**4. Find and document as much as possible for Remote Desktop Protocol.**

**Remote Desktop Protocol** (**RDP**) is a [proprietary protocol](http://en.wikipedia.org/wiki/Proprietary_protocol) developed by [Microsoft](http://en.wikipedia.org/wiki/Microsoft), which provides a user with a [graphical interface](http://en.wikipedia.org/wiki/Graphical_user_interface) to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software.

Clients exist for most versions of [Microsoft Windows](http://en.wikipedia.org/wiki/Microsoft_Windows) (including [Windows Mobile](http://en.wikipedia.org/wiki/Windows_Mobile)), [Linux](http://en.wikipedia.org/wiki/Linux), [Unix](http://en.wikipedia.org/wiki/Unix), [OS X](http://en.wikipedia.org/wiki/OS_X), [iOS](http://en.wikipedia.org/wiki/IOS), [Android](http://en.wikipedia.org/wiki/Android_(operating_system)), and other modern [operating systems](http://en.wikipedia.org/wiki/Operating_system). RDP servers are built into Windows operating systems; an RDP server for Unix and OS X also exists. By default, the server listens on [TCP](http://en.wikipedia.org/wiki/Transmission_Control_Protocol) [port](http://en.wikipedia.org/wiki/Computer_port_(software)) 3389 and [UDP](http://en.wikipedia.org/wiki/User_Datagram_Protocol) port 3389.

Microsoft currently refers to their official RDP server software as [Remote Desktop Services](http://en.wikipedia.org/wiki/Remote_Desktop_Services), formerly "Terminal Services". Their official client software is currently referred to as [Remote Desktop Connection](http://en.wikipedia.org/wiki/Remote_Desktop_Connection), formerly "Terminal Services Client".

The protocol is an extension of the [ITU-T](http://en.wikipedia.org/wiki/ITU_Telecommunication_Standardization_Sector) [T.128](http://en.wikipedia.org/wiki/T.120) application sharing protocol

Remote Desktop Protocol is based on, and is an extension of, the T-120 family of protocol standards. A multichannel capable protocol allows for separate virtual channels for carrying presentation data, serial device communication, licensing information, highly encrypted data (keyboard, mouse activity), and so on. As RDP is an extension of the core T.Share protocol, several other capabilities are retained as part of the RDP, such as the architectural features necessary to support multipoint (multiparty sessions). Multipoint data delivery allows data from an application to be delivered in "real-time" to multiple parties without having to send the same data to each session individually (for example, Virtual Whiteboards).   
  
In this first release of Windows Terminal Server, however, we are concentrating on providing reliable and fast point-to-point (single- session) communications. Only one data channel will be used in the initial release of Terminal Server 4.0 However, the flexibility of RDP gives plenty of room for functionality in future products.   
  
One reason that Microsoft decided to implement RDP for connectivity purposes within Windows NT Terminal Server is that it provides a very extensible base from which to build many more capabilities. This is because RDP provides 64,000 separate channels for data transmission. However, current transmission activities are only using a single channel (for keyboard, mouse, and presentation data).   
  
Also, RDP is designed to support many different types of Network topologies (such as ISDN, POTS, and many LAN protocols such as IPX, NetBIOS, TCP/IP, and so on). The current version of RDP will only run over TCP/IP but, with customer feedback, other protocol support may be added in future versions.   
  
The activity involved in sending and receiving data through the RDP stack is essentially the same as the seven-layer OSI model standards for common LAN networking today. Data from an application or service to be transmitted is passed down through the protocol stacks, sectioned, directed to a channel (through MCS), encrypted, wrapped, framed, packaged onto the network protocol, and finally addressed and sent over the wire to the client. The returned data works the same way only in reverse, with the packet being stripped of its address, then unwrapped, decrypted, and so on until the data is presented to the application for use. Key portions of the protocol stack modifications occur between the fourth and seventh layers, where the data is encrypted, wrapped and framed, directed to a channel and prioritized.   
  
One of the key points for application developers is that, in using RDP, Microsoft has abstracted away the complexities of dealing with the protocol stack. This allows them to simply write clean, well-designed, well-behaved 32-bit applications, and then the RDP stack implemented by the Terminal Server and its client connections takes care of the rest.   
  
For more information on how applications interact on the Terminal Server and what to be aware of when developing applications for a Windows Terminal Server infrastructure, look at the "Optimizing Applications for Windows NT Server 4.0, Terminal Server Edition" white paper. Four components worth discussing within the RDP stack instance are the Multipoint Communication Service (MCSMUX), the Generic Conference Control (GCC), Wdtshare.sys, and Tdtcp.sys. MCSmux and GCC are part of the International Telecommunication Union (ITU) T.120 family. The MCS is made up of two standards: T.122, which defines the multipoint services, and T.125, which specifies the data transmission protocol. MCSMux controls channel assignment (by multiplexing data onto predefined virtual channels within the protocol), priority levels, and segmentation of data being sent. It essentially abstracts the multiple RDP stacks into a single entity, from the perspective of the GCC. GCC is responsible for management of those multiple channels. The GCC allows the creation and deletion of session connections and controls resources provided by MCS. Each Terminal Server protocol (currently, only RDP and Citrix's ICA are supported) will have a protocol stack instance loaded (a listener stack awaiting a connection request). The Terminal Server device driver coordinates and manages the RDP protocol activity and is made up of smaller components, an RDP driver (Wdtshare.sys) for UI transfer, compression, encryption, framing, and so on, and a transport driver (Tdtcp.sys) to package the protocol onto the underlying network protocol, TCP/IP.   
  
RDP was developed to be entirely independent of its underlying transport stack, in this case TCP/IP. RDP, being completely independent of its transport stack, means that we can add other transport drivers for other network protocols as customers needs for them grow, with little or no significant changes to the foundational parts of the protocol. These are key elements to the performance and extendibility of RDP on the network.

**History**

Every Windows version beginning with Windows XPncludes an installed Remote Desktop Connection (RDC) ("Terminal Services") client (mstsc.exe) whose version is determined by that of the operating system or last applied Windows Service Pack. The Terminal Services server is supported as an official feature on Windows NT 4.0 Terminal Server Edition, [Windows 2000 Server](http://en.wikipedia.org/wiki/Windows_2000_Server), all editions of [Windows XP](http://en.wikipedia.org/wiki/Windows_XP) except Windows XP Home Edition, [Windows Server 2003](http://en.wikipedia.org/wiki/Windows_Server_2003), [Windows Home Server](http://en.wikipedia.org/wiki/Windows_Home_Server), on [Windows Fundamentals for Legacy PCs](http://en.wikipedia.org/wiki/Windows_Fundamentals_for_Legacy_PCs), in [Windows Vista](http://en.wikipedia.org/wiki/Windows_Vista) Ultimate, Enterprise and Business editions, [Windows Server 2008](http://en.wikipedia.org/wiki/Windows_Server_2008) and Windows Server 2008 R2 and on Windows 7 Professional and above.

Microsoft provides the client required for connecting to newer RDP versions for downlevel operating systems. Since the server improvements are not available downlevel, the features introduced with each newer RDP version only work on downlevel operating systems when connecting *to* a higher version RDP server from these older operating systems, and not when using the RDP server in the older operating system.

**Version 4.0**

Based on the [ITU-T](http://en.wikipedia.org/wiki/ITU_Telecommunication_Standardization_Sector) T.128 application sharing protocol (during draft also known as "T.share") from the [T.120](http://en.wikipedia.org/wiki/T.120) recommendation series, the first version of RDP (named version 4.0) was introduced by Microsoft with "Terminal Services", as a part of their product [Windows NT 4.0 Server, Terminal Server Edition](http://en.wikipedia.org/wiki/Windows_NT_4.0). The Terminal Services Edition of NT 4.0 relied on [Citrix](http://en.wikipedia.org/wiki/Citrix_Systems)'s MultiWin technology, previously provided as a part of [Citrix WinFrame](http://en.wikipedia.org/wiki/Citrix_WinFrame) atop Windows NT 3.51, in order to support multiple users and login sessions simultaneously. Microsoft required Citrix to license their MultiWin technology to Microsoft in order to be allowed to continue offering their own terminal services product, then named Citrix MetaFrame, atop Windows NT 4.0. The Citrix provided DLLs included in Windows NT 4.0 Terminal Services Edition still carry a Citrix copyright rather than a Microsoft copyright. Later versions of Windows integrated the necessary support directly. The T.128 application sharing technology was acquired by Microsoft from UK software developer Data Connection Limited.

**Version 5.0**

This version was introduced with [Windows 2000 Server](http://en.wikipedia.org/wiki/Windows_2000#Server_family_functionality), added support for a number of features, including printing to local printers, and aimed to improve network bandwidth usage.

**Version 5.1**]

This version was introduced with [Windows XP Professional](http://en.wikipedia.org/wiki/Windows_XP), included support for 24-bit color and sound. The client is available for [Windows 2000](http://en.wikipedia.org/wiki/Windows_2000), [Windows 9x](http://en.wikipedia.org/wiki/Windows_9x), [Windows NT 4.0](http://en.wikipedia.org/wiki/Windows_NT_4.0). With this version, the name of the client was changed from *Terminal Services Client* to *Remote Desktop Connection*.

**Version 5.2**

This version was introduced with [Windows Server 2003](http://en.wikipedia.org/wiki/Windows_Server_2003), included support for console mode connections, a session directory, and local resource mapping. It also introduces Transport Layer Security (TLS) 1.0 for server authentication, and to encrypt terminal server communications. This version is built into Windows XP Professional x64 Edition and Windows Server 2003 x64 & x86 Editions.

**Version 6.0**

This version was introduced with [Windows Vista](http://en.wikipedia.org/wiki/Windows_Vista) and incorporated support for [Windows Presentation Foundation](http://en.wikipedia.org/wiki/Windows_Presentation_Foundation) applications, [Network Level Authentication](http://en.wikipedia.org/wiki/Network_Level_Authentication), multi-monitor spanning and large desktop support, and support for [TLS 1.0](http://en.wikipedia.org/wiki/Transport_Layer_Security) connections. Version 6.0 client is available for Windows XP SP2, Windows Server 2003 SP1/SP2 (x86 and x64 editions) and Windows XP Professional x64 Edition. Microsoft Remote Desktop Connection Client for Macintosh OS X is also available with support for Intel and PowerPC Mac OS versions 10.4.9 and greater.

**Version 6.1**

This version was released in February 2008 and is included with [Windows Server 2008](http://en.wikipedia.org/wiki/Windows_Server_2008), as well as with Windows Vista Service Pack 1. The client is included with Windows XP Service Pack 3. It is also installable through KB952155 for Windows XP SP2. In addition to changes related to how a remote administrator connects to the "console", this version incorporates new functionality introduced in Windows Server 2008, such as connecting remotely to individual programs and a new Terminal Services Easy Print driver—a new client-side printer redirection system that makes the client's full print capabilities available to applications running on the server, without having to install print drivers on the server.

**Version 7.0**

This version was released to manufacturing in July 2009 and is included with [Windows Server 2008](http://en.wikipedia.org/wiki/Windows_Server_2008) R2, as well as with [Windows 7](http://en.wikipedia.org/wiki/Windows_7) With this release, the server name was also changed from*Terminal Services* to *Remote Desktop Services*. This version incorporates new functionality such as Windows Media Player redirection, bidirectional audio, true multimonitor support, Aero glass support, enhanced bitmap acceleration (which improves user experience over high latency network connections), Easy Print redirection, [Language Bar](http://en.wikipedia.org/wiki/Text_Services_Framework) docking. The RDP 7.0 client is available on Windows XP SP3 and Windows Vista SP1/SP2 through KB969084. RDP 6.1 client and RDP 7.0 client are not supported on Windows Server 2003 x86 and Windows Server 2003 / Windows XP Professional x64 editions. RDP 7.0 clients also do not support connecting to terminal servers running [Windows 2000 Server](http://en.wikipedia.org/wiki/Windows_2000_Server).

Most RDP 7.0 features like Aero glass remoting, bidirectional audio, Windows Media Player redirection, true multiple monitor support and Remote Desktop Easy Print are only available in Windows 7 Enterprise or Ultimate editions.

**Version 7.1**

This version appeared in Windows 7 SP1 and Server 2008 R2 SP1. It adds [RemoteFX](http://en.wikipedia.org/wiki/RemoteFX) functionality.

**Version 8.0**

This version appeared in [Windows 8](http://en.wikipedia.org/wiki/Windows_8) and [Windows Server 2012](http://en.wikipedia.org/wiki/Windows_Server_2012). This version incorporates new functionality such as Adaptive Graphics (progressive rendering and related techniques), automatic selection of TCP or UDP as transport protocol, [multi touch](http://en.wikipedia.org/wiki/Multi_touch) support, DirectX 11 support for vGPU, [USB redirection](http://en.wikipedia.org/w/index.php?title=USB_redirection&action=edit&redlink=1) supported independently of vGPU support, etc. A "connection quality" button is displayed in the RDP client connection bar for RDP 8.0 connections; clicking on it provides a bit of further information about connection, including whether UDP is in use or not.

The RDP 8.0 client and server components are also available as an add-on for Windows 7 SP1. The RDP 8.0 client is also available for Windows Server 2008 R2 SP1, but the server components are not. The add-on requires the [DTLS](http://en.wikipedia.org/wiki/DTLS) protocol to be installed as prerequisite.[[21]](http://en.wikipedia.org/wiki/Remote_Desktop_Protocol#cite_note-kb2592687-21) Even after installing the updates, for the RDP 8.0 protocol to be usable between Windows 7 machines, an extra configuration step is needed using the [Group Policy](http://en.wikipedia.org/wiki/Group_Policy) editor.

A new feature in RDP 8.0 is limited support for RDP session nesting; it only works for Windows 8 and Sever 2012 though, Windows 7 and Sever 2008 (even with the RDP 8.0 update) do not support this feature.

The "shadow" feature from RDP 7, which allowed an administrator to monitor (snoop) on a RDP connection has been removed in RDP 8. The Aero Glass remoting feature (applicable to Windows 7 machines connecting to each other) has also been removed in RDP 8.

Server 2012 can support RDC 6.0 or later.

**Version 8.1**[[edit](http://en.wikipedia.org/w/index.php?title=Remote_Desktop_Protocol&action=edit&section=11)]

This version appeared in [Windows 8.1](http://en.wikipedia.org/wiki/Windows_8.1) and [Windows Server 2012 R2](http://en.wikipedia.org/wiki/Windows_Server_2012_R2). A RDP 8.1 client update exists for Windows 7 SP1 as well, but unlike the RDP 8.0 update for Windows 7, it does not add a RDP 8.1 server component to Windows 7. Furthermore, if RDP 8.0 server functionality is desired on Windows 7, the KB 2592687 (RDP 8.0 client and server components) update must be installed before installing the RDP 8.1 update.

Support for session shadowing was added back in RDP version 8.1. This version also fixes some visual glitches with [Microsoft Office 2013](http://en.wikipedia.org/wiki/Microsoft_Office_2013) when running as a [RemoteApp](http://en.wikipedia.org/wiki/RemoteApp).

Version 8.1 of the RDP protocol also enables a "restricted admin" mode. Logging into this mode only requires knowledge of the hashed password, rather than of its [plaintext](http://en.wikipedia.org/wiki/Plaintext), therefore making a[pass the hash](http://en.wikipedia.org/wiki/Pass_the_hash) attack possible. Microsoft has released an 82-page document explaining how to mitigate against this type of attack

**Features**

* 32-bit color support. 8-, 15-, 16-, and 24-bit color are also supported.
* 128-bit encryption, using the [RC4](http://en.wikipedia.org/wiki/RC4) encryption algorithm, as of Version 6.[[28]](http://en.wikipedia.org/wiki/Remote_Desktop_Protocol#cite_note-28)
* Audio Redirection allows users to run an audio program on the remote desktop and have the sound redirected to their local computer.
* File System Redirection allows users to use their local files on a remote desktop within the terminal session.
* Printer Redirection allows users to use their local printer within the terminal session as they would with a locally or network shared printer.
* Port Redirection allows applications running within the terminal session to access local serial and parallel ports directly.
* The clipboard can be shared between the remote computer and the local computer.

The following features were introduced with the release of RDP 6.0 in 2006:

* Seamless Windows: Remote applications can run on a client machine that is served by a Remote Desktop connection. It is available since RDP 6.[[29]](http://en.wikipedia.org/wiki/Remote_Desktop_Protocol#cite_note-MSRDPERP-29)
* Remote Programs: Application publishing with client-side file type associations.
* Terminal Services Gateway: Enables the ability to use a front-end IIS server to accept connections (over [port 443](http://en.wikipedia.org/wiki/Port_443)) for back-end Terminal Services servers via an [https](http://en.wikipedia.org/wiki/Https) connection, similar to how[RPC](http://en.wikipedia.org/wiki/Remote_procedure_call) over https allows Outlook clients to connect to a back-end Exchange 2003 server. Requires [Windows Server 2008](http://en.wikipedia.org/wiki/Windows_Server_2008)
* [Network Level Authentication](http://en.wikipedia.org/wiki/Network_Level_Authentication)
* Support for remoting the [Aero Glass](http://en.wikipedia.org/wiki/Windows_Aero) Theme (or Composed Desktop), including [ClearType](http://en.wikipedia.org/wiki/ClearType) font smoothing technology.
* Support for remoting of [Windows Presentation Foundation](http://en.wikipedia.org/wiki/Windows_Presentation_Foundation) applications: Compatible clients that have [.NET Framework 3.0](http://en.wikipedia.org/wiki/.net_framework_3) support will be able to display full [Windows Presentation Foundation](http://en.wikipedia.org/wiki/Windows_Presentation_Foundation)effects on a local machine.
* Rewrite of device redirection to be more general-purpose, allowing a greater variety of devices to be accessed.
* Fully configurable and scriptable via [Windows Management Instrumentation](http://en.wikipedia.org/wiki/Windows_Management_Instrumentation).
* Improved bandwidth tuning for RDP clients.
* Support for [Transport Layer Security](http://en.wikipedia.org/wiki/Transport_Layer_Security) (TLS) 1.0 on both server and client ends (can be negotiated if both parties agree, but is not mandatory in a default configuration of any version of Windows).
* Multiple monitor support for allowing one session to use multiple monitors on the client (disables desktop composition)

The following features were introduced with the release of RDP 7.1 in 2010:

* [RemoteFX](http://en.wikipedia.org/wiki/RemoteFX): RemoteFX provides virtualized GPU support and host side encoding and is being shipped as part of Windows Server 2008 R2 SP1.

## Security issues

The RDP protocol in its default configuration is vulnerable to a [man-in-the-middle attack](http://en.wikipedia.org/wiki/Man-in-the-middle_attack). Administrators can enable [transport layer encryption](http://en.wikipedia.org/wiki/Transport_layer_encryption) to mitigate this risk.

RDP sessions are also susceptible to in-memory credential harvesting, which can be used to launch [pass the hash](http://en.wikipedia.org/wiki/Pass_the_hash) attacks.

In March 2012, Microsoft released an update for a critical security vulnerability in the RDP protocol. The vulnerability allowed a Windows computer to be compromised by unauthenticated clients and [computer worms](http://en.wikipedia.org/wiki/Computer_worm).

RDP client version 6.1 can be used to reveal the names and pictures of all users on the RDP Server (no matter which Windows version) in order to pick one, if no username is specified for the RDP connection.

http://en.wikipedia.org/wiki/Remote\_Desktop\_Protocol

<http://support.microsoft.com/>