Remote connections

Previously, you learned about the fundamentals of remote access. In this reading, you will learn about various methods and tools for connecting remotely. You will also learn about some of the security risks related to using remote connections.

Remote connections can be used by IT Support professionals to troubleshoot remote systems. Remote systems may include laptops, PCs, workstations, servers, data center machines, and other IT equipment that supports remote access. Additionally, remote connections can be used for file transfers and terminal emulations. IT Support professionals often use remote access software to save time by eliminating the need to travel to the computer system's location.

Remote access software can also be used for remote and flexible work arrangements, which have been increasing in popularity in recent years. Numerous organizations have developed remote, hybrid, and flexible work opportunities to give employees the option to work from home. Through these arrangements, employers and employees have discovered the benefits of remote work. Employees save time and money by avoiding the commute to work. Employees also report an improvement in their work-life balance. Employers can save on the costs of maintaining physical offices. Employers can opt to expand their hiring pool far beyond their physical locations by hiring talent in other cities, regions, states, or even countries.

Multiple surveys have revealed that up to 95% of employers and employees in the United States would like to keep remote, hybrid, and/or flexible work options permanently. Recently, Microsoft reported that 66% of employers around the world are adapting their workplaces to support hybrid work models (see the Resources section at the bottom of this reading for more information). Given this workplace transformation, organizations are likely to ask IT Support professionals to design, configure, manage, and/or troubleshoot remote connections for business networks.

Remote access software for IT management

Unlike RDP and VPN, there are some types of remote access software that are typically used only by IT management and other computer support professionals. These remote applications help IT Support teams manage and monitor large networks more efficiently.

- **Secure Shell or Secure Socket Shell (SSH):** SSH is a network protocol and suite of tools that can be used to establish a secure connection between a computer and a private network over the internet. SSH is included with Linux/Unix and Mac Server operating systems. SSH provides identity and access management protocols through robust password authentication and public key authentication. SSH also encrypts data transmissions over the internet. Sessions are established by using an SSH client application to connect to an SSH server. For security, SSH keys are used to provide single sign-on (SSO) services and to automate access to servers for running scripts, backups, and configuration tools. SSH is primarily used by IT Support professionals to remotely manage file transfers and terminal emulators on Linux/Unix systems. For example, IT Support staff can use the SSH network protocol tool to establish an encrypted tunnel from their computer to a remote server over a network. The SSH file transfer tool can then be used to transfer a file, like a firmware update package, to the remote server. Finally, the SSH terminal emulator can be used to issue command lines to install the firmware onto the remote server.
- **Remote Monitoring and Management (RMM):** RMM is used by IT Support professionals to remotely monitor and manage information systems. Implementing RMM involves installing an RMM agent on each endpoint within a network, including servers, workstations, and mobile devices. The agents then send periodic status reports about the health of each endpoint to IT Support staff. RMM tools also help IT Support professionals proactively maintain the network by facilitating the remote installation of security patches and updates. If a problem occurs on an endpoint, the RMM agent will create a ticket, classify the problem type and severity, and then forward the ticket to IT Support staff. RMM systems enable IT Support providers to improve efficiency in information systems management. IT Support providers can manage and even automate routine maintenance for multiple endpoints simultaneously through a unified RMM dashboard.

Remote access software

End user remote connections to business networks can be established using remote access software. IT professional can also use this software to manage business networks remotely. There are multiple options available for remote access software, each with their own benefits and disadvantages. The following list provides a few options for various uses, workforce sizes, and network environments:

- **Remote Desktop Protocol (RDP):** RDP is a remote protocol developed by Microsoft. It is compatible with most Windows and Mac operating systems. An RDP solution may work well for flexible or hybrid work environments where employees split their work schedule between being physically in the office and working remotely. With RDP, end users can remotely access the physical computers housed at their offices, in addition to the desktop, software, files, and network access available to those systems. IT Support professionals can also use RDP software to troubleshoot, repair, patch and update end user computers without needing to be in the same room as the PCs.

RDP works by encrypting and transmitting the user's desktop, data, keystrokes, and mouse movements over the internet. Users may notice delayed responses to their keystrokes and mouse activity during the transmission process. RDP creates a dedicated network channel and uses network port 3389 to transmit this information using the TCP/IP protocol standard. Unfortunately, using a single dedicated port creates

a security weakness that cybercriminals can target for on-path attacks. Further, RDP does not enforce strong sign-in credentials, which leaves RDP systems vulnerable to stolen credential and brute force attacks.

- **Virtual Private Network (VPN):** VPNs are often described as private tunnels through the public internet. Organizations can use VPNs to create encrypted connections over the internet between remote computers or mobile devices and the organizations' networks. VPNs can be implemented as software running on networked servers or on network routers with VPN features enabled. When the employees remotely connect to their VPN, they are able to access their organization's network as though they were physically in the office, eliminating the need to travel to the office in person. VPNs work well for small to medium sized organizations, but may not be adequate for large enterprises. Additionally, VPNs might not be the right solution for organizations that need to provide restricted levels of network access to groups like contractors or vendors.

Third party tools

- **Integrated video conferencing, screen sharing, and desktop management apps:** Video conferencing apps like Google Meet, Zoom, Microsoft Teams, Skype, etc. are growing in popularity as remote work tools. Video conferencing allows two or more people to meet "face-to-face" in a virtual environment. Some video conferencing apps also offer screen sharing tools, remote desktop control, polling tools, text messaging, meeting transcripts, webinar management options, the ability to record meetings, and more. The growing popularity of these tools for remote work has also invited an increase in related security attacks. Fortunately, the major providers of video conferencing software continuously update and patch their applications in response to these attacks.
- **File sharing and transfer platforms:** Cloud storage platforms, like Google Drive, Microsoft OneDrive, and Dropbox, have largely replaced file transfer protocol (FTP) tools. File sharing through a cloud platform provides the benefits of asynchronous file transfers, file transfer and data encryption, customizable security and authentication settings, and the ability to file share with multiple users simultaneously. File owners can share individual files, folders, or entire drives. However, cloud storage might not be an appropriate option for organizations affected by certain privacy laws, regulations, or other security concerns. These organizations can still use FTP applications based on SSH or HTTPS protocols for secure file transfers over the internet.

Resources for more information

- How to use Remote Desktop - Walkthrough from Microsoft on how to use Remote Desktop to connect to a remote Windows 10 or 11 computer from a device running Windows, Android, or iOS.
- The Next Great Disruption Is Hybrid Work—Are We Ready? - Microsoft's Work Trend Index report on global workplace trends regarding hybrid work environments.
- Remote Work Stats & Trends: Navigating Work From Home Jobs - Provides findings from multiple surveys about attitudes and growing prevalence of remote work