12) Used as described in [\[RFC2616\]](#) section 1.3. See [\[MS-NTHT\]](#).
- (13) For the purposes of [\[MS-RDC\]](#), the server is the source location.
- (14) Any process that accepts commands for execution from a client by using the PowerShell Remoting Protocol.

Server Message Block (SMB): A protocol that is used to request file and print services from server systems over a network. The SMB protocol extends the CIFS protocol with additional security, file, and disk management support. For more information, see [\[CIFS\]](#) and [\[MS-SMB\]](#).

server name: The name of a server, as specified in the operating system settings for that server.

server object: (1) A class of **object** in the **configuration naming context (config NC)**. A **server object** can have an **nTDSDSA object** as a child.

(2) Part of the **Remoting Data Model**. A **server object** is an instance of a **Server Type**. A **server object** is either an **SAO** or an **MSO**.

(3) The database object in the account domain with an object class of samServer.

Server Reflexive Candidate: A **candidate** whose transport addresses is a **network address translation (NAT)** binding that is allocated on a NAT when an **endpoint** (5) sends a packet through the NAT to the server. A Server Reflexive Candidate can be discovered by sending an allocate request to the **TURN server** or by sending a binding request to a **Simple Traversal of UDP through NAT (STUN)** server.

Server Scale Secure Real-Time Transport Protocol (Server SS RTP): A derivative of the **Scale Secure Real-Time Transport Protocol (SS RTP)** that is used by applications to receive media from multiple senders and fan-out media to multiple receivers. Typically, applications such as Multipoint Control Units (MCUs) use this mode of encryption.

Server Type: Part of the **Remoting Data Model**. A **Server Type** contains **Remote Methods**.

server-activated object (SAO): A server object that is created on demand in response to a client request. See also **marshaled server object**.

server-relative URL: A relative URL that does not specify a scheme or host, and assumes a **base URI** of the root of the host, as described in [\[RFC3986\]](#).

service: (1) A process or agent available on the network, offering resources or services for clients. Examples of services include file servers, web servers, and so on.

(2) A process or agent that is available on the network, offering resources or services for clients. Examples of services include file servers, web servers, and so on.

(3) A program that is managed by the **Service Control Manager (SCM)**. The execution of this program is governed by the rules defined by the **SCM**.

(4) The receiving endpoint of a **web services** request message, and sender of any resulting **web services** response message.

(5) A logical functional unit that represents the smallest units of control and that exposes actions and models the state of a physical device with state variables. For more information, see [\[UPNPARCH1.1\]](#) section 3.

(6) An application that provides management services to clients through the WS-Management Protocol and other web services.

(7) A **SIP method** defined by Session Initiation Protocol Extensions used by the **client** to request a service from the **server**.

SERVICE: A method that is defined by **Session Initiation Protocol (SIP)** extensions and is used by an SIP client to request a service from a server.

service application: A middle-tier application that runs without any user interface components and supports other applications by performing tasks such as retrieving or modifying data in a database.

Service Control Manager (SCM): An **RPC** server that enables configuration and control of **service** programs.

session: (1) A unidirectional communication channel for a stream of messages that are addressed to one or more destinations. A destination is specified by a resource URL, an identity URL, and a device URL. More than one session can be multiplexed over a single connection.

(2) A representation of application data in system memory. It is used to maintain state for application data that is being manipulated or monitored on a protocol server by a user.

(3) A collection of multimedia senders and receivers and the data streams that flow between them. A multimedia conference is an example of a multimedia session.

(4) In **Kerberos**, an active communication channel established through **Kerberos** that also has an associated cryptographic **key**, message counters, and other state.

(5) In **Server Message Block (SMB)**, a persistent-state association between an **SMB** client and **SMB** server. A **session** is tied to the lifetime of the underlying **NetBIOS** or TCP connection.

(6) In the **Challenge-Handshake Authentication Protocol (CHAP)**, a **session** is a lasting connection between a peer and an authenticator.

(7) In the Workstation service, an authenticated connection between two computers.

(8) An active communication channel established through NTLM, that also has an associated cryptographic **key**, message counters, and other state.

(9) In **OleTx**, a transport-level connection between a **Transaction Manager** and another Distributed Transaction participant over which multiplexed logical connections and messages flow. A **session** remains active so long as there are logical connections using it.

(10) The state maintained by the server when it is **streaming content** to a client. If a server-side **playlist** is used, the same **session** is used for all **content** in the **playlist**.

(11) An **authenticated context** that is established between an SMB 2 Protocol client and an SMB 2 Protocol server over an SMB 2 Protocol **connection** for a specific security principal. There could be multiple active **sessions** over a single SMB 2 Protocol **connection**. The SessionId field in the SMB2 packet header distinguishes the various **sessions**.

(12) An authenticated communication channel between the client and server correlating a group of messages into a conversation.

(13) A collection of state information on a directory server. An implementation of the **SOAP session extensions (SSE)** is free to choose the state information to store in a session.

(14) In **LU 6.2**, a **session** is a **connection** between **LUs** that can be used by a succession of **conversations**. A given pair of LU 6.2s may be connected by multiple **sessions**. For a more complete definition, see [\[LU62Peer\]](#).

(15) A context for managing communication over LLTD among **stations**.

(16) The operational environment in which an application and its **commands** execute.

(17) A context for managing communication over **qWave-WD** among devices. This is equivalent to a **TCP** connection.

(18) A multimedia **session** is a set of multimedia senders and receivers and the data streams flowing from senders to receivers. A multimedia conference is an example of a multimedia **session**.

(19) A set of multimedia senders and receivers and the data streams flowing from senders to receivers. A multimedia **conference** is an example of a multimedia session.

Session Description Protocol (SDP): (1) A protocol that is used to announce sessions, manage session invitations, and perform other types of initiation tasks for multimedia sessions, as described in [\[RFC3264\]](#).

(2) A protocol that is used for session announcement, session invitation, and other forms of **multimedia session** initiation. For more information see [\[MS-SDP\]](#) and [\[RFC3264\]](#).

session identifier: (1) A unique string that is used to identify a specific instance of session data and is used by stored procedures as an opaque primary key.

(2) A key that enables an application to make reference to a session.

(3) Unique identifier that an operating system generates when a session is created. A session spans the period of time from logon until logoff from a specific system.

Session Initiation Protocol (SIP): An application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. **SIP** is defined in [\[RFC3261\]](#).

Session Initiation Protocol (SIP) address: A URI that does not include a "sip:" prefix and is used to establish multimedia communications sessions between two or more users over an IP network, as described in [\[RFC3261\]](#).

session key: (1) A symmetric key that is derived from a master key and is used to encrypt or authenticate a specific media stream by using the **Secure Real-Time Transport Protocol (SRTP)** and **Scale Secure Real-Time Transport Protocol (SSRTP)**.

(2) A relatively short-lived **symmetric key** (a cryptographic key negotiated by the client and the server based on a shared secret). A session key's lifespan is bounded by the **session** to which it is associated. A **session key** should be strong enough to withstand cryptanalysis for the lifespan of the **session**.

session recycling: A process in which active **sessions** (2) are closed to start new sessions and to limit the total number of active sessions.

Setting: A partition of a **metadata store**. It is used to store Properties, localized names, and **access control entries (ACEs)** for **MetadataObjects**.

setup path: The location where supporting files for a product or technology are installed.

SHA: See **system health agent (SHA)**.

SHA-1: An algorithm that generates a 160-bit hash value from an arbitrary amount of input data, as described in [\[RFC3174\]](#). SHA-1 is used with the Digital Signature Algorithm (DSA) in the Digital Signature Standard (DSS), in addition to other algorithms and standards.

SHA-1 hash: A hashing algorithm as specified in [\[FIPS180-2\]](#) that was developed by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA).

SHA-256: An algorithm that generates a 256-bit hash value from an arbitrary amount of input data, as described in [\[FIPS180-2\]](#).

shade: A color that is mixed with black. A 10-percent shade is one part of the original color and nine parts black.

shading pattern: A **background color** pattern against which characters and graphics are displayed, typically in tables. The color can be no color or it can be a specific color with a transparency or pattern value.

shadow copy: A duplicate of data held on a **volume** at a well-defined instant in time.

shadow effect: A formatting effect that makes a font or object appear to be elevated from the page or screen surface, and therefore casts a shadow.

shallow refinement: A type of query refinement that is based on the aggregation of managed property statistics for only some results of a search query. The number of refined results varies according to implementation. See also **deep refinement**.

shape: A collection of qualifiers, such as names, and quantifiers, such as coordinates, that is used to represent a geometric object. A shape can be contained in a document, file structure, run-time structure, or other medium.

shape identifier: An integer that corresponds to a shape object or an instantiation of a shape object.

share: (1) A resource offered by a Common Internet File System (CIFS) server for access by CIFS clients over the network. A **share** typically represents a directory tree and its included files (referred to commonly as a "disk share" or "file share") or a printer (a "print share"). If the information about the **share** is saved in persistent store (for example, Windows registry) and reloaded when a file server is restarted, then the **share** is referred to as a "sticky share". Some **share** names are reserved for specific functions and are referred to as special **shares**: IPC\$, reserved for interprocess communication, ADMIN\$, reserved for remote administration, and A\$, B\$, C\$ (and other local disk names followed by a dollar sign), assigned to local disk devices.

(2) To make content on a **host** desktop available to **participants**. **Participants** with a sufficient **control level** may interact remotely with the **host** desktop by sending input commands.

(3) A local resource that is offered by an SMB 2 Protocol server for access by SMB 2 Protocol clients over the network. The SMB 2 Protocol defines three types of **shares**: file (or disk) **shares**, which represent a directory tree and its included files; pipe **shares**, which expose access to named pipes; and print **shares**, which provide access to print resources on the server. A pipe **share** as defined by the SMB 2 Protocol must always have the name "IPC\$". A pipe **share** must only allow named pipe operations and DFS referral requests to itself.

shared lock: A condition in which multiple protocol clients or protocol servers can read or write data concurrently, but no transaction can acquire an **exclusive lock** on the data until all of the shared locks have been released.

shared search scope: An administrator-defined **restriction** (1) that can be added to a query to limit query results to a collection of content. This restriction is available to multiple **site collections**.

Shared Services Provider (SSP): A logical grouping of shared service applications, and their supporting resources, that can be configured and managed from a single server and can be used by multiple server farms.

shared space: A set of tools that is synchronized between different **endpoints** (3), as described in [\[MS-GRVDYNM\]](#).

shared view: A view of a list or **Web Parts Page** that every user who has the appropriate permissions can see.

shared workbook: A workbook that is configured to enable multiple users on a network to view and make changes to it at the same time. Each user who saves the workbook sees the changes that are made by other users.

sheet: (1) A part of an Excel workbook. There are four types of sheets: **worksheet**, **macro sheet**, **dialog sheet**, and **chart sheet**. Multiple sheets are stored together within a workbook.

(2) A worksheet. The term sheet frequently refers to a worksheet because worksheets are the most common type of sheet.

sheet stream: See **stream** (1) and **document stream**.

sheet tab: A control that is used to select a sheet.

sheet view: A collection of display settings, such as which cells are shown, and the zoom level for a sheet window.

short-term lock: A type of check-out process in Windows SharePoint Services. Short-term checkouts are implicit and are done when a file is opened for editing. A lock is applied to the file while it is being edited in the client application so that other users cannot modify it. After the client application is closed, the lock is released.

shrink to fit: The process of adjusting the font size of text in a cell to fit the current height and width of the cell.

Side: An area on a **physical medium** that can store data. Although most **physical media** have only a single **side**, some may have two **sides**. For instance, a magneto-optic (MO) disk has two **sides**: an "A" **side** and a "B" **side**. When an MO disk is placed in a **drive** with the "A" **side** up, the "A" **side** is accessible and the "B" **side** is not. To access the "B" **side**, the disk must be inserted with the "B" **side** up. The data stored on different **sides** of the same **physical medium** are independent of one another.

signature: (1) A synonym for hash.

(2) A value computed with a cryptographic algorithm and bound to data in such a way that intended recipients of the data can use the **signature** to verify that the data has not been altered and/or has originated from the signer of the message, providing message integrity and **authentication**. The **signature** can be computed and verified either with **symmetric key** algorithms, where the same **key** is used for signing and verifying, or with asymmetric **key** algorithms, where different **keys** are used for signing and verifying (a private and public **key** pair are used). For more information, see [\[WSFedPRP\]](#).

(3) The lowest **node ID** in the **graph**.

(4) A structure containing a hash and block **chunk** size. The hash field is 16 bytes, and the **chunk** size field is a 2-byte unsigned integer.

silence suppression: A mechanism for conserving bandwidth by detecting silence in the audio input and not sending packets that contain only silence.

Simple Mail Transfer Protocol (SMTP): A member of the TCP/IP suite of protocols that is used to transport Internet messages, as described in [\[RFC5321\]](#).

Simple Symmetric Transport Protocol (SSTP): A protocol that enables two applications to engage in bi-directional, asynchronous communication. SSTP supports multiple application **endpoints** (5) over a single network connection between client nodes.

Simple Symmetric Transport Protocol Security Protocol (SSTP) security: An independent sub-protocol that is exchanged within defined **Simple Symmetric Transport Protocol (SSTP)** messages, and is used for mutual **authentication** (2) between a relay server and a client device or an account.

Simple Traversal of UDP through NAT (STUN): A protocol that enables applications to discover the presence of and types of network address translations (NATs) and firewalls that exist between those applications and the Internet.

simple type: An element that can contain only text and appears as <simpleType> in an **XML document** or any **attribute** (1) of an element. Attributes are considered simple types because they contain only text. See also **complex type**.

single accounting: An underline style that places one line beneath the text. Single accounting can be used to indicate subtotals.

single sign-on (SSO): A process that enables users who have a domain user account to log on to a network and gain access to any computer or resource in the domain without entering their **credentials** multiple times.

single sign-on (SSO) administrator: A **security principal** (2) who is authorized to change a single sign-on (SSO) configuration and to obtain master secrets from a master secret server.

single sign-on (SSO) identifier: A string that represents the definition of user credentials that permit a user to access a network. See also **single sign-on (SSO)**.

single-valued claim: See **claim**.

SIP element: An entity that understands the **Session Initiation Protocol (SIP)**.

SIP message: The data that is exchanged between **Session Initiation Protocol (SIP)** elements as part of the protocol. An SIP message is either a request or a response.

SIP method: The primary function that an **SIP request** is meant to call on a **server**. This method is carried in the **request** message itself. Example methods are **INVITE** and **BYE**.

SIP protocol client: A network client that sends **Session Initiation Protocol (SIP)** requests and receives SIP responses. An SIP client does not necessarily interact directly with a human user. **User agent clients (UACs)** and proxies are SIP clients.

SIP registrar: A **Session Initiation Protocol (SIP)** server that accepts REGISTER requests and places the information that it receives from those requests into the location service for the domain that it handles.

SIP request: A **Session Initiation Protocol (SIP)** message that is sent from a **user agent client (UAC)** to a **user agent server (UAS)** to call a specific operation.

SIP response: A **Session Initiation Protocol (SIP)** message that is sent from a **user agent server (UAS)** to a **user agent client (UAC)** to indicate the status of a request from the UAC to the UAS.

SIP response code: A three-digit code in a **Session Initiation Protocol (SIP)** message, as described in [\[RFC3261\]](#).

SIP transaction: A **SIP transaction** occurs between a **UAC** and a **UAS**. The **SIP transaction** comprises all messages from the first **request** sent from the **UAC** to the **UAS** up to a **final response** (non-1xx) sent from the **UAS** to the **UAC**. If the **request** is **INVITE**, and the **final response** is a non-2xx, the **SIP transaction** also includes an ACK to the **response**. The ACK for a 2xx **response** to an **INVITE request** is a separate **SIP transaction**.

site: (1) A group of related webpages that is hosted by a server on the World Wide Web or an intranet. Each website has its own entry points, metadata, administration settings, and workflows. Also referred to as web site.

(2) A group of related pages and data within a SharePoint site collection. The structure and content of a site is based on a site definition. Also referred to as SharePoint site and web site.

(3) A collection of one or more well-connected (reliable and fast) TCP/IP subnets. By defining **sites** (represented by site objects) an administrator can optimize both **Active Directory** access and **Active Directory replication** with respect to the physical network. When users log in, **Active Directory** clients find **domain controllers (DCs)** that are in the same **site** as the user, or near the same **site** if there is no **DC** in the **site**. See also **Knowledge Consistency Checker (KCC)**. For more information, see [\[MS-ADTS\]](#).

site collection: A set of **websites** (1) that are in the same **content database**, have the same owner, and share administration settings. A site collection can be identified by a **GUID** or the **URL** of the **top-level site** for the site collection. Each site collection contains a top-level site, can contain one or more subsites, and can have a shared navigational structure.

site collection administrator: A user who has administrative permissions for a site collection.

site collection group: A named collection of users and domain groups that can be managed for a site collection or site. A group can be used to assign permission levels, send email messages, and indicate site membership for multiple users simultaneously.

site collection identifier: A GUID that identifies a site collection. In stored procedures, the identifier is typically "@SiteId" or "@WebSiteId". In databases, the identifier is typically "SiteId/tp_SiteId".

site content type: A named and uniquely identifiable collection of settings and fields that store metadata for lists within individual sites.

site definition: A family of site definition configurations. Each site definition specifies a name and contains a list of associated site definition configurations.

site definition configuration: An XML-based definition of lists, features, modules, and other data that collectively define a type of SharePoint site. Site definition configurations are stored in the ONET.xml file.

site hop: The process of traversing from one website to another during a crawl. See also **page hop**.

site identifier: A GUID that is used to identify a site in a **site collection**.

site map provider: An object that provides a hierarchy of nodes that represent navigation for a **site** (2).

site membership: The status of being a member of a site and having a defined set of user rights for accessing or managing content on that site.

site solution: A deployable, reusable package that contains a set of features, site definitions, and assemblies that apply to sites, and can be enabled or disabled individually.

site subscription: A logical grouping of **site collections** that share a common set of features and service data.

site subscription identifier: A GUID that is used to identify a site subscription.

site template: An XML-based definition of site settings, including formatting, lists, views, and elements such as text, graphics, page layout, and styles. Site templates are stored in .stp files in the content database.

site-collection relative URL: A URL that is relative to the site collection that contains a resource, and does not begin with a leading slash (/).

site-relative URL: A URL that is relative to the site that contains a resource and does not begin with a leading slash (/).

slicer: A mechanism that is used to filter data in one or more PivotTable reports or cube functions.

slicer header: A user interface element that displays the **caption** for a slicer that can be or is being used to filter one or more PivotTable reports or cube functions. It also provides a command button for removing all applied filters.

slicer item: A user interface element that displays filter values that can be applied to one or more PivotTable reports or cube functions by using a slicer.

slide: A frame that contains text, shapes, pictures, or other content. A slide is a digital equivalent to a traditional film slide.

slide layout: An organizational scheme, such as Title Only or Comparison, for content on a presentation slide.

Slide Library: A type of a document library that is optimized for storing and reusing presentation slides that conform to the format described in [\[ISO/IEC-29500:2008\]](#).

slide show: A delivery of a sequence of presentation slides, typically to an audience.

slide show broadcast: A delivery of a sequence of presentation slides, typically to an audience, as a single session between a protocol server and one or more protocol clients.

Slot: A storage location within a **library**. For example, a tape **library** has one **slot** for each tape that the **library** can hold. A stand-alone **drive library** has no **slots**. Most **libraries** have at least four **slots**. Sometimes **slots** are organized into collections of **slots** called **magazines**. **Magazines** are usually removable.

smart document: A file that is programmed to assist the user as the user creates or updates the document. Several types of files, such as forms and templates, can also function as smart documents.

smart tag: A feature that adds the ability to recognize and label specific data types, such as people's names, within a document and displays an action button that enables users to perform common tasks for that data type.

smart tag actions button: A user interface control that displays a menu of actions that are associated with a specific smart tag.

smart tag indicator: A triangular symbol that appears in the bottom right corner of a cell and indicates that the cell contains a smart tag.

smart tag recognizer: An **add-in** that can interpret a specific type of smart tag, such as an address or a financial symbol, in a document and display an action button that enables users to perform common tasks for that data type.

snapshot: (1) A copy of a workbook that contains only values and formatting. It does not contain any formulas or data connections.

(2) The point in time at which a **shadow copy** of a **volume** is made.

SOAP: A lightweight protocol for exchanging structured information in a decentralized, distributed environment. **SOAP** uses **XML** technologies to define an extensible messaging framework, which provides a message construct that can be exchanged over a variety of underlying protocols. The framework has been designed to be independent of any particular programming model and other implementation-specific semantics. **SOAP 1.2** supersedes **SOAP 1.1**. See [\[SOAP1.2-1/2003\]](#).

SOAP 1.1: (1) Version 1.1 of the **SOAP** (Simple Object Access Protocol) standard. For the complete definition of **SOAP 1.1**, see [\[SOAP1.1\]](#).

(2) Simple Object Access Protocol (SOAP) 1.1 [\[SOAP1.1\]](#).

SOAP 1.2: Version 1.2 of the **SOAP** standard. Some examples of changes introduced in **SOAP 1.2** include an updated envelope structure, as well as updates to the structure and semantics for **SOAP faults**. The binding framework was also updated to allow binding to non-HTTP transports. Starting with version 1.2, **SOAP** is no longer an acronym. See also **SOAP**. For the complete specification of **SOAP 1.2**, see [\[SOAP1.2-1/2007\]](#) and [\[SOAP1.2-2/2007\]](#).

SOAP action: The HTTP request header field used to indicate the intent of the **SOAP** request, using a **URI** value. See [\[SOAP1.1\]](#) section 6.1.1 for more information.

SOAP body: A container for the payload data being delivered by a **SOAP message** to its recipient. See [\[SOAP1.2-1/2007\]](#) section 5.3 for more information.

SOAP envelope: A container for **SOAP message** information and the root element of a **SOAP** document. See [\[SOAP1.2-1/2007\]](#) section 5.1 for more information.

SOAP fault: A container for error and status information within a **SOAP message**. See [\[SOAP1.2-1/2007\]](#) section 5.4 for more information.

SOAP fault code: The algorithmic mechanism for identifying a **SOAP fault**. See [\[SOAP1.2-1/2007\]](#) section 5.6 for more information.

SOAP fault detail: A string containing a human-readable explanation of a **SOAP fault**, which is not intended for algorithmic processing. See [\[SOAP1.2-1/2007\]](#) section 5.4.5 for more information.

SOAP header: A mechanism for implementing extensions to a **SOAP message** in a decentralized manner without prior agreement between the communicating parties. See [\[SOAP1.2-1/2007\]](#) section 5.2 for more information.

SOAP message: An **XML** document consisting of a mandatory **SOAP envelope**, an optional **SOAP header**, and a mandatory **SOAP body**. See [\[SOAP1.2-1/2007\]](#) section 5 for more information.

SOAP Message: The data encapsulated in a SOAP envelope that flows back and forth between a protocol client and a web service, as described in [\[SOAP1.1\]](#).

SOAP Message Transmission Optimization Mechanism (MTOM): A method that is used to optimize the transmission and format of **SOAP messages** by encoding parts of the message, as described in [\[SOAP1.2-MTOM\]](#).

SOAP node: An element in a **SOAP message** that identifies the node on a SOAP message path that causes a fault to occur, as described in [\[SOAP1.1\]](#).

SOAP operation: An action that can be performed by a **Simple Object Access Protocol (SOAP)** service, as described in [\[SOAP1.1\]](#).

SOAP session extensions (SSE): Extensions to DSML that make it possible to maintain state information across multiple request/response operations.

social data: A collection of ratings, tags, and comments about webpages and items on a SharePoint site or the Internet. Individual users create this data and, by default, share it with other users.

social networking: The use of websites and services that provide enhanced information and interaction capabilities with regard to people and resources.

social rating: A user-defined value that indicates the perceived quality of a webpage or item on a SharePoint site or the Internet. Individual users create these ratings and, by default, share them with other users.

social tag: A user-defined keyword and hyperlink to a webpage or item on a SharePoint site or the Internet. Individual users create these tags and, by default, share them with other users.

social tag user: The user who created a **social tag**.

SOCKS proxy: A network device that routes network packets between protocol clients and protocol servers by using the SOCKS protocol and the proxy server features that are described in [\[RFC1928\]](#).

solution gallery: A **gallery** (1) that is used to store solution packages.

solution package: A compressed file that can be deployed to a server farm or a site. It can contain assemblies, resource files, site and feature definitions, templates, code access security policies, and Web Parts. Solution packages have a .wsp file name extension.

sort: A process that arranges cells in ascending or descending order, based on cell content.

sort condition: A condition that determines how to sort cells in a range.

sort order: (1) A set of rules in a search query that defines the order of relevant results. Each rule consists of a managed property, such as modified date or size, and a direction for order, such as ascending or descending. Multiple rules are applied sequentially.

(2) A specific arrangement of cells that is based on cell content. The order can be ascending or descending.

(3) The order in which the rows in a **Table object** are requested to appear. This can involve sorting on multiple properties and sorting of **categories** (5).

(4) The set of rules in a search query that define the ordering of rows in the search result. Each rule consists of a property (for example, name or size) and a direction for the ordering (ascending or descending). Multiple rules are applied sequentially.

source data: (1) The data that is used as the basis for charts, PivotTable reports, and other data visualization features.

(2) See **source file**.

source file: A **file** on a **source location** that is to be copied by **RDC**. Sometimes referred to as source.

source location: (1) A server, disk, file, document, or other collection of information from which a file or data is copied.

(2) The **source location** is the location from which a **file** is being transferred after it has been compressed with **RDC**.

source term: A specific instance of a **term**, in a specific term set, that is used to define permissions for the term.

source variation site: A **website** (2) that contains a collection of publishing pages to be copied to other sites, which are referred to as target variation sites. After the publishing pages are copied to a target variation site, they can be translated into another language. See also **target variation site**.

spam: An unsolicited email message.

sparkline: A miniature chart that can be inserted into text or embedded in a cell on a worksheet to illustrate highs, lows, and trends in data.

special folder: One of a default set of **Folder objects** that can be used by an implementation to store and retrieve user data objects.

SpecificFinder: A type of **MethodInstance** that can be called to return a specific EntityInstance of a specific Entity given its EntityInstanceId. SpecificFinder input is defined and ordered by the Identifiers that are associated with the Entity that is associated with the Method that is associated with the SpecificFinder.

split pane: A pane that consists of two or more discrete areas of a window. Each area displays content and scrolls independently from other areas of the window. See also **frozen panes**.

SplitButtonMRUPopup control: A type of **SplitButtonPopup control** whose icon changes to reflect the command that the user most recently selected from the menu that is displayed by that button.

SplitButtonPopup control: A type of Button control that performs an action when clicked, and can also display a menu of related commands when the user clicks a drop-down arrow that appears on the button.

SplitDropDown control: A type of Button control that performs a default action when clicked, and can also expand to display a list of other possible actions when the user clicks a drop-down arrow that appears on the button.

pool file: A representation of application content data than can be processed by a print driver. Common examples are enhanced metafile format and XML paper specification. For more information, see [\[MSDN-META\]](#) and [\[MSDN-XMLP\]](#).

spreadsheet data model: A local **Online Analytical Processing (OLAP)** storage of data used by a spreadsheet application.

SQL authentication: One of two mechanisms for validating attempts to connect to instances of SQL Server. In SQL authentication, users specify a SQL Server login name and password when they connect. The SQL Server instance ensures that the login name and password combination are valid before permitting the connection to succeed.

SQL statement: (1) A complete phrase in SQL that begins with a keyword and completely describes an action to be taken on data.

(2) A character string expression in a language that the server understands.

sRGB: (1) A standard color space that enables various devices, including cameras, scanners, displays, and printers, to produce colors that are reasonably identical, as described in [\[IEC-RGB\]](#).

(2) A standard, predefined **color space** that is portable across all devices and allows accurate **color matching** with little overhead. sRGB was developed by Hewlett-Packard and Microsoft and is specified in [\[IEC-RGB\]](#). It is available to users of Windows. Windows NT 3.1,

Windows NT 3.5, Windows NT 3.51, Windows 95, and Windows NT 4.0: **sRGB** color management technology is not available.

SsoTicketFilter: A **FilterDescriptor** type that is used in conjunction with a single sign-on (SSO) system to transmit an SSO ticket to a line-of-business (LOB) system.

SSRTP stream: A sequence of **Scale Secure Real-Time Transport Protocol (SSRTP)** packets from a sender and to a receiver who are identified by the same Synchronization Source (SSRC).

staging file: The backup of the changed file or folder. It encapsulates the data and attributes associated with a replicated file or folder. By creating the staging file, File Replication Service (FRS) ensures that file data can be supplied to partners regardless of any activity that might prevent access to the original file. The staging files can be compressed to save disk space and network bandwidth during replication.

staging object: A block of data that represents an instance of an object type as defined in the connected data source.

stamp: Information that describes an **originating update** by a **domain controller (DC)**. The **stamp** is not the new data value; the **stamp** is information about the update that created the new data value. A **stamp** is often called metadata, because it is additional information that "talks about" the conventional data values. A **stamp** contains the following pieces of information: the unique identifier of the **DC** that made the **originating update**; a sequence number characterizing the order of this change relative to other changes made at the originating **DC**; a version number identifying the number of times the data value has been modified; and the time when the change occurred.

start address: A URL that identifies a point at which to start a crawl. Administrators specify start addresses when they create or edit a content source.

startup directory: The directory from which an application opens data files when the application starts.

state changing: A type of operation that changes the state of a session.

statement of health ReportEntry (SoH ReportEntry): A collection of data that represents a specific aspect of the **health state** of a client.

static rank: The component of a rank that does not depend on a search query. It represents the perceived importance of an item and can be related to the origin of the item, and relationships between the item and other items or business rules that are defined in the search application. See also **dynamic rank**.

station: Any device that implements LLTD.

Status-Code: A 3-digit integer result code in an HTTP response message, as described in [\[RFC2616\]](#).

Status-Line: The first line of an HTTP response message, as described in [\[RFC2616\]](#).

stemming: A type of query expansion that factors relationships between words by reducing inflected words to their stem form or expanding stems to their inflected forms. For example, the words "swimming" and "swam" can be associated with the stem "swim."

stock chart: A custom chart type that is designed to display stock market data on multiple series; for example, high, low, close, and volume.

stop word: A language-specific token that is not indexed and is ignored in a query. It typically has low semantic content and is used only for grammatical purposes, for example “a” and “and” in the English language.

storage: (1) An element of a compound file that is a unit of containment for one or more storages and streams, analogous to directories in a file system, as described in [\[MS-CFB\]](#).

(2) A set of elements with an associated CLSID used to identify the application or component that created the storage.

(3) A storage object, as defined in [\[MS-CFB\]](#).

stored procedure: A precompiled collection of SQL statements and, optionally, control-of-flow statements that are stored under a name and processed as a unit. They are stored in a SQL database and can be run with one call from an application. Stored procedures return an integer return code and can additionally return one or more result sets. Also referred to as *sproc*.

store-relative form: See **store-relative URL**.

store-relative URL: A URL that consists only of a **path segment** and does not include the leading and trailing slash.

stream: (1) An element of a compound file, as described in [\[MS-CFB\]](#). A stream contains a sequence of bytes that can be read from or written to by an application, and they can exist only in storages.

(2) A flow of data from one host to another host, or the data that flows between two hosts.

(3) A sequence of bytes written to a file on the **NTFS** file system. Every file stored on a **volume** that uses the **NTFS** file system contains at least one **stream**, which is normally used to store the primary contents of the file. Additional **streams** within the file may be used to store file **attributes**, application parameters, or other information specific to that file. Every file has a default data **stream**, which is unnamed by default. That data **stream**, and any other data **stream** associated with a file, may optionally be named.

(4) A sequence of bytes that typically encodes application data.

(5) A sequence of **ASF** media objects ([\[ASF\]](#) section 5.2) that can be selected individually. For example, if a movie has an English and a Spanish soundtrack, each may be encoded in the **ASF** file as a separate **stream**. The video data would also be a separate **stream**.

(6) A **sequence** of **messages** whose delivery is guaranteed exactly once and in order.

(7) A set of **tracks** interchangeable at the client when playing **media**.

(8) An individual audio or video data-flow in a **presentation**. The **media data** in an individual **stream** always uses the same **media data format**.

(9) A flow of data from one host to another host. May also be used to reference the flowing data.

(10) A stream object, as defined in [\[MS-CFB\]](#).

stream cipher: A cryptographic algorithm that transforms plaintext bits into cipher text one bit or byte at a time. When the process is reversed, cipher text is transformed into plaintext one bit or byte at a time. See also **block cipher**.

StreamAccessor: A type of **MethodInstance** that can be called to retrieve a **Field** (4) of an EntityInstance in the form of a data stream of bytes.

streaming: (1) The act of transferring **content** from a sender to a receiver.

(2) The act of processing a part of an XML Infoset without requiring that the entire XML Infoset be available.

strikethrough formatting: A formatting option in which characters are crossed out by horizontal line.

stripe band: One or more adjacent **columns** (2) or **rows** (2) that are in a table and have the same **stripe formatting**.

stripe formatting: A table formatting option that applies **background colors** to alternating **rows** (2) or **columns** (2) to increase legibility.

stroke order: A sort order that arranges items in a sort range according to the number of strokes that is used to write each glyph. Stroke order is used when sorting text that is written in some East Asian languages.

strong name: A name that consists of the simple text name, version number, and culture information of an **assembly**, strengthened by a public key and a digital signature that is generated over the assembly.

structural object class: An **object class** that is not an **88 object class** and can be instantiated to create a new **object**.

structured document tag: An entity in a document that is used to denote content that is stored as **XML** data.

structured document tag bookmark: An entity in a document that is used to denote the location and presence of a **structured document tag**.

Structured Query Language (SQL): A database query and programming language that is widely used for accessing, querying, updating, and managing data in relational database systems.

structured XML query: An XML document that specifies a **query** that may contain multiple **subqueries**. For more information, see section 2.2.16.

STUN candidate: A **candidate** whose transport addresses are STUN-derived transport addresses. See also **Simple Traversal of UDP through NAT (STUN)**.

STUN-derived transport address: A **derived transport address** that is obtained by an **endpoint** (5) from a configured STUN server. See also **Simple Traversal of UDP through NAT (STUN)**.

style: A set of formatting options that is applied to text, tables, charts, and other objects in a document.

SubAuthority: A variable-length array of unsigned, 32-bit integer values that is part of a **security identifier (SID)**. Each of these values is called a **SubAuthority**. All **SubAuthority** values excluding the last one collectively identify a **domain**. The last value, termed as the **relative identifier (RID)**, identifies a particular **group** or account relative to the **domain**. For more information, see [\[SIDD\]](#).

submit: The process of sending data to an external data source such as a web service, database, Internet message, or SharePoint site.

subquery: A component of a **structured XML query**. For more information, see section 2.2.16.

Subrequest: A request within a SYNC_VOLUMES request. For details on requests, see section 3.1.4.

SUBSCRIBE: A **Session Initiation Protocol (SIP)** method that is used to request asynchronous notification of an event or a set of events at a later time.

subscriber: (1) A **Session Initiation Protocol (SIP)** client that is making a SUBSCRIBE request.

(2) An application that needs to receive events that are published by another application.

(3) An application that needs to receive historical data published by another application.

subscription: (1) The result of a SUBSCRIBE request from a **Session Initiation Protocol (SIP)** element.

(2) The end result of an act of a **SIP element** sending a **SUBSCRIBE** request.

(3) A registration performed by a **subscriber** to specify a requirement to receive events, future messages, or historical data.

(4) A request for a copy of a publication to be delivered to a subscriber. For more information, see [\[MSDN-RepPub\]](#).

subsite: A complete website that is stored in a named subdirectory of another website. The parent website can be the top-level site of a site collection or another subsite. Also referred to as subweb.

suffix length: An integer that represents the number of bytes of the current index key string minus the number of identical bytes at the beginning of the current and previous index key strings. See also **prefix length**.

summary: The orientation of **outline expand** and **outline collapse** symbols in relation to the data that is outlined.

Super P-frame (SP-frame): A special P-frame that uses the previous **cached frame** instead of the previous **P-frame** or **I-frame** as a reference frame.

surface chart: A chart that shows a three-dimensional surface that connects a set of data points. It can be used to determine the optimum combination between two sets of data.

surrogate pair: A pair of 16-bit Unicode encoding values that, together, represent a single 32-bit character, as described in [\[ISO-10646\]](#). For more information about surrogate pairs and combining character sequences, see the Unicode Standard in [\[UNICODE\]](#).

survey list: A list that is preconfigured and optimized for conducting surveys and compiling survey results into graphical views.

survivable mode: A mode that enables a protocol client to access basic voice services if some server or network resources are unavailable.

switch: (1) A data link-layer device that propagates frames between segments and allows communication among stations on different segments. Stations that are connected through a

switch see only those frames destined for their segments. Compare this term with hub and router.

(2) A logical device type that provides options to run a terminal window or a custom script for a dial-up connection. This device type is not used for dialing a connection.

switchable site map provider: A **site map provider** that uses other site map providers as its source data when constructing a site map.

symbol file: A file that contains information about an executable image, including the names and addresses of functions and variables.

symmetric key: A **secret key** used with a cryptographic symmetric algorithm. The key needs to be known to all communicating parties. For an introduction to this concept, see [\[CRYPTO\]](#) section 1.5.

synchronization engine: A code module that creates an integrated view of objects that are stored in multiple, connected data sources, and manages information in those data sources.

synchronization source (SSRC): The source of a **stream** (6) of **RTP packets**, identified by a 32-bit numeric SSRC identifier carried in the RTP header so as not to be dependent upon the network address. All packets from a synchronization source form part of the same timing and sequence number space, so a receiver groups packets by synchronization source for playback. Examples of synchronization sources include the sender of a **stream** of packets derived from a signal source such as a microphone or a camera, or an RTP **mixer**. A synchronization source may change its data format (for example, audio encoding) over time. The SSRC identifier is a randomly chosen value meant to be globally unique within a particular **RTP session**. A **participant** need not use the same SSRC identifier for all the **RTP sessions** in a **multimedia session**; the binding of the SSRC identifiers is provided through RTCP. If a **participant** generates multiple **streams** in one **RTP session**, for example from separate video cameras, each MUST be identified as a different SSRC. See [\[RFC3550\]](#) section 3.

Synchronization Source (SSRC): A 32-bit identifier that uniquely identifies a media **stream** (2) in a **Real-Time Transport Protocol (RTP)** session. An SSRC value is part of an **RTP packet** header, as described in [\[RFC3550\]](#).

Synchronized Multimedia Integration Language (SMIL): An XML-based language that enables a data stream to be divided, transmitted as separate streams, and then recombined as a single stream, as described in [\[W3C-SMIL3.0\]](#).

syntax: See **attribute syntax**.

system health agent (SHA): The client components that make declarations on a specific aspect of the client **health state** and generate a **statement of health ReportEntry (SoH ReportEntry)**.

system palette: (1) An itemization of all of the colors that can be displayed by the operating system for a device.

(2) The **palette** that is actually in use to reproduce colors on a device such as a computer screen. A system palette has predefined, device-specific colors that are used by default, so that individual applications do not have to set them up.

system partition: A partition that contains the boot loader needed to invoke the operating system on the boot partition. A system partition must also be an active partition. It can be, but is not required to be, the same partition as the boot partition.

system resources: The physical resources of a server computer, such as memory, disk space, CPU, and network bandwidth.

system volume (SYSVOL): A shared directory that stores the server copy of the **domain's** public files that must be shared for common access and replication throughout a **domain**.

SystemID: A binary identifier that is used to uniquely identify a **security principal** (2). For Windows integrated authentication, it is a **security identifier (SID)**. For an **ASP.NET** Forms Authentication provider, it is the binary representation that is derived from a combination of the provider name and the user login name.

22 T

table: (1) A **list** (2) that is defined in a workbook.

(2) A data region on a report layout that displays data in a columnar format.

(3) A two-dimensional object in a relational database that stores data in rows and columns.

table header: The top row of a table, where the column names are displayed.

Table object: An object that is used to view properties for a collection of objects of a specific type, such as a **Message object** or a **Folder object**. A Table object is structured in a row and column format with each row representing an object and each column representing a property of the object.

table style: A set of formatting options, such as font, **border formatting**, and **row banding**, that are applied to a table. The regions of a table, such as the header row, header column, and data area, can be variously formatted.

tablix: A data region that contains rows and columns that resembles a table or matrix, possibly sharing characteristics of both.

tag prefix: In **ASP.NET** markup, an identifier that appears before the name of a control and specifies the **assembly** that contains the control. A tag prefix is assigned on a per-page or per-site basis.

Tagged Image File Format: See **TIFF**.

target: An **actor** to which a **task** (2) is assigned.

target application: A logical entity that represents a software system for which credentials are maintained. It consists of metadata including the number and type of credentials that are required by the software system and a set of **claims** (2) that identify the administrators who can update, read, and delete the entity.

target group: A named collection of **client computers** whose members are defined administratively.

target location: The **target location** is the destination location of a file that has been compressed by **RDC**.

target variation site: A **website** (2) to which a collection of publishing pages were copied from another site, which is referred to as a source variation site. See also **source variation site**.

task: (1) An act to be executed by all **query servers**, and any requisite information for those query servers to execute that act correctly.

(2) A component of an **action** (1) that defines the work that **actors** need to do within a workflow system. An action can have zero or more tasks that are each assigned to different **targets**. There is a one-to-one correlation between tasks and targets.

(3) An **object** (1) that represents an assignment to be completed.

(4) An object identifying an administrative action (for example, running a program) to be performed on specified **triggers** and **conditions** (for example, every day at a specific time).
Synonym for **job**.

(5) The building block of a package. A task consists of code that executes a function, as specified by the options, settings, and parameters of the task that are specified when the task is called.

task pane app: An **app for Office** that appears docked in a task pane.

taxonomy navigation: A hierarchy of navigation menus that represents the navigation menus in terms and term sets and are independent of where their underlying objects, such as pages, are located.

taxonomy site map provider: A **site map provider** that uses **taxonomy navigation** as its source data for constructing a site map.

TCP/IP: A set of networking protocols that is widely used on the Internet and provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. It includes standards for how computers communicate and conventions for connecting networks and routing traffic.

telespace: See **shared space**.

template: A file that contains pre-defined formatting including layout, text and graphics. It serves as the basis for new documents that have a similar look or purpose. See also **form template** (Microsoft InfoPath) and **site template** (SharePoint Products and Technologies).

tenant: (1) A protocol client or protocol server that accesses a partition in a shared service database.

(2) A built-in custom field in IPAM that is used to specify the tenant machine.

term: A concept or an idea that is stored and can be used as metadata.

term label: A string that is used as the display value for a term. Each term label is associated with a specific language.

term set: A collection of terms that are arranged into and stored as a hierarchy or a flat list.

term set group: A collection of **term sets**.

term store: A database in which managed metadata is stored in the form of **term sets** and **terms**.

text importation: A process that incorporates textual data into a workbook, either by opening a text file or through an external link.

text ruler: A collection of settings for tabs, margins, and indentation of text. See also **ruler**.

text run: A string of characters that represents a discrete span of text with the same formatting properties.

theme: A set of unified design elements, such as colors, fonts, graphics, and styles, that define the appearance of a website, document, or data visualization.

thicket: A means of storing a complex HTML document with its related files. It consists of a thicket main file and a hidden thicket folder that contains a thicket manifest and a set of thicket supporting files that, together, store the referenced content of the document.

thicket folder: A hidden folder that contains a thicket manifest and a set of thicket supporting files that, together, store the referenced content of a complex HTML document.

thicket main file: The core file of a complex HTML document. It references contained elements such as graphics, pictures, or other media that are stored as thicket supporting files in a thicket folder. The thicket main file is the target that is used by a protocol client to access the content of the document.

thicket supporting file: A file that contains a graphic element, a picture, or other media that is referenced by the **thicket main file** and is stored in the **thicket folder**.

third-party request: A **conference control request** that modifies the state of participants other than the participant who sent the request.

throttle configuration setting: A set of configuration information that supports algorithms that are implementation-specific and enforce time and space limits when executing operations against a **line-of-business (LOB) system**. Examples are: limiting the number of concurrent operations against the LOB system, stopping an operation after a specific amount of time, and rejecting operations that read or write more than a specific quantity of data.

thumbnail: A miniature version of an image that is typically used to browse multiple images quickly.

tick mark: A small line of measurement, similar to a division line on a ruler, that intersects an axis in a chart.

ticket: A record generated by the **key distribution center (KDC)** that helps a client authenticate to a service. It contains the client's identity, a unique cryptographic key for use with this ticket (the **session key**), a time stamp, and other information, all sealed using the service's **secret key**. It only serves to authenticate a client when presented along with a valid authenticator.

TIFF: A high-resolution, tag-based image format. **Tagged Image File Format (TIFF)** is used for the universal interchange of digital images. For more information, see [\[RFC3302\]](#).

time code: A digital signal applied to a stream. The signal assigns a number to every frame of video, representing hours, minutes, seconds, and frames.

time condition: A logical condition that can be evaluated, or an event that can be triggered, to determine whether timed object behavior starts or ends. Conditions include items such as the start or end of time nodes, keyboard presses, mouse clicks, or delegate events. See also **time node**.

time hierarchy: A specialized Online Analytical Processing (OLAP) hierarchy that can be organized into lower and higher levels of detail, such as Year, Quarter, Month, and Day.

time node: A record or parent node that stores the information that is necessary to cause a time- or action-based effect to occur. Each time node has a corresponding object to which an effect is applied. It can be used randomly, simultaneously, or sequentially, and it can be used to specify certain time-based effects between objects that are being animated. Effects include visual and media behaviors.

time stamp authority: A service acknowledging that a datum existed before a specific time. The service is typically a trusted third party.

time zone: A geographical area that observes the same local time. The local time has a positive, zero, or negative offset from **Coordinated Universal Time (UTC)**. The offset can be different during standard time and daylight saving time.

time zone bias: The positive, zero, or negative offset in minutes from **Coordinated Universal Time (UTC)**. For example, Middle European Time (MET, GMT+01:00) has a time zone bias of "-60" because it is one hour ahead of UTC. Pacific Standard Time (PST, GMT-08:00) has a time zone bias of "+480" because it is eight hours behind UTC.

time zone daylight bias: The positive, zero, or negative offset in minutes that is added to the time zone bias during daylight saving time. For example, daylight saving time advances the clock by one hour. The time zone daylight bias is set to "-60".

time zone daylight date: The date and time when the change from standard time to daylight saving time occurs.

time zone standard bias: A positive, zero, or negative offset in minutes that is added to the time zone bias outside daylight saving time.

time zone standard date: The date and time when the change from daylight saving time to standard time occurs.

timestamp: A condition of a **digital signature** (2) that indicates whether the signature was created with a valid **certificate** (1) that has expired or was created with a certificate that had expired already. If the certificate expired after the signature was created, the signature can be trusted. If it expired before the signature was created, it cannot be trusted.

TimeStampFilter: A **FilterDescriptor** type that is used when querying a line-of-business (LOB) system. Its value can be a timestamp that specifies the earliest update to return, if the LOB system can return data that was updated after a specified time.

title master slide: A slide that defines the formatting and content that can be used by presentation slides that have a title slide layout. If a slide uses formatting and content from a title master slide, it is referred to as following a title master slide.

token: (1) A word in an item or a search query that translates into a meaningful word or number in written text. A token is the smallest textual unit that can be matched in a search query. Examples include "cat", "AB14", or "42".

(2) A set of rights and privileges for a given user.

(3) The byte that specifies the start of a record.

(4) A block of data that is issued to a **user** on successful **authentication** by the **authentication server**. Such a **token** is presented to a service to prove one's identity and attributes to a service. The **token** is used in the process of determining the **user's** authorization and access privileges.

tombstone: (1) An individual record of scheduling data that represents a **Meeting object** where an attendee declined a meeting.

(2) An object that has been deleted, but remains in storage until a configured amount of time (the **tombstone lifetime**) has passed, after which the object is permanently removed from storage. By keeping the **tombstone** in existence for the **tombstone lifetime**, the deleted state of the object is able to replicate. **Tombstones** exist only when the **Recycle Bin optional feature** is not enabled.

(3) In Distributed File System Replication (DFS-R), an update pertaining to a file deletion.

(4) A marker that is used to represent an item that has been deleted. A tombstone is used to track deleted items and prevent their reintroduction into the synchronization community.

(5) An inactive DNS node which is not considered to be part of a DNS **zone** but has not yet been deleted from the **zone** database in the **directory server**. **Tombstones** may be permanently deleted from the **zone** once they reach a certain age. **Tombstones** are not used for DNS **zones** that are not stored in the **directory server**. A node is a tombstone if its `dnsTombstoned` attribute has been set to "TRUE".

tombstone lifetime: The amount of time a deleted directory object remains in storage before it is permanently deleted. To avoid inconsistencies in object deletion, the **tombstone lifetime** is configured to be many times longer than the worst-case replication latency.

toolbar: A row, column, or block of controls that represent tasks or commands within an application. A toolbar can be either a menu toolbar, which provides access to menu commands, or a **basic toolbar**, which contains buttons that provide shortcuts to tasks that are frequently accessed from menus.

toolbar control: An object that appears on a toolbar and enables user interaction or input, typically to initiate an action, display information, or set values.

toolbar control identifier (TCID): An integer that identifies a specific control on a toolbar.

toolbar delta: A file component that stores a modification that a user made to a built-in toolbar. Stored modifications include adding, changing, or removing a control from a built-in toolbar.

ToolTip: A small pop-up window that provides brief context-sensitive help when users point to an item. Also referred to as ScreenTip.

top N filter: A filter that matches the top or bottom N items or N% of items in a specified **column** (2).

top N filter by count: A type of top N filter that matches the N largest numerical values or the N newest time and date values.

top N filter by percent: A type of top N filter that matches the N percent largest numerical values or the N percent newest time and date values.

top N filter by sum: A type of top N filter that matches the largest numerical values or the newest time and date values whose sum is equal to or greater than N.

top-level site: The first site in a site collection. All other sites within a site collection are child sites of the top-level site. The URL of the top-level site is also the URL of the site collection.

top-level toolbar: A **basic toolbar** that is not contained by another **toolbar**.

topology: The structure of the connections between members.

topology discovery test: A test that an application or higher-layer protocol can use to facilitate discovering the link-layer topology of a single link in a network. That is, to facilitate discovering the set of **segments** and **switches**, and determining which **responders** are on which segments. Compare this term with **quick discovery**.

total row: A row in a **list** (2) or table that provides a selection of aggregate functions that are useful for working with numerical data.

tour: A **scene** or sequence of scenes that describe a story about geographical locations, time periods, and data visualization.

track: (1) Any of the concentric circles on a disk platter over which a magnetic head (used for reading and writing data on the disk) passes while the head is stationary but the disk is spinning. A track is subdivided into sectors, upon which data is read and written.

(2) A time-ordered collection of samples of a particular type (such as audio or video).

transaction: (1) An object that stores the state and metadata for an item during a crawl.

(2) A single unit of work. If a transaction is successful, all data modifications that were made during the transaction are committed and become a permanent part of the database. If a transaction encounters an error and is canceled or rolled back, all data modifications are erased.

(3) The process of opening or creating an object on a server, and the subsequent committing of changes to the object by calling the required save function, at which time all changes to that instance of the object are either saved to the server, or discarded if a failure occurs before saving is finished successfully. Until successfully saved, changes are invisible to any other instances of the object.

(4) In OleTx, an **atomic transaction**.

transaction manager: The party that is responsible for managing and distributing the outcome of **atomic transactions**. A transaction manager is either a root transaction manager or a subordinate transaction manager for a specified transaction.

transactional message: A **message** sent as part of a transaction. Transaction **messages** must be sent to **transactional queues**.

transactional queue: A **queue** that contains only **transactional messages**.

Transact-SQL: The Microsoft proprietary version of SQL, the structured query language.

Transact-Structured Query Language (T-SQL): A language that contains the commands that are used to manage instances of Microsoft SQL Server, create and manage all objects in an instance of SQL Server, and to insert, retrieve, modify, and delete all data in SQL Server tables. Transact-SQL is an extension of the language that is defined in the SQL standards that are published by the International Standards Organization (ISO) and the American National Standards Institute (ANSI).

transfer protocol: A protocol that governs the transfer of files, Internet messages, and webpages between networked computers. On the Open Systems Interconnection (OSI) Basic Reference Model, these are application layer protocols. Examples of transfer protocols are **Hypertext Transfer Protocol (HTTP)**, **Simple Mail Transfer Protocol (SMTP)**, and **File Transfer Protocol (FTP)**.

transform: (1) An operation that is performed on data to change it from one form to another. Two examples of transforms are compression and encryption.

(2) An algorithm that transforms the size, orientation, and shape of objects that are copied from one **coordinate space** into another. Although a transform affects an object as a whole, it is applied to each point, or to each line, in the object.

transition: The **camera** path and time period that connects one **scene** to another.

transition formula entry: A worksheet option that enables users to enter formulas that use IBM Lotus 1-2-3 syntax.

transition formula evaluation: A setting that enables formulas in a worksheet to be calculated in a manner that is consistent with IBM Lotus 1-2-3.

translation group: A subset of translation items within a **translation job** that share the same base locations for source files and target files.

translation item: A data structure containing information that pertains to the machine translation of a single file, including the locations of the source and target files.

translation job: A set of translation items which are created at the same time and share the same machine translation settings, including target language.

translation rule: A tuple that consists of a regular expression that matches a subset of local numbers and a replacement pattern for it.

Transmission Control Protocol (TCP): A protocol used with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. TCP handles keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

transport address: (1) A 3-tuple that consists of a port, an IPv4 or IPV6 address, and a transport protocol of User Datagram Protocol (UDP) or Transmission Control Protocol (TCP).

(2) The combination of a network address and **port** that identifies a transport-level endpoint, for example an IP address and a **UDP port**. Packets are transmitted from a source transport address to a destination transport address. See [\[RFC3550\]](#) section 3.

transport address pair: The **transport address** of a component of the **local candidate** and the transport address of the same component of the **remote candidate** in a **candidate pair**.

Transport Layer Security (TLS): A security protocol that supports confidentiality and integrity of messages in client and server applications communicating over open networks. **TLS** supports server and, optionally, client authentication by using X.509 certificates (as specified in [\[X509\]](#)). **TLS** is standardized in the IETF TLS working group. See [\[RFC4346\]](#).

Traversal Using Relay NAT (TURN): A protocol that is used to allocate a public IP address and port on a globally reachable server for the purpose of relaying media from one **endpoint** (5) to another **endpoint** (5).

trendline: A line that is added to a chart to show the trend of multiple data points in a series. A trendline is used to facilitate regression analysis.

trigger: A change of state (for example, reaching a specific time of day) that signals when a **task** is to run. A **task** runs when any of its **triggers** and all of its **conditions** are satisfied.

trust: (1) The state of accepting another authority's statements for the purposes of authentication and authorization. If domain A trusts domain B, domain A will accept domain B's authentication and authorization statements for principals represented by security principal objects in domain B; for example, the list of groups to which a particular user belongs. As a noun, a trust is the relationship between two domains described in the previous sentence.

(2) To accept another authority's statements for the purposes of **authentication** and **authorization**, especially in the case of a relationship between two domains. If **domain A** trusts **domain B**, **domain A** accepts **domain B**'s **authentication** and **authorization** statements for **principals** represented by **security principal objects** in **domain B**; for example, the list of groups to which a particular user belongs. As a noun, a **trust** is the relationship between two **domains** described in the previous sentence.

(3) The characteristic that one entity is willing to rely on a second entity to execute a set of actions and/or to make a set of assertions about a set of subjects and/or scopes. For more information, see [\[WSFedPRP\]](#) sections 1.4 and 2.

trusted location: (1) A directory with properties that indicate how an application processes documents.

(2) A directory from which files can be opened without being checked by the security features of a Microsoft Office application.

trusted subsystem: A method of communication in which two-way trust is established between two server features. Each server feature communicates with the other feature by using an account that is authorized to perform privileged actions, such as retrieving files and settings.

tunnel: (1) The encapsulation of one network protocol within another.

(2) Establishes a context in which all further method calls or data transfer can be performed between the RDG client and the RDG server. A tunnel is unique to a given combination of a RDG server and RDG client instance. All operations on the tunnel are stateful.

tuple: An ordered grouping of members from different dimensions or hierarchies. A single member is a special case of a tuple and can be used as an expression. Every hierarchy does not have to be represented in a tuple.

TURN candidate: A **candidate** whose transport addresses are TURN-derived transport addresses. See also **Traversal Using Relay NAT (TURN)**.

TURN client: An **endpoint** (5) that generates **Traversal Using Relay NAT (TURN)** request messages.

TURN server: An **endpoint** (5) that receives **Traversal Using Relay NAT (TURN)** request messages and sends TURN response messages. The protocol server acts as a data relay, receiving data on the public address that is allocated to a protocol client and forwarding that data to the client.

twiddled type library: A modified **Automation type library** in which all controls are marked as extensible. A twiddled type library is generated automatically by the Visual Basic Editor when a user adds one or more controls to a document.

twip: A unit of measurement that is used in typesetting and desktop publishing. It equals one-twentieth of a printer's point, or 1/1440 of an inch.

two-variable data table: A data table that consists of two input cells, a row input cell and a column input cell.

Two-Way Method: A **Remote Method** that has a response sent from the implementation of the **Remote Method** back to the caller.

type information: A collection of information that describes the characteristics and capabilities of an object, including the properties, events, and methods for the object.

type library: (1) A binary file that describes the methods, properties, and data structure of a component.

(2) A type collection which defines an **event class** in terms of its **event interfaces**. A type library is specified by using a **type library file**.

type library file: A **path** name that identifies a **type library**.

TypeDescriptor: A type of **MetadataObject** that describes a subset of the structure of a Parameter of a Method of the native API of a line-of-business (LOB) system. A TypeDescriptor can contain TypeDescriptors to form hierarchies that describe Parameters representing complex types, where the leaf TypeDescriptors describe simple or primitive types. A root TypeDescriptor, together with DefaultValues for leaf TypeDescriptors can be used to instantiate an instance of a Parameter value to send to a LOB system to execute a Method.

typeface: The primary design of a set of printed characters such as Courier, Helvetica, and Times Roman. The terms typeface and font are sometimes used interchangeably. A font is the particular implementation and variation of the typeface such as normal, bold, or italics. The distinguishing characteristic of a typeface is often the presence or absence of serifs.

type-length-value (TLV): (1) A method of organizing data that involves a Type code (16-bit), a specified length of a Value field (16-bit), and the data in the Value field (variable).

(2) A property of a network interface, so named because each property is composed of a Type field, a Length field, and a value.

(3) Information element encoded within [MS-PEAP]. Type and length fields are a fixed size (that is, 1 to 4 bytes), and the value field is variable. "Type" indicates what kind of field is encoded; "Length" indicates the size of "Value"; "Value" defines the data portion of the **TLV** element.

TypeReflector: A unit of **business logic** (2) that converts data structures between the type system of the protocol client and the native type system of a line-of-business (LOB) system.

23 U

UI culture: The language that is used to display strings and graphical elements in a user interface.

UNC volume: A storage device that is accessible by network protocols and addressed in the standard Universal Naming Convention format, for example, "\\Server Name\Share Name".

uncustomized: A condition of a document whose content is stored in a location other than the content database. If a document is uncustomized, the front-end web server determines the location of the content by using the SetupPath value for the document. Also referred to as ghosted.

unhosted: (1) See **customized** (1).

(2) See **customized** (2).

unicast: (1) A delivery method used by media servers for providing content to connected clients in which each client receives a discrete stream that no other client has access to.

(2) A style of resource location or a data transmission in which a client makes a request to a single party.

(3) The process of sending traffic to a unique address. Unicast routing is the process of forwarding unicasted traffic from a source to a **destination** on an internetwork.

Unicode: (1) A character encoding standard developed by the Unicode Consortium that represents almost all of the written languages of the world. The Unicode standard provides three forms (UTF-8, UTF-16, and UTF-32) and seven schemes (**UTF-8**, **UTF-16**, UTF-16 BE, UTF-16 LE, UTF-32, UTF-32 LE, and UTF-32 BE).

(2) A character encoding standard developed by the Unicode Consortium that represents almost all of the written languages of the world. The **Unicode** standard [\[UNICODE5.0.0/2007\]](#) provides three forms (UTF-8, UTF-16, and UTF-32) and seven schemes (UTF-8, UTF-16, UTF-16 BE, UTF-16 LE, UTF-32, UTF-32 LE, and UTF-32 BE).

(3) The set of characters as defined by [\[UNICODE5.0.0/2007\]](#) that is encoded in UCS-2.

Unicode character: Unless otherwise specified, a 16-bit UTF-16 code unit.

Unicode code point: Any value in the Unicode codespace, which is a range of integers from "0" to "10FFFF16". Each code point is a unique positive integer that maps to a specific character.

Unicode string: A **Unicode** 8-bit string is an ordered sequence of 8-bit units, a **Unicode** 16-bit string is an ordered sequence of 16-bit code units, and a **Unicode** 32-bit string is an ordered sequence of 32-bit code units. In some cases, it may be acceptable not to terminate with a terminating null character. Unless otherwise specified, all **Unicode strings** follow the **UTF-16LE** encoding scheme with no Byte Order Mark (BOM).

Unified Communications: A system that integrates platforms for communications including email, voice mail, telephony, instant messaging, and voice and video conferencing.

Uniform Resource Identifier (URI): A string that identifies a resource. The URI is the Web service addressing mechanism defined in Internet Engineering Task Force (IETF) Uniform Resource Identifier (URI): Generic Syntax [\[RFC3986\]](#).

Uniform Resource Locator (URL): A string of characters in a standardized format that identifies a document or resource on the World Wide Web. The format is as specified in [\[RFC1738\]](#).

Uniform Resource Name (URN): (1) A string that identifies a persistent Internet resource, as described in [\[RFC2141\]](#). A URN can provide a mechanism for locating and retrieving a schema file that defines a specific namespace. Although a URL can provide similar functionality, a URN can refer to more than one URL and is not location-dependent.

(2) This term is used as specified in [\[RFC1737\]](#).

unique identifier (UID): A pair consisting of a **GUID** and a version sequence number to identify each resource uniquely. The UID is used to track the object for its entire lifetime through any number of times that the object is modified or renamed.

Universal Data Connection (.udc, .udcx) file: An **XML** file that has a .udc or .udcx file name extension that contains user credentials and other authentication information that is used to connect to a data source.

universal group: An **Active Directory group** that allows **user objects**, **global groups**, and **universal groups** from anywhere in the **forest** as members. A **group object** g is a **universal group** if and only if GROUP_TYPE_UNIVERSAL_GROUP is present in g! groupType. A security-enabled universal group is valid for inclusion within ACLs anywhere in the **forest**. If a **domain** is in **mixed mode**, then a **universal group** cannot be created in that **domain**. See also **domain local group**, **security-enabled group**.

Universal Naming Convention (UNC): A string format that specifies the location of a resource. For more information, see [\[MS-DTYP\]](#) section 2.2.57.

universal serial bus (USB): An external bus that supports Plug and Play installation. It allows devices to be connected and disconnected without shutting down or restarting the computer.

universally unique identifier (UUID): A 128-bit value. UUIDs can be used for multiple purposes, from tagging objects with an extremely short lifetime, to reliably identifying very persistent objects in cross-process communication such as client and server interfaces, manager entry-point vectors, and **RPC** objects. UUIDs are highly likely to be unique. UUIDs are also known as a **globally unique identifiers (GUIDs)** and these terms are used interchangeably in the Microsoft protocol technical documents (TDs). Interchanging the usage of these terms does not imply or require a specific algorithm or mechanism to generate the UUID. Specifically, the use of this term does not imply or require that the algorithms described in [\[RFC4122\]](#) or [\[C706\]](#) must be used for generating the UUID.

unmarshal: (1) The process of deserializing one or more data structures from an octet stream using a specific transfer syntax (for example, unmarshaling a 32-bit integer).

(2) In **remote procedure call (RPC)**, the process of decoding one or more data structures from an octet stream using a specific **RPC** Transfer Syntax.

up bar: See **up-down bar**.

update: (1) An add, modify, or delete of one or more objects or attribute values. See **originating update**, **replicated update**.

(2) The combination of **metadata** and associated **content** for a software update. An **update** is identified by a **GUID**.

(3) The set of metadata pertaining to a file or file deletion. The main fields in an update consist of the **unique identifier (UID)**, **global version sequence number (GVSN)**, file name, file attributes, and flags indicating whether the update is for an existing file, or for a file deletion.

UPDATE: The set of metadata pertaining to a file or file deletion. The main fields in an update consist of the **unique identifier (UID)**, global version sequence number (GVSN), file name, file attributes, and flags indicating whether the update is for an existing file, or for a file deletion.

update server: A computer that implements the Windows Update Services: Server-Server Protocol or the Windows Server Update Services: Client-Server Protocol to provide **updates** to **client computers** and other **update servers**.

Updater: A type of **MethodInstance** that can be called to update an EntityInstance identified by a specified EntityInstanceId. The set of **Fields** (4) that is required to update the EntityInstance is referred to as the Updater View.

up-down bar: A vertical bar that highlights the difference between data points in a line chart that contains more than one data series.

upgrade evaluation site collection: A copy of the current **site collection**, used to evaluate the functionality of a site collection after it is upgraded.

URI fragment: The portion of a **Uniform Resource Identifier (URI)** that allows indirect identification of a secondary resource by reference to a primary resource and additional identifying information, as described in [\[RFC3986\]](#). A fragment component is indicated by a number sign (#) and is terminated by the end of the URI.

URI query: The portion of a **Uniform Resource Identifier (URI)** that, in conjunction with the data in the path component, identifies a resource within the scope of a URI's scheme and naming authority, if any, as described in [\[RFC3986\]](#). A query component is indicated by the first question mark (?) character and is terminated by a number sign (#) or the end of the URI.

URI scheme: The portion of a **Uniform Resource Identifier (URI)** that refers to a specification for assigning identifiers within the URI, as described in [\[RFC3986\]](#).

URL encode: The process of encoding characters that have reserved meanings for a **Uniform Resource Locator (URL)**, as described in [\[RFC1738\]](#).

URL moniker: A Component Object Model (COM) object that stores a **Uniform Resource Locator (URL)** as a string, based on either a full URL or the combination of a **base URL** and a partial URL string.

URL space: A list of **Uniform Resource Locators (URLs)** that contains information about the links from each URL to other URLs.

URL zone: A specific base **Uniform Resource Locator (URL)** that can be used to access a resource within a **web application** (1). A web application can have multiple URL zones.

user: (1) A person who employs a **web browser requestor** to access a **WS resource**.

(2) The real person who has a member account. The user is **authenticated** by being asked to prove knowledge of the secret password associated with the user name.

user account directory path: A string representation of the Lightweight Directory Access Protocol (LDAP) distinguished name for an AD DS container. It defines a set of users, as described in [\[RFC4514\]](#).

user agent: An HTTP user agent, as specified in [\[RFC2616\]](#).

user agent client (UAC): A logical entity that creates a new **request**, and then uses the **client** transaction state machinery to send it. The role of **UAC** lasts only for the duration of that transaction. In other words, if a piece of software initiates a **request**, it acts as a **UAC** for the duration of that transaction. If it receives a **request** later, it assumes the role of a **user agent server (UAS)** for the processing of that transaction.

user agent server (UAS): A logical entity that generates a response to a **Session Initiation Protocol (SIP)** request. The response either accepts, rejects, or redirects the request. The role of the UAS lasts only for the duration of that transaction. If a process responds to a request, it acts as a UAS for that transaction. If it initiates a request later, it assumes the role of a **user agent client (UAC)** for that transaction.

user code: Managed code that can be uploaded to a site by a site collection administrator, without approval from the server farm administrator. It cannot access code or data on other site collections.

User Datagram Protocol (UDP): The connectionless protocol within TCP/IP that corresponds to the transport layer in the ISO/OSI reference model.

user display name: A **user profile** property that contains the preferred name of a user. See also **display name**.

user identifier: An integer that uniquely identifies a **security principal** (2) as distinct from all other **security principals** (2) and site groups within the same site collection.

user information list: A list that contains items, each of which represents a **security principal** (2) in a site collection. Each site collection has only one such list and it resides in the top-level site of the site collection.

user interface (UI) version: A single 4-byte integer that stores the version number that appears as a document version number in the user interface. The lower 9 bits correspond to the minor version number of the displayed version. The remaining 23 bits correspond to the major version number of the displayed version. See also **displayed version**.

user name: A unique name that identifies a specific user account. The user name of an account is unique among the other group names and user names within its own domain or workgroup.

user object: An object of class user. A user object is a security principal object; the principal is a person or service entity running on the computer. The shared secret allows the person or service entity to authenticate itself, as described in ([MS-AUTHSOD] section 1.1.1.1).

user principal name (UPN): A user account name (sometimes referred to as the user logon name) and a domain name that identifies the domain in which the user account is located. This is the standard usage for logging on to a Windows domain. The format is: someone@example.com (in the form of an email address). In **Active Directory**, the userPrincipalName **attribute** (2) of the account object, as described in [\[MS-ADTS\]](#).

user profile: A collection of properties that pertain to a specific person or entity within a portal site.

user profile import: The process of importing records from a **directory service (DS)** to a user profile store.

user profile privacy policy: A set of rules that governs all interactions with user profiles.

User Profile Service: A data source that stores, provides, and applies information about users.

user profile store: A database that stores information about each user profile.

User-Agent header: An HTTP request-header field, as described in [\[RFC2616\]](#). It contains information about the **user agent** that originated a request.

user-agent string: A string that identifies the protocol client that is initiating a request, as described in [\[RFC2616\]](#).

UserContextFilter: A **FilterDescriptor** type that is used when querying a line-of-business (LOB) system. Its value can be set automatically by a protocol client to the identity of the user who is calling the LOB system. This value can then be used by the LOB system to authorize and filter the results that are returned.

UserCultureFilter: A **FilterDescriptor** type that is used when querying a line-of-business (LOB) system. Its value specifies the locale that is used by the application initiating the call.

user-defined function (UDF): A function that is coded in a VBA module, macro sheet, **add-in**, or **Excel Linked Library (XLL)**. A UDF can be used in formulas to return values to a worksheet, similar to built-in functions.

UsernameCredentialFilter: A **FilterDescriptor** type that is used when querying a line-of-business (LOB) system and can hold the user name of an account that is defined in that system. When used in conjunction with PasswordCredentialFilter, the LOB system can use its value to restrict access to data.

UserProfileFilter: A **FilterDescriptor** type that is used when querying a line-of-business (LOB) system and whose value can be obtained by examining the current user's profile. The LOB system can use its value to filter the results that are returned.

UTC (Coordinated Universal Time): A high-precision atomic time standard that approximately tracks Universal Time (UT). It is the basis for legal, civil time all over the Earth. Time zones around the world are expressed as positive and negative offsets from UTC. In this role, it is also referred to as Zulu time (Z) and Greenwich Mean Time (GMT). In these specifications, all references to UTC refer to the time at UTC-0 (or GMT).

UTF-16: A standard for encoding **Unicode characters**, defined in the Unicode standard, in which the most commonly used characters are defined as double-byte characters. Unless specified otherwise, this term refers to the UTF-16 encoding form specified in [\[UNICODE5.0.0/2007\]](#) section 3.9.

UTF-16LE: The Unicode Transformation Format - 16-bit, Little Endian encoding scheme. It is used to encode **Unicode** characters as a sequence of 16-bit codes, each encoded as two 8-bit bytes with the least-significant byte first.

UTF-8: A byte-oriented standard for encoding **Unicode characters**, defined in the Unicode standard. Unless specified otherwise, this term refers to the UTF-8 encoding form specified in [\[UNICODE5.0.0/2007\]](#) section 3.9.

24 V

Valid List: A list of **candidate pairs** that have been validated by **connectivity checks**.

variant type: (1) A data type that can represent any other data type, such as integer, floating-point, single- and double-precision, and object, except fixed-length string type.

(2) An unsigned 16-bit integer that indicates the data type of a variant, as described in [\[MS-OAUT\]](#).

variation label: A hierarchy of **sites** (2), typically in one language and are identified by the **URL** name of the site at the top of the hierarchy and often contain recognizable locale identifiers such as "en-us", "en-uk", and "fr-fr".

variations: An application that facilitates translation and related management processes for **websites** (2) and publishing pages. It can be used to copy content from one site, which is referred to as the source variation site, to one or more other sites, which are referred to as target variation sites. After the content is copied, it can be translated into different languages for those target variation sites.

VBA: See **Visual Basic for Applications (VBA)**.

VBA project: A collection of the modules, class modules, and user forms that are needed to create an application. Modules, class modules, and user forms can be imported into and exported from a project.

vCard: A format for storing and exchanging electronic business cards, as described in [\[RFC2426\]](#).

Vector Markup Language (VML): A system of marking up or tagging two-dimensional vector graphics for publication on the World Wide Web. VML graphics are scalable and editable, and typically require less disk space and less time to download.

version: (1) See **displayed version**, **historical version**, **major version**, and **minor version**.

(2) A snapshot of data members within a model that may correspond to a specific period of time.

(3) A saved collection within a package. Each time a new collection is saved into a package, that new collection becomes the default version that is used by the package.

(4) A number that identifies the specific release and version of RPL. The version is specified by using major, minor, and build fields.

version control: The establishment and maintenance of baselines for documents or list items, and the identification of changes to those baselines. Version control makes it possible to return to a previous baseline. See also **major version** and **minor version**.

version sequence number (VSN): A 64-bit unsigned number. Version sequence numbers are assigned to global version sequence numbers as part of file metadata in monotonic increasing order.

vertical alignment: A formatting setting that specifies how content is positioned within the vertical space of a cell, object, or page. Content can be aligned along the top or bottom edge, or distributed evenly across the vertical space.

vertical indent: An indent that is used in a cell to adjust cell content vertically.

vertical text: Text that is rendered vertically in a cell.

video container: A data type that stores information needed to display videos on a collaboration server.

video encapsulation: A mechanism for transporting video payload and metadata in **Real-Time Transport Protocol (RTP)** packets.

video frame: A single still image that is shown as part of a quick succession of images in a video.

view: (1) See **form view** (Microsoft InfoPath), **list view** (SharePoint Products and Technologies), or **View** (Microsoft Business Connectivity Services).

(2) A subset of the **routing table** and contains a group of related routes (for example, **multicast** routes). **Views** are sometimes called routing information bases (RIBs).

View: A set of **Fields** (4) of an **Entity**, or the schema of an Entity. An Entity can have several Views, each consisting of a different set of Fields, but all containing Identifier Fields. Views are associated with **MethodInstances** and define the shape of a MethodInstance's input or output.

view identifier: A GUID that is used to uniquely identify a view.

view session: A **session** (2) that is based on a workbook file and during which the file can be viewed by one or more users. Any changes to the file, such as sorting or filtering data, are not persisted to that file.

view style: A pre-defined, named collection of settings that specify how to lay out data in a list view.

ViewAccessor: A type of **MethodInstance** that can be called to return a different View for a given EntityInstance of a specific Entity, without changing the EntityInstanceId of the EntityInstance.

view-only mode: A display mode in which data in a workbook can only be viewed, sorted, and filtered by users. Users cannot change any of the data in the workbook and any changes to the display of the data are not persisted to the workbook file.

virtual directory: (1) An HTTP URL that represents the root of a location where content can be published administratively.

(2) A URL prefix that corresponds to a physical directory on the **server**.

(3) An HTTP URL that represents the root of a location to which **content** may be published administratively.

virtual key code: (1) A symbolic constant name, hexadecimal value, or mouse or keyboard equivalent that provides a hardware- and language-independent method of identifying keyboard keys. Each virtual key code represents a unique keyboard key and also identifies the purpose of that key. The keyboard driver provides one or more keyboard layouts that maps keyboard scan codes to the appropriate virtual key codes.

(2) A device-independent code assigned to each keyboard key. [MS-TVTT] specifies virtual key codes only of the keyboard keys relevant to remote terminal applications. Valid virtual key code values are specified in section 2.2.1:

virtual private networking (VPN): A private data network that makes use of the public telecommunication infrastructure.

virus scanner: Software that is used to search for and remove computer viruses, worms, and Trojan horses.

visible: A condition of an object that allows it to be displayed in rendered output.

Visual Basic for Applications (VBA): A macro-based programming language that derives from Visual Basic and can be used to customize and extend an application. Unlike Visual Basic, VBA code and macros can be run only from within a host application that supports VBA.

visual best bet: A URL that specifies the address of an image and is assigned to a keyword by a site collection administrator as being relevant for that keyword. See also **best bet**.

VML: See **Vector Markup Language (VML)**.

Voice over IP (VoIP): The use of the Internet Protocol (IP) for transmitting voice communications. VoIP delivers digitized audio in packet form and can be used to transmit over intranets, extranets, and the Internet.

volatile: A condition of a formula in which the formula is calculated every time the workbook is calculated. This is unlike a non-volatile formula, which is calculated only when dependent values are changed.

volume: A group of one or more partitions that forms a logical region of storage and the basis for a file system. A **volume** is an area on a storage device that is managed by the file system as a discrete logical storage unit. A partition contains at least one **volume**, and a volume can exist on one or more partitions.

volume sequence number (VSN) (for file replication service): A unique sequence number assigned to a change order to order the event sequence in a replica. It is a monotonically increasing sequence number assigned to each change that originates on a given replica member. If one change order has a smaller **volume sequence number (VSN)** than another change order, the change that the first change order represents occurs before the change that the second change order represents.

25 W

wall: An extension of the background of a 3-D chart to create a three-dimensional effect. See also **floor**.

watched cell: A cell whose value is monitored in a separate window while formulas that are associated with the cell are calculated.

waveform (WAV): A file format in which Windows stores sounds as waveforms. Depending on the sampling frequency, whether the sound is monaural or stereo, and whether 8 or 16 bits are used for each sample, one minute of sound can occupy as little as 644 kilobytes or as much as 27 megabytes of storage. Waveform files have a .wav file name extension.

web app: See **web application**.

web application: (1) A container in a configuration database that stores administrative settings and entry-point **URLs** for **site collections**.

(2) A software application that uses **HTTP** as its core communication protocol and delivers information to the user by using web-based languages such as **HTML** and **XML**.

(3) A collection of URLs that share a server execution environment. This collection is defined relative to a root URL. A **web application** runs in response to HTTP requests for the URLs in the collection. The process or processes that run in response to such an HTTP request are termed the application host.

web application identifier: (1) A GUID that identifies a web application.

(2) Each **ASP.NET** application running on a web server is uniquely identified with a **web application identifier**. The **web application identifier** is the virtual path of the web application on the web server. A **web application identifier** is used as part of the identifying key on a state server when storing and retrieving session data for a specific browser session.

web bot: See **bot**.

web browser requestor: An HTTP 1.1 web browser client that transmits protocol messages between an **IP/STS** and a **relying party**.

web control: A server-side component that encapsulates user interface and related functionality.

web discussion: A component and **add-in** that enables users to enter comments about documents and pages without modifying the actual content of those documents or pages.

web discussion comment: An individual comment that is added to a web discussion.

Web Distributed Authoring and Versioning Protocol (WebDAV): The Web Distributed Authoring and Versioning Protocol, as described in [\[RFC2518\]](#) or [\[RFC4918\]](#).

web log: See **blog** (1).

Web Part: A reusable component that contains or generates web-based content such as **XML**, **HTML**, and scripting code. It has a standard property schema and displays that content in a cohesive unit on a webpage. See also **Web Parts Page**.

Web Part chrome: A set of common user interface elements that frame a Web Part within a given zone. The Web Part chrome includes a border, a title bar, and the icons, title text, and verbs menu that appear within the title bar.

Web Part connection: An element in a Web Parts Page that defines a provider-consumer data relationship between two Web Parts. When a Web Parts Page is rendered, data provided by one Web Part can affect how and what is rendered by the other Web Part.

Web Part Page: An **ASP.NET** webpage that includes Web Part controls that enable users to customize the page, such as specifying which information to display. Referred to as Web Parts Page in SharePoint Foundation 2010.

Web Part type identifier: A unique 16-byte value that is assigned to each Web Part type.

Web Part zone: A structured HTML section of a Web Parts Page that contains zero or more Web Parts and can be configured to control the organization and format of those Web Parts.

Web Part zone identifier: A string that identifies a Web Part zone on a Web Parts Page.

Web Part zone index: An integer that specifies the relative position of a Web Part in a Web Part zone. Web Parts are positioned from the smallest to the largest zone index. If two or more Web Parts have the same zone index they are positioned adjacent to each other in an undefined order.

Web Parts Page: An **ASP.NET** webpage that includes **Web Part** controls that enable users to customize the page, such as specifying which information to display. Referred to as **Web Part Page** in Windows SharePoint Services 3.0.

web query: An external data connection that retrieves a table from a website and inserts table data into a workbook.

web server: A server computer that hosts websites and responds to requests from applications.

web service: (1) A unit of application logic that provides data and services to other applications and can be called by using standard Internet transport protocols such as **HTTP**, **Simple Mail Transfer Protocol (SMTP)**, or **File Transfer Protocol (FTP)**. Web services can perform functions that range from simple requests to complicated business processes.

(2) A software entity that responds to SOAP messages ([\[SOAP1.1\]](#), [\[WSDL\]](#)).

web service (WS) resource: A destination HTTP 1.1 web application or an HTTP 1.1 resource serviced by the application. In the context of this protocol, it refers to the application or manager of the resource that receives identity information and assertions issued by an **IP/STS** using this protocol. The **WS resource** is a **relying party** in the context of this protocol. For more information, see [\[WSFedPRP\]](#) sections 1.4 and 2.

web service method: A procedure that is exposed to web service clients as an operation that can be called on the web service. Also referred to as web method.

Web Services Description Language (WSDL): An XML format for describing network services as a set of endpoints that operate on messages that contain either document-oriented or procedure-oriented information. The operations and messages are described abstractly and are bound to a concrete network protocol and message format in order to define an endpoint. Related concrete endpoints are combined into abstract endpoints, which describe a network service. WSDL is extensible, which allows the description of endpoints and their messages regardless of the message formats or network protocols that are used.

web ticket: A security token that is sent by a protocol client to a web application during **authentication** (2). The security token can be included in either the body or the header of an HTTP message.

WebDAV client: A computer that uses **WebDAV**, as described in [\[RFC2518\]](#) or [\[RFC4918\]](#), to retrieve data from a **WebDAV server**.

WebDAV server: A computer that supports **WebDAV**, as described in [\[RFC2518\]](#) or [\[RFC4918\]](#), and responds to requests from **WebDAV clients**.

website: (1) A group of related webpages that is hosted by a server on the World Wide Web or an intranet. Each website has its own entry points, metadata, administration settings, and workflows. Also referred to as site.

(2) A group of related pages and data within a SharePoint site collection. The structure and content of a site is based on a site definition. Also referred to as SharePoint site and site.

Welcome page: A page, such as default.aspx, that can be specified as the default redirect target when users browse to a URL without specifying a **leaf name**.

white space: A character that represents a blank space in typography and is not rendered on a screen.

whitespace: A character that can be found between words, including a space (" "), a carriage return in combination with a line feed (newline), and a tab character.

wide katakana: A non-cursive **character set** (1) that is used to write non-Japanese words phonetically in Japanese. Wide katakana characters are represented with two bytes.

WildcardFilter: A **FilterDescriptor** type that is used when querying a line-of-business (LOB) system. Its value represents a pattern of regular and wildcard characters that is matched against the value of a particular **Field** (4) of the set of EntityInstances. The LOB system returns only those EntityInstances whose Field values match the specified pattern.

Windows code page: A table that relates the character codes (code point values) that are used by an application to keys on a keyboard or to characters on a display. This provides support for **character sets** (1) and keyboard layouts for different countries or regions. Also referred to as character set or charset.

Windows collation name: A string identifier that follows the format of the **Transact-Structured Query Language (T-SQL)** COLLATE clause.

Windows Management Instrumentation (WMI): The Microsoft implementation of **Common Information Model (CIM)**, as specified in [\[DMTF-DSP0004\]](#). WMI allows an administrator to manage local and remote machines and models computer and network objects using an extension of the **CIM** standard..

Windows Metafile Format (WMF): A vector graphics format for Windows-compatible computers. Windows Metafile Format is used primarily as a clip-art format in word-processing documents.

Windows security descriptor: See **security descriptor**.

work: The set of state changes that are applied to **resources** inside an **atomic transaction**.

workbook: A container for a collection of **sheets** (1).

workbook file: A file that contains a byte stream representation of a workbook.

workbook parameter: A single cell that is designated to receive input from users.

workbook stream: See **stream** (1) and **document stream**.

workflow: (1) An automation of business processes that passes business documents and tasks automatically from one user to another for action, according to a defined sequence.

(2) A structured modular component that enables the automated movement of documents or items through a specific sequence of actions or tasks that are related to built-in or user-defined business processes.

workflow association: An association of a workflow template to a specific list or content type.

workflow events: An event that starts or resumes a **workflow instance**.

workflow identifier: A GUID that is used to identify a workflow.

workflow initiation form: An implementation-specific file, typically an ASPX page, that is a part of a workflow. It contains fields and other elements that can be used to initiate a process for a list item, based on the rules and settings in a workflow template that is associated with the list that contains the item.

workflow instance: An instance of a workflow association that performs on a list item the process that is defined in a workflow template.

workflow store: A stored collection of workflow definitions, **workflow associations**, and files that are related to workflows.

workflow subscription: A relationship that determines the data a **workflow** uses and when the workflow will launch.

workflow task: An action or task in a sequence that is related to a built-in or user-defined business process.

workflow template: A definition of operations, the sequence of operations, constraints, and timing for a specific process.

worksheet: A single logical container for a set of tabular data and other objects in a workbook.

worksheet header: The row and column headings of a worksheet.

worksheet image: A chart image that is embedded in a worksheet or chart sheet.

workspace: A set of remote resources, such as **remote applications** and desktops, which are published to end users.

write reservation: A field or condition that is set on a document, workbook, or presentation to help prevent users from modifying it.

write-reservation password: A sequence of characters that need to be entered to modify a document.

WSDL message: An abstract, typed definition of the data that is communicated during a **WSDL operation**, as described in [\[WSDL\]](#).

WSDL operation: A single action or function of a web service. The execution of a WSDL operation typically requires the exchange of messages between the service requestor and the service provider.

WSDL port type: A named set of logically-related, abstract **Web Services Description Language (WSDL)** operations and messages.

WS-Management: A public standard **SOAP**-based protocol for sharing management data among all operating systems, computers, and devices.

26 X

X.509: An ITU-T standard for public key infrastructure subsequently adapted by the IETF, as specified in [\[RFC3280\]](#).

XML: The Extensible Markup Language, as described in [\[XML1.0\]](#).

XML attribute: A name/value pair, separated by an equal sign (=) and included in a tagged element, that modifies features of an element. All XML attribute values are stored as strings enclosed in quotation marks.

XML decode: A process that is used to convert encoded **XML** content to its original form.

XML document: A document object that is well formed, as described in [\[XML\]](#), and might be valid. An XML document has a logical structure that is composed of declarations, elements, comments, character references, and processing instructions. It also has a physical structure that is composed of entities, starting with the root, or document, entity.

XML element: An **XML** structure that typically consists of a start tag, an end tag, and the information between those tags. Elements can have **attributes** (1) and can contain other elements.

XML encode: A process that is used to convert **XML** content from one code to another to use that content without affecting the structure or validity of an **XML document**.

XML fragment: Lines of text that adhere to **XML** tag rules, as described in [\[XML\]](#), but do not have a Document Type Definition (DTD) or schema, processing instructions, or any other header information.

XML Information Set (Infoset): An abstract data set that provides a consistent set of definitions for use in specifications that refer to the information in a well-formed **XML document**, as described in [\[XMLINFOSET\]](#).

XML map: A feature that is used to import data from databases and applications and to map **XML elements** and **attributes** (1) from the associated **XML schema** to cells in a worksheet. The revised **XML** data can then be exported for interaction with other databases and applications.

XML namespace: A collection of names that is used to identify elements, types, and attributes in XML documents identified in a URI reference [\[RFC3986\]](#). A combination of XML namespace and local name allows XML documents to use elements, types, and attributes that have the same names but come from different sources. For more information, see [\[XMLNS-2ED\]](#).

XML namespace prefix: An abbreviated form of an **XML namespace**, as described in [\[XML\]](#).

XML node: The smallest unit of a valid, complete structure in an **XML document**. For example, a node can represent an element, an **attribute** (1), or a text string.

XML Paper Specification (XPS): A Microsoft XML-based document format introduced in Windows Vista. **XML Paper Specification (XPS)** specifies the set of conventions for the use of XML and other widely available technologies to describe the content and appearance of paginated documents. For more information, see [\[MSFT-XMLPAPER\]](#).

XML Path Language (XPath): A language used to create expressions that can address parts of an XML document, manipulate strings, numbers, and Booleans, and can match a set of nodes in the document, as specified in [\[XPath\]](#). XPath models an XML document as a tree of nodes of different types, including element, attribute, and text. XPath expressions can identify the

nodes in an XML document based on their type, name, and values, as well as the relationship of a node to other nodes in the document.

XML schema: A description of a type of **XML document** that is typically expressed in terms of constraints on the structure and content of documents of that type, in addition to the basic syntax constraints that are imposed by **XML** itself. An XML schema provides a view of a document type at a relatively high level of abstraction.

XML Schema (XSD): A language that defines the elements, attributes, namespaces, and data types for **XML** documents as defined by [\[XMLSCHEMA1/2\]](#) and [\[W3C-XSD\]](#) standards. An XML schema uses **XML** syntax for its language.

XML schema definition (XSD): The World Wide Web Consortium (W3C) standard language that is used in defining XML schemas. Schemas are useful for enforcing structure and constraining the types of data that can be used validly within other XML documents. XML schema definition refers to the fully specified and currently recommended standard for use in authoring **XML schemas**.

XML schema document: See **XML schema**.

XMLHttpRequest (XHR): A software component that is used by browser-based scripts to transfer data between a web browser and a web server.

XOR obfuscation: A type of file encryption that helps protect private data by using an exclusive or bitwise operation. This is done by adding a mathematical expression that prevents a simple reverse-engineering process.

XPath expression: An expression that searches an **XML document** and can extract and manipulate data in elements or **attributes** (1) within that document.

XSL: See **Extensible Stylesheet Language (XSL)**.

XSL Transformation (XSLT): A declarative, XML-based language that is used to present or transform XML data. It is designed for use as part of the **Extensible Stylesheet Language (XSL)**.

28 Z

zero-based index: An index in which the first item has an index of "0" (zero).

zone: A domain namespace is divided up into several sections called zones [\[RFC1034\]](#) and [\[RFC2181\]](#). A **zone** represents authority over a portion of the DNS namespace, excluding any subzones that are below delegations.

zoom level: The degree to which a portion of an image, document, or other screen object is made to appear closer or farther away relative to its default appearance. This value is usually expressed as a percentage of the default appearance.

z-order: The rendering order of an object on a z axis.

29 Change Tracking

This section identifies changes that were made to the [MS-OFCGLOS] protocol document between the July 2014 and October 2014 releases. Changes are classified as New, Major, Minor, Editorial, or No change.

The revision class **New** means that a new document is being released.

The revision class **Major** means that the technical content in the document was significantly revised. Major changes affect protocol interoperability or implementation. Examples of major changes are:

- A document revision that incorporates changes to interoperability requirements or functionality.
- The removal of a document from the documentation set.

The revision class **Minor** means that the meaning of the technical content was clarified. Minor changes do not affect protocol interoperability or implementation. Examples of minor changes are updates to clarify ambiguity at the sentence, paragraph, or table level.

The revision class **Editorial** means that the formatting in the technical content was changed. Editorial changes apply to grammatical, formatting, and style issues.

The revision class **No change** means that no new technical changes were introduced. Minor editorial and formatting changes may have been made, but the technical content of the document is identical to the last released version.

Major and minor changes can be described further using the following change types:

- New content added.
- Content updated.
- Content removed.
- New product behavior note added.
- Product behavior note updated.
- Product behavior note removed.
- New protocol syntax added.
- Protocol syntax updated.
- Protocol syntax removed.
- New content added due to protocol revision.
- Content updated due to protocol revision.
- Content removed due to protocol revision.
- New protocol syntax added due to protocol revision.
- Protocol syntax updated due to protocol revision.
- Protocol syntax removed due to protocol revision.

- Obsolete document removed.

Editorial changes are always classified with the change type **Editorially updated**.

Some important terms used in the change type descriptions are defined as follows:

- **Protocol syntax** refers to data elements (such as packets, structures, enumerations, and methods) as well as interfaces.
- **Protocol revision** refers to changes made to a protocol that affect the bits that are sent over the wire.

The changes made to this document are listed in the following table. For more information, please contact dochelp@microsoft.com.

Section	Tracking number (if applicable) and description	Major change (Y or N)	Change type
	Multiple new terms were added to this document.	Y	New content added.
	Multiple terms have additional definitions added.	Y	New content added.