Remote Desktop Protocol

By Contributors to Wikimedia projects

Published: 2004-05-13 · Archived: 2026-04-05 13:06:12 UTC

From Wikipedia, the free encyclopedia

Remote Desktop Protocol (**RDP**) is a proprietary protocol developed by Microsoft Corporation which provides a user with a graphical interface to connect to another computer over a network connection.[1] The user employs RDP client software for this purpose, while the other computer must run RDP server software.

Several clients exist for most versions of Microsoft Windows (including Windows Mobile but the support has ended), Linux (for example FreeRDP, Krdc, Remmina, Vinagre or rdesktop), Unix, macOS, iOS, Android, and other operating systems. RDP servers are built into the server and professional editions of Windows operating systems but not home editions; an RDP server for Unix and OS X also exists (for example xrdp). By default, the server listens on TCP port 3389[2] and UDP port 3389.[3]

Microsoft currently refers to their official RDP client software as Remote Desktop Connection, formerly "Terminal Services Client".

The protocol is an extension of the ITU-T T.128 application sharing protocol. Microsoft makes some specifications public on their website.[4]

Every server and professional version of Microsoft Windows from Windows XP onward[5] includes an installed Remote Desktop Connection (RDC) ("Terminal Services") client (mstsc.exe) whose version is determined by that of the operating system or by the last applied Windows Service Pack. The Terminal Services server is supported as an official feature on Windows NT 4.0 Terminal Server Edition, released in 1998, Windows 2000 Server, all editions of Windows XP except Windows XP Home Edition, Windows Server 2003, Windows Home Server, on Windows Fundamentals for Legacy PCs, in Windows Vista Ultimate, Enterprise and Business editions, Windows Server 2008 and Windows Server 2008 R2 and on Windows 7 Professional and above. The home versions of Windows do not support RDP.

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.[*clarification needed*]

Based on the ITU-T T.128 application sharing protocol (during draft also known as "T.share") from the 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.[1] The Terminal Services Edition of NT 4.0 relied on Citrix's MultiWin technology, previously provided as a part of 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.[6]

This version was introduced with Windows 2000 Server, added support for a number of features, including printing to local printers, and aimed to improve network bandwidth usage. The RDP clients available through the Windows 2000 Terminal Server Disk Creation Tool is tested and working on even 16 bit Windows 3.1 using 3rd party TCP/IP libraries such as Trumpet WinSock.

This version was introduced with Windows XP Professional and included support for 24-bit color and sound. It is supported on Windows 2000, Windows 9x, and Windows NT 4.0.[7] With this version, the name of the client was changed from *Terminal Services Client* to *Remote Desktop Connection*; the heritage remains to this day, however, as the underlying executable is still named mstsc.exe.

This version was introduced with 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.[8] This version is built into Windows XP Professional x64 Edition and Windows Server 2003 x64 & x86 Editions, and also available for Windows XP as a download.

This version was introduced with Windows Vista and incorporated support for Windows Presentation Foundation applications, Network Level Authentication, multi-monitor spanning and large desktop support, and TLS 1.0 connections.[9] The RDP 6.0 client is available on Windows XP SP2, Windows Server 2003 SP1/SP2 (x86 and x64 editions) and Windows XP Professional x64 Edition through KB925876. 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.

This version was released in February 2008 and is first included with Windows Server 2008 and Windows Vista with Service Pack 1 and later backported to Windows XP with Service Pack 3. The RDP 6.1 client is available on Windows XP SP2, Windows Server 2003 SP1/SP2 (x86 and x64 editions) and Windows XP Professional x64 Edition through KB952155.[10] In addition to changes related to how a remote administrator connects to the "console",[11] this version has new functionality introduced in Windows Server 2008, such as connecting remotely to individual programs and a new client-side printer redirection system that makes the client's print capabilities available to applications running on the server, without having to install print drivers on the server[12][13] also on the other hand, remote administrator can freely install, add/remove any software or setting at the client's end. However, to start a remote administration session, one must be a member of the Administrators group on the server to which one is trying to get connected.[14]

This version was released to manufacturing in July 2009 and is included with Windows Server 2008 R2, as well as with Windows 7.[15] With this release, also changed from *Terminal Services* to *Remote Desktop Services*. This version has new functions such as Windows Media Player redirection, bidirectional audio, multi-monitor support,

Aero glass support, enhanced bitmap acceleration, Easy Print redirection,[16] Language Bar docking. The RDP 7.0 client is available on Windows XP SP3 and Windows Vista SP1/SP2 through KB969084,[17] and is not officially supported on Windows Server 2003 x86 and Windows Server 2003 / Windows XP Professional x64 editions. It is also not officially supported on Windows Server 2008.

Most RDP 7.0 features like Aero glass remote use, bidirectional audio, Windows Media Player redirection, multiple monitor support and Remote Desktop Easy Print are only available in Windows 7 Enterprise or Ultimate editions.[18][19]

Release 7.1 of RDP was included with Windows 7 Service Pack 1 and Windows Server 2008 R2 SP1 in 2010. It introduced RemoteFX, which provides virtualized GPU support and host-side encoding.

This version was released in Windows 8 and Windows Server 2012. This version has new functions such as Adaptive Graphics (progressive rendering and related techniques), automatic selection of TCP or UDP as transport protocol, multi touch support, DirectX 11 support for vGPU, USB redirection supported independently of vGPU support, etc.[20][21] A "connection quality" button is displayed in the RDP client connection bar for RDP 8.0 connections; clicking on it provides further information about connection, including whether UDP is in use or not.[22]

The RDP 8.0 client and server components are available on Windows 7 SP1 and Windows Server 2008 R2 SP1 through KB2592687. The RDP 8.0 client is also available for Windows Server 2008 R2 SP1, but the server components are not. The RDC 8.0 client includes support for session encryption using the TLS 1.2 standard.[23] The add-on requires the DTLS protocol to be installed as prerequisite.[22] After installing the updates, for the RDP 8.0 protocol to be enabled between Windows 7 machines, an extra configuration step is needed using the Group Policy editor.[24]

A new feature in RDP 8.0 is limited support for RDP session nesting; it only works for Windows 8 and Server 2012 though, Windows 7 and Server 2008 R2 (even with the RDP 8.0 update) do not support this feature.[25]

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.[21][22]

This version was released with Windows 8.1 and Windows Server 2012 R2. The RDP 8.1 client, like the RDP 8.0 client, is available on Windows 7 SP1 and Windows Server 2008 R2 SP1 through KB2923545 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 function 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.[26][27]

Support for session shadowing was added back in RDP version 8.1. This version also fixes some visual glitches with Microsoft Office 2013 when running as a RemoteApp.[26]

Version 8.1 of the RDP also enables a "restricted admin" mode. Logging into this mode only requires knowledge of the hashed password, rather than of its plaintext, therefore making a pass the hash attack possible.[28] Microsoft

has released an 82-page document explaining how to mitigate this type of attack.[29]

Version 10.0 of the RDP was introduced with Windows 10 and includes the following new features: AutoSize zoom (useful for HiDPI clients). In addition graphics compression improvements were included utilizing H.264/AVC.[30]

- 32-bit color support. 8-, 15-, 16-, and 24-bit color are also supported.
- Encryption: option of legacy 56-bit or 128-bit RC4 and modern MITM-resistant TLS since version 5.2[8]
- Audio Redirection allows users to process audio on a 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 remote computer and the local computer can share the clipboard.
- Compression goes beyond a framebuffer and takes advantage of font knowledge and tracking of window states (inherited from T.128); later extensions add more content-aware features (e.g MS-RDPCR2).

Microsoft introduced the following features 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.[31]
- 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) for back-end Terminal Services servers via an https connection, similar to how RPC over https allows Outlook clients to connect to a back-end Exchange 2003 server. Requires Windows Server 2008.
- Network Level Authentication
- Support for remoting the Aero Glass Theme (or Composed Desktop), including ClearType font-smoothing technology.
- Support for remoting Windows Presentation Foundation applications: compatible clients that have .NET Framework 3.0 support can display full 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.
- Improved bandwidth tuning for RDP clients.[*citation needed*]
- Support for Transport Layer Security (TLS) 1.0 on both server and client ends (can be negotiated if both parties agree, but 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)

Release 7.1 of RDP in 2010 introduced the following feature:

- RemoteFX: RemoteFX provides virtualized GPU support and host-side encoding; it ships as part of Windows Server 2008 R2 SP1.

The latest version of RDP supports Transport Layer Security (TLS) version 1.1, 1.2 and 1.3 to protect RDP traffic.[32]

Version 5.2 of the RDP in its default configuration is vulnerable to a man-in-the-middle attack. Administrators can enable transport layer encryption to mitigate this risk.[33][34]

RDP sessions are also susceptible to in-memory credential harvesting, which can be used to launch pass the hash attacks.[35]

In March 2012, Microsoft released an update for a critical security vulnerability in the RDP. The vulnerability allowed a Windows computer to be compromised by unauthenticated clients and computer worms.[36]

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.[*citation needed*]

In March 2018 Microsoft released a patch for CVE-2018-0886, a remote code execution vulnerability in CredSSP, which is a Security Support Provider involved in the Microsoft Remote Desktop and Windows Remote Management, discovered by Preempt.[37][38]

In May 2019 Microsoft issued a security patch for CVE-2019-0708 ("BlueKeep"), a vulnerability which allows for the possibility of remote code execution and which Microsoft warned was "wormable", with the potential to cause widespread disruption. Unusually, patches were also made available for several versions of Windows that had reached their end-of-life, such as Windows XP. No immediate malicious exploitation followed, but experts were unanimous that this was likely, and could cause widespread harm based on the number of systems that appeared to have remained exposed and unpatched.[39][40][41]

In July 2019, Microsoft issued a security patch for CVE-2019-0887, a RDP vulnerability that affects Hyper-V.[42]

In April 2025, a security researcher discovered that it is possible to log into accounts through RDP using passwords that have already been revoked. According to Microsoft, this was by design, and not a bug or vulnerability.[43]

Since the release of Remote Desktop Connection, there have been several additional Remote Desktop Protocol clients created by both Microsoft and other parties including Microsoft Remote Desktop, rdesktop, and FreeRDP.

In addition to the Microsoft-created Remote Desktop Services, open-source RDP servers on Unix include FreeRDP (see above), ogon project and xrdp. The Windows Remote Desktop Connection client can be used to connect to such a server. There is also Azure Virtual Desktop which makes use of RDP and is a part of the Microsoft Azure platform.

There is also a VirtualBox Remote Display Protocol (VRDP) used in the VirtualBox virtual machine implementation by Oracle.[44] This protocol is compatible with all RDP clients, such as that provided with Windows but, unlike the original RDP, can be configured to accept unencrypted and password unprotected

connections, which may be useful in secure and trusted networks, such as home or office LANs. By default, Microsoft's RDP server refuses connections to user accounts with empty passwords (but this can be changed with the Group Policy Editor[45]). External and guest authorization options are provided by VRDP as well. It does not matter which operating system is installed as a guest because VRDP is implemented on the virtual machine (host) level, not in the guest system. The proprietary VirtualBox Extension Pack is required.

Microsoft requires third-party implementations to license the relevant RDP patents.[46] As of February 2014, the extent to which open-source clients meet this requirement remains unknown.

Security researchers reported in 2016-17 that cybercriminals were selling compromised RDP servers on underground forums as well as specialized illicit RDP shops.[47][48] These compromised RDPs may be used as a "staging ground" for conducting other types of fraud or to access sensitive personal or corporate data.[49] Researchers further report instances of cybercriminals using RDPs to directly drop malware on computers.[50]

- Comparison of remote desktop software
- Desktop virtualization
- Secure Shell
- SPICE and RFB protocol
- Virtual private server

1. ^ Jump up to: *a b* *Deland-Han. "Understanding Remote Desktop Protocol (RDP) – Windows Server". docs.microsoft.com. Archived from the original on October 17, 2020. Retrieved October 12, 2020.*
2. ^ *"How to change the listening port for Remote Desktop". Microsoft. January 31, 2007. Archived from the original on November 4, 2007. Retrieved November 2, 2007.* Microsoft KB article 306759, revision 2.2.
3. ^ *"Service Name and Transport Protocol Port Number Registry". Internet Assigned Numbers Authority. January 9, 2015. Retrieved January 13, 2015.*
4. ^ *"rdesktop: A Remote Desktop Protocol Client". www.rdesktop.org. Archived from the original on December 1, 2008. Retrieved November 29, 2008.*
5. ^ *Microsoft. "Connecting to another computer Remote Desktop Connection". Archived from the original on January 16, 2013. Retrieved December 22, 2012.*
6. ^ Implementing Collaboration Technologies in Industry, Bjørn Erik Munkvold, 2003; Chapter 7
7. ^ *"Windows XP Remote Desktop Connection software [XPSP2 5.1.2600.2180]". Microsoft.com. August 27, 2012. Archived from the original on September 8, 2010. Retrieved March 11, 2014.*
8. ^ Jump up to: *a b* *"Configuring authentication and encryption". January 21, 2005. Archived from the original on March 18, 2009. Retrieved March 30, 2009.* Microsoft Technet article
9. ^ *"Remote Desktop Connection (Terminal Services Client 6.0)". June 8, 2007. Archived from the original on July 17, 2007. Retrieved June 20, 2007.* Microsoft KB article 925876, revision 7.0.
10. ^ *"Description of the Remote Desktop Connection 6.1 client update for Terminal Services in Windows XP Service Pack 2". microsoft. Archived from the original on August 29, 2008. Retrieved March 11, 2014.*
11. ^ *"Changes to Remote Administration in Windows Server 2008". Terminal Services Team Blog. Microsoft. December 17, 2007. Archived from the original on March 5, 2009. Retrieved February 10, 2008.*
12. ^ *"Terminal Services Printing". TechNet – Windows Server 2008 Technical Library. Agozik-Microsoft. January 10, 2008. Archived from the original on January 21, 2014. Retrieved February 10, 2008.*

13. ^ *"Introducing Terminal Services Easy Print: Part 1 – Remote Desktop Services (Terminal Services) Team Blog – Site Home – MSDN Blogs"*. *Blogs.msdn.com. Archived from the original on February 13, 2014. Retrieved February 13, 2014.*
14. ^ *"Securing Remote Desktop (RDP) for System Administrators | Information Security Office"*. *security.berkeley.edu. Archived from the original on October 12, 2020. Retrieved October 12, 2020.*
15. ^ *"Remote Desktop Connection 7 for Windows 7, Windows XP & Windows Vista"*. *Terminal Services Team Blog. Microsoft. August 21, 2009. Archived from the original on August 27, 2009. Retrieved August 21, 2009.*
16. ^ *"Using Remote Desktop Easy Print in Windows 7 and Windows Server 2008 R2"*. *Blogs.msdn.com. Archived from the original on May 8, 2010. Retrieved March 11, 2014.*
17. ^ *"Announcing the availability of Remote Desktop Connection 7.0 for Windows XP SP3, Windows Vista SP1, and Windows Vista SP2"*. *Blogs.msdn.com. Archived from the original on March 8, 2010. Retrieved March 11, 2014.*
18. ^ *"Aero Glass Remoting in Windows Server 2008 R2"*. *Blogs.msdn.com. Archived from the original on June 27, 2009. Retrieved March 11, 2014.*
19. ^ *"Remote Desktop Connection 7 for Windows 7, Windows XP & Windows Vista"*. *Blogs.msdn.com. Archived from the original on August 27, 2009. Retrieved March 11, 2014.*
20. ^ *"Windows Server 2012 Remote Desktop Services (RDS) – Windows Server Blog – Site Home – TechNet Blogs"*. *Blogs.technet.com. May 8, 2012. Archived from the original on October 5, 2013. Retrieved February 13, 2014.*
21. ^ Jump up to: ***a*** ***b*** *"How Microsoft RDP 8.0 addresses WAN, graphics shortcomings"*. *Searchvirtualdesktop.techtarget.com. Archived from the original on February 9, 2014. Retrieved February 13, 2014.*
22. ^ Jump up to: ***a*** ***b*** ***c*** *"Remote Desktop Protocol (RDP) 8.0 update for Windows 7 and Windows Server 2008 R2"*. *Support.microsoft.com. Archived from the original on October 25, 2012. Retrieved February 13, 2014.*
23. ^ *"Incorrect TLS is displayed - Windows Server"*. *June 5, 2024.*
24. ^ *"Get the best RDP 8.0 experience when connecting to Windows 7: What you need to know – Remote Desktop Services (Terminal Services) Team Blog – Site Home – MSDN Blogs"*. *Blogs.msdn.com. Archived from the original on February 12, 2014. Retrieved February 13, 2014.*
25. ^ *"Running a Remote Desktop Connection session within another Remote Desktop Connection session is supported with Remote Desktop Protocol 8.0 for specific scenarios"*. *Support.microsoft.com. November 2, 2012. Archived from the original on January 17, 2014. Retrieved February 13, 2014.*
26. ^ Jump up to: ***a*** ***b*** *"Update for RemoteApp and Desktop Connections feature is available for Windows"*. *Support.microsoft.com. February 11, 2014. Archived from the original on February 9, 2014. Retrieved March 11, 2014.*
27. ^ *"Remote Desktop Protocol 8.1 Update for Windows 7 SP1 released to web – Remote Desktop Services (Terminal Services) Team Blog – Site Home – MSDN Blogs"*. *Blogs.msdn.com. Archived from the original on February 22, 2014. Retrieved February 13, 2014.*
28. ^ *"New "Restricted Admin" feature of RDP 8.1 allows pass-the-hash"*. *Labs.portcullis.co.uk. October 20, 2013. Archived from the original on February 10, 2014. Retrieved March 11, 2014.*

29. ^ *"Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques"*. *Microsoft.com. Archived from the original on April 21, 2014. Retrieved March 11, 2014.*
30. ^ *"Remote Desktop Protocol (RDP) 10 AVC/H.264 improvements in Windows 10 and Windows Server 2016 Technical Preview"*. *Microsoft.com. Archived from the original on August 17, 2016. Retrieved January 12, 2016.*
31. ^ *"[MS-RDPERP]: Remote Desktop Protocol: Remote Programs Virtual Channel Extension"*. *Msdn.microsoft.com. Archived from the original on April 14, 2012. Retrieved February 13, 2014.*
32. ^ *"[MS-RDPBCGR]: Enhanced RDP Security"*. *April 23, 2024.*
33. ^ *"National Vulnerability Database (NVD) National Vulnerability Database (CVE-2005-1794)"*. *Web.nvd.nist.gov. July 19, 2011. Archived from the original on September 14, 2011. Retrieved February 13, 2014.*
34. ^ *"Configuring Terminal Servers for Server Authentication to Prevent "Man in the Middle" Attacks"*. *Microsoft. July 12, 2008. Archived from the original on November 6, 2011. Retrieved November 9, 2011.*
35. ^ *"Mimikatz and Windows RDP: An Attack Case Study"*. *SentinelOne. June 6, 2019. Archived from the original on October 16, 2020. Retrieved October 12, 2020.*
36. ^ *"Microsoft Security Bulletin MS12-020 – Critical"*. *Microsoft. March 13, 2012. Archived from the original on February 13, 2014. Retrieved March 16, 2012.*
37. ^ *"CVE-2018-0886 – CredSSP Remote Code Execution Vulnerability"*. *microsoft.com. Archived from the original on March 23, 2018. Retrieved March 23, 2018.*
38. ^ *Karni, Eyal. "From Public Key to Exploitation: How We Exploited the Authentication in MS-RDP". Archived from the original on March 23, 2018. Retrieved March 23, 2018.*
39. ^ *Cimpanu, Catalin. "Even the NSA is urging Windows users to patch BlueKeep (CVE-2019-0708)". ZDNet. Archived from the original on September 6, 2019. Retrieved June 20, 2019.*
40. ^ *Goodin, Dan (May 31, 2019). "Microsoft practically begs Windows users to fix wormable BlueKeep flaw". Ars Technica. Archived from the original on July 22, 2019. Retrieved May 31, 2019.*
41. ^ *Warren, Tom (May 14, 2019). "Microsoft warns of major WannaCry-like Windows security exploit, releases XP patches". The Verge. Archived from the original on September 2, 2019. Retrieved June 20, 2019.*
42. ^ *Ilascu, Ionut (7 August 2019). "Microsoft Ignored RDP Vulnerability Until it Affected Hyper-V". Bleeping Computer. Archived from the original on 8 August 2019. Retrieved 8 August 2019.*
43. ^ *Goodin, Dan (April 30, 2025). "Windows RDP lets you log in using revoked passwords. Microsoft is OK with that". Ars Technica. Retrieved May 13, 2025.*
44. ^ *"VirtualBox Manual: 7.1. Remote Display (VRDP Support)". VirtualBox. Archived from the original on November 21, 2019. Retrieved February 27, 2020.*
45. ^ *Bens, Jelle (January 31, 2010). "Jelle Bens: Windows 7 RDP with blank password". Jellebens.blogspot.ru. Archived from the original on May 8, 2013. Retrieved March 11, 2014.*
46. ^ *"Remote Desktop Protocol Licensing Available for RDP 8". Blogs.msdn.com. December 11, 2014. Archived from the original on February 8, 2018. Retrieved February 8, 2018.*
47. ^ *GReAT (June 15, 2016). "xDedic – the shady world of hacked servers for sale". SecureList. Archived from the original on December 15, 2018. Retrieved December 15, 2018.*
48. ^ *Kremez, Vitali; Rowley, Liv (October 24, 2017). ""Ultimate Anonymity Services" Shop Offers Cybercriminals International RDP Servers". Archived from the original on December 15, 2018. Retrieved*

December 15, 2018.

49. ^ *Bisson, David (July 19, 2018). "Dark Web 'RDP Shops' Offer Access to Vulnerable Systems for as Little as $3". Security Intelligence. Archived from the original on December 15, 2018. Retrieved December 15, 2018.*
50. ^ *Ragan, Steve (July 19, 2018). "Samsam infected thousands of LabCorp systems via brute force RDP". CSO Online. Archived from the original on December 15, 2018. Retrieved December 15, 2018.*

- Remote Desktop Protocol – from Microsoft's Developer Network
- Understanding the Remote Desktop Protocol – from support.microsoft.com
- MS-RDPBCGR: Remote Desktop Protocol: Basic Connectivity and Graphics Remoting Specification – from Microsoft's Developer Network

---