Ch 4: Network Management Tools

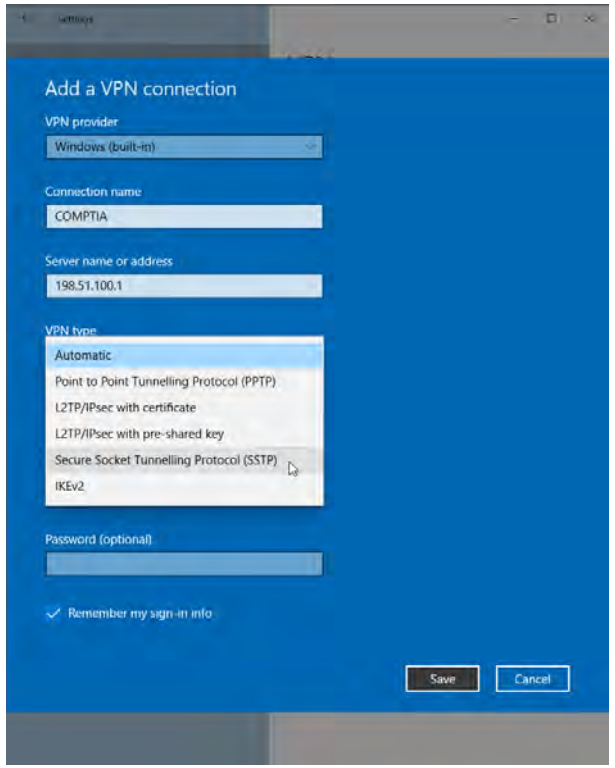
Covered in CH 5 &6

Topic A: Network Connectivity

- PAN (personal area network): consists of personal devices such as a cell phone and laptop
- LAN (local area network): group of computers connected by cabling and one or more network switches that are all installed at a single location.
- WLAN (wireless local area network): uses radios and antennas for data transmission and reception. WIFI
- MAN (metropolitan area network): covers a large campus or city
- WAN (wide area network): covers a large geographic area and is made up of small networks
- SAN (Storage Area Network) is a specialized, high-speed network that provides network access to storage devices.

WWAN & VPN

- Wireless wide area network (WWAN)
  - Cellular adapter and SIM card
  - Metered connections and limitations
- Virtual private network (VPN)
  - Protocol support in Windows versus third-party clients
  - Remote network address
  - Connecting and disconnecting

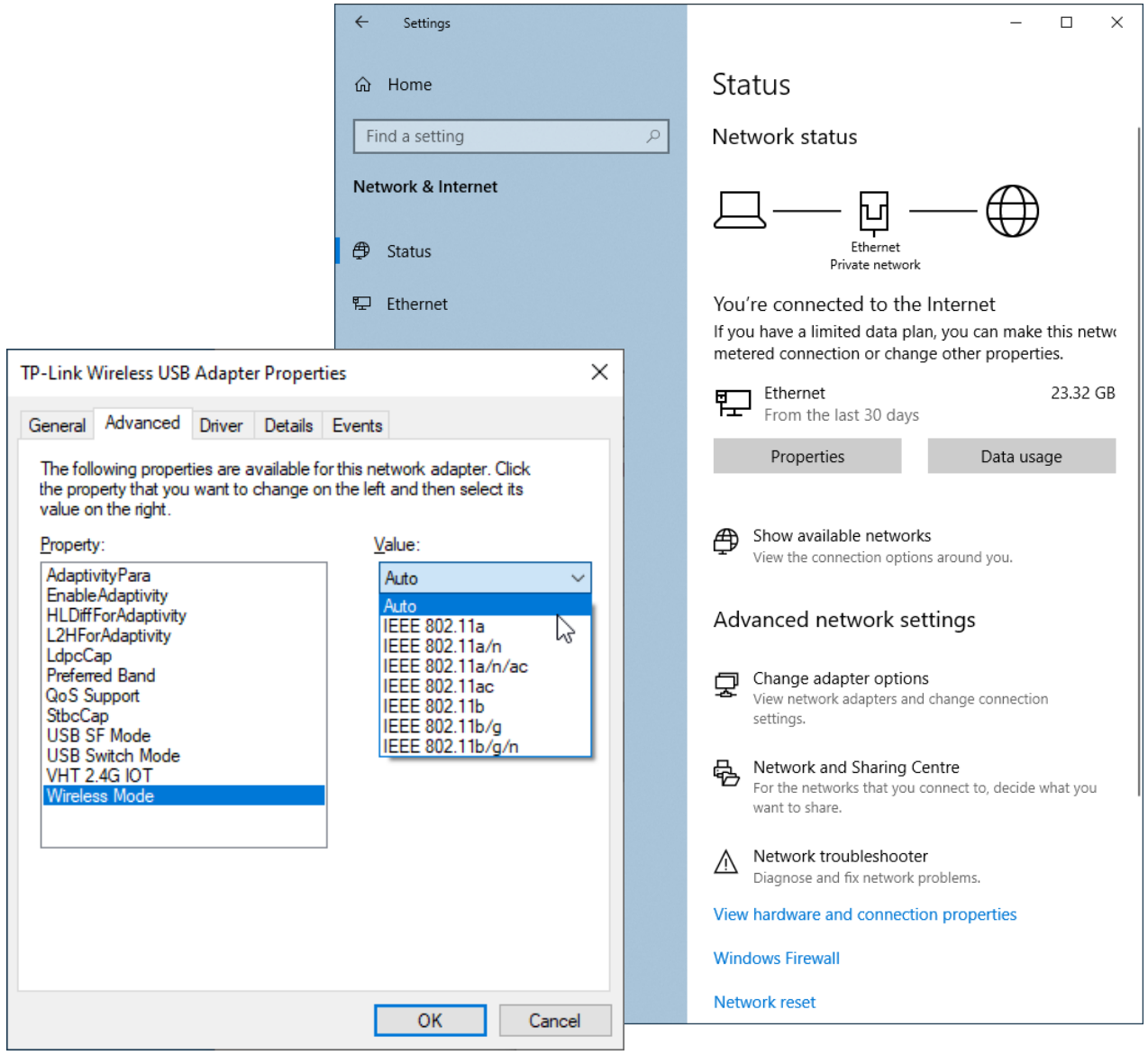


IP Addressing

- Default gateway
- Domain Name System (DNS) settings
- Static versus dynamic configuration
- Internet Protocol (IP) addressing scheme
- IPv4 address
- IPv6 address

Connection Types

- Wired (Ethernet)
  - Device Manager properties
- Wireless
  - Network name/service set ID (SSID) list
  - Joining a non-broadcast network
  - Adapter properties
    - Standards support, transmit power, and roaming aggressiveness

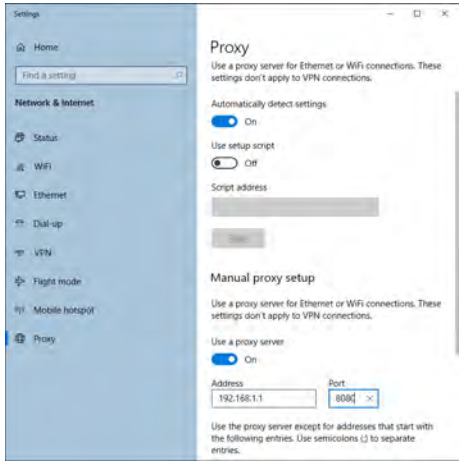


Proxy Settings

- A proxy server can improve both performance and security. PCs pass Internet requests to the proxy server, which forwards them to the Internet.

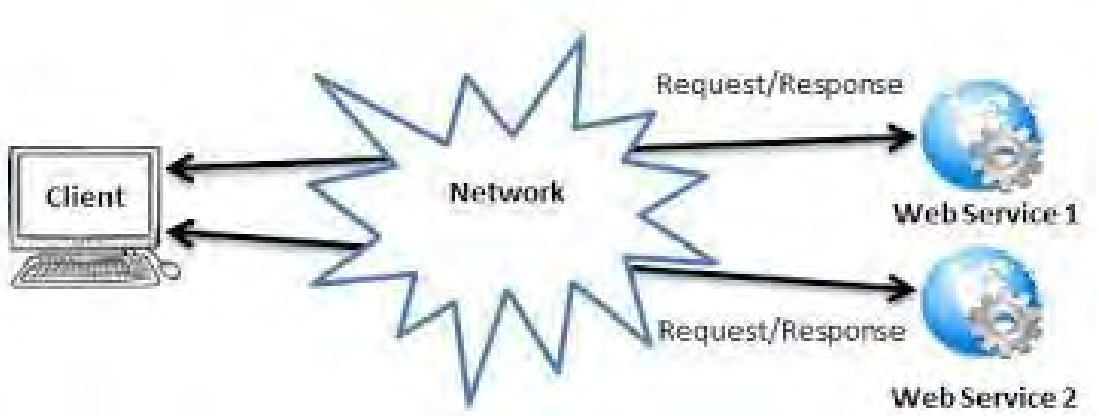
- Clients connect to Internet via server
  - Content filtering and security
  - Caching to improve performance
  - An intercepting or transparent proxy does not require any client setup (autoconfiguring)
  - If neither of these cases apply, each client must
  - Manual setup IP address and TCP port to use to forward traffic must be entered

These proxy settings are configured via Network & Internet settings

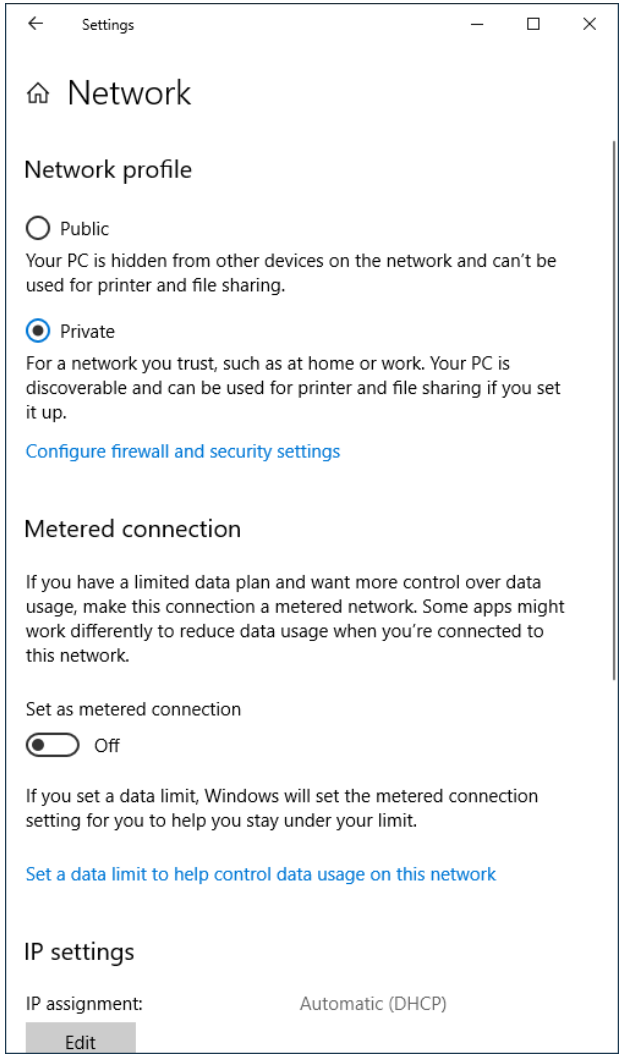


Windows Client Configuration

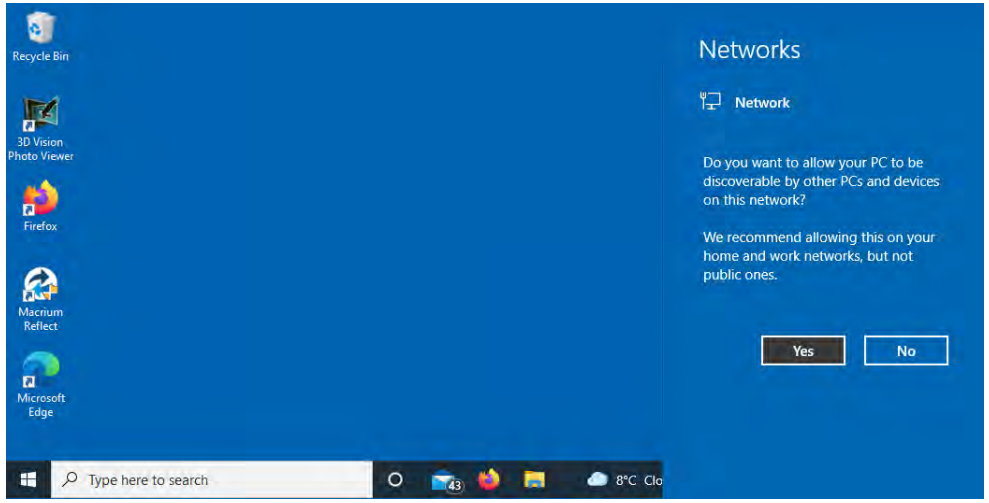
- Clients, protocols, and services
- IPv4 properties
  - Obtain an IP address automatically (DHCP)
  - Static configuration



Location Services



- Public versus private
- Network Location Awareness
- Controls whether host discovery and sharing is enabled
- Network navigation in File Explorer

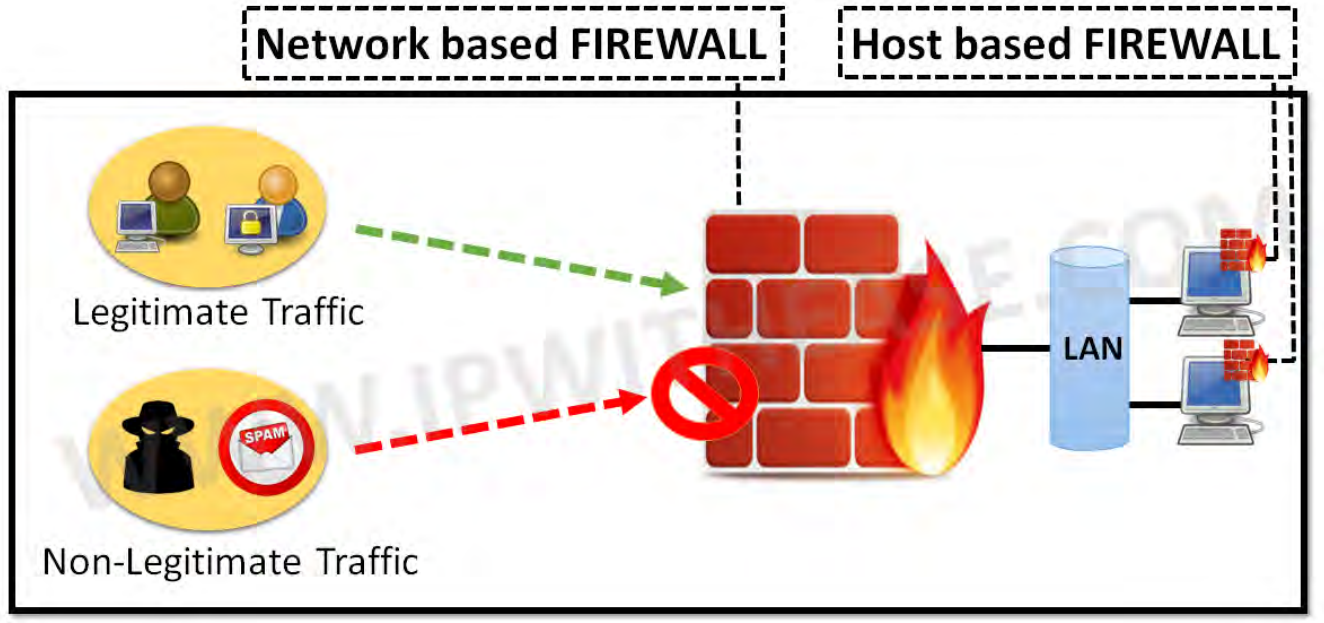


Firewalls

Many types and implementations

- Primary distinction:
  Network firewall: Inline on the network / Inspects all traffic

- Host firewall: Installed on host / Inspects traffic to that host

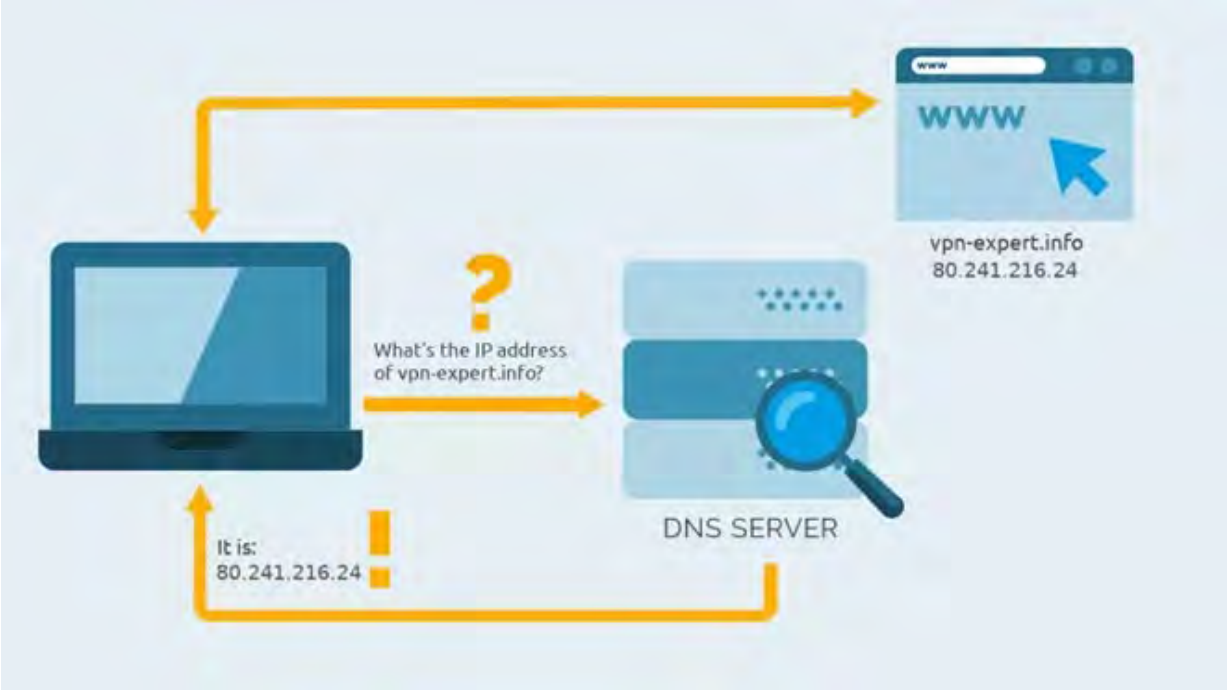


Network Troubleshooting

- Windows includes several utilities you can use to troubleshoot networking problems:
  - ping
  - ipconfig
  - nslookup
  - tracert
  - Two net commands
  - netstat

Network Troubleshooting

- Windows adapter error states
  - Limited connectivity versus No Internet
- ipconfig Command
  - (/all)
  - DHCP (/release and /renew)
  - DNS cache (/displaydns and /flushdns)
- Hostname Command
- Network reset



Network Ports Troubleshoot

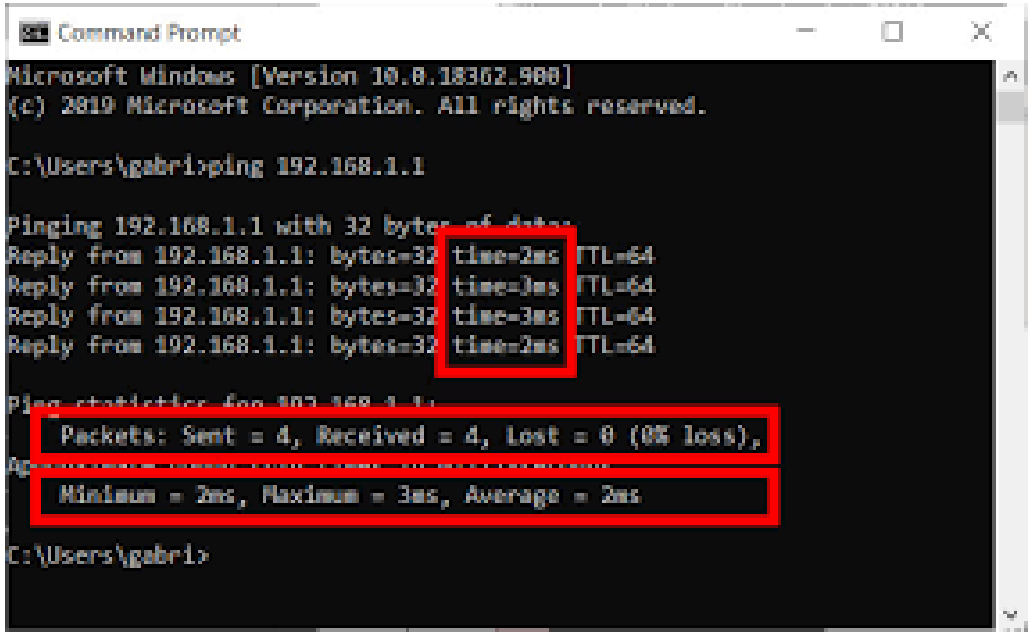
- netstat
  - Report port status and connections

- Switches
  - -a to show all
  - -b and -o report process that opened the port
  - -n use numerical formats
  - -e and -s to report statistics

Network Connectivity

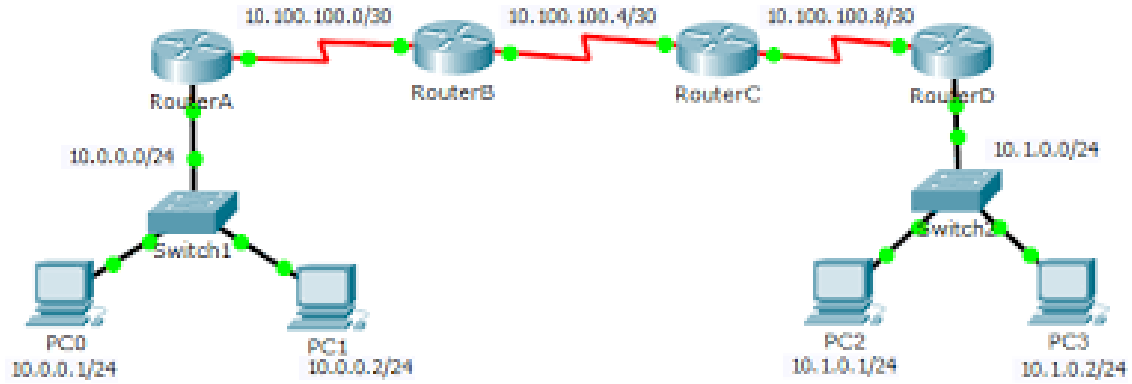
- ping to test connectivity with host
  - ping loopback and own IP
  - ping gateway
  - ping remote host

- Response types
  - Round-trip time (RTT) if responses received
  - Destination unreachable
  - No reply (request timed out)
  - ping by name



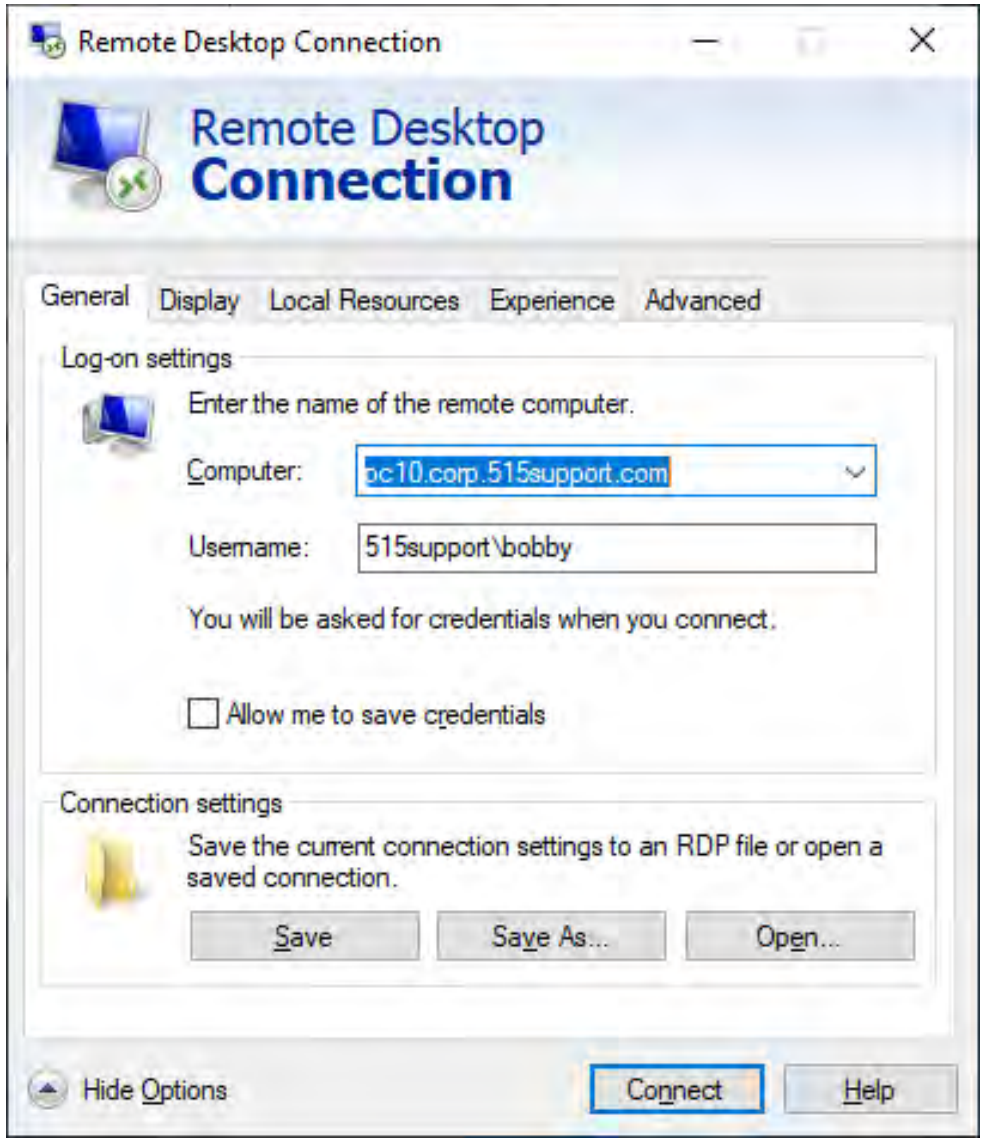
Network Connectivity

- pathing
  - Measure more accurate latency statistics
- tracert
  - Path from gateway to remote hosts
  - Hop count
  - Router ingress interface
  - RTT



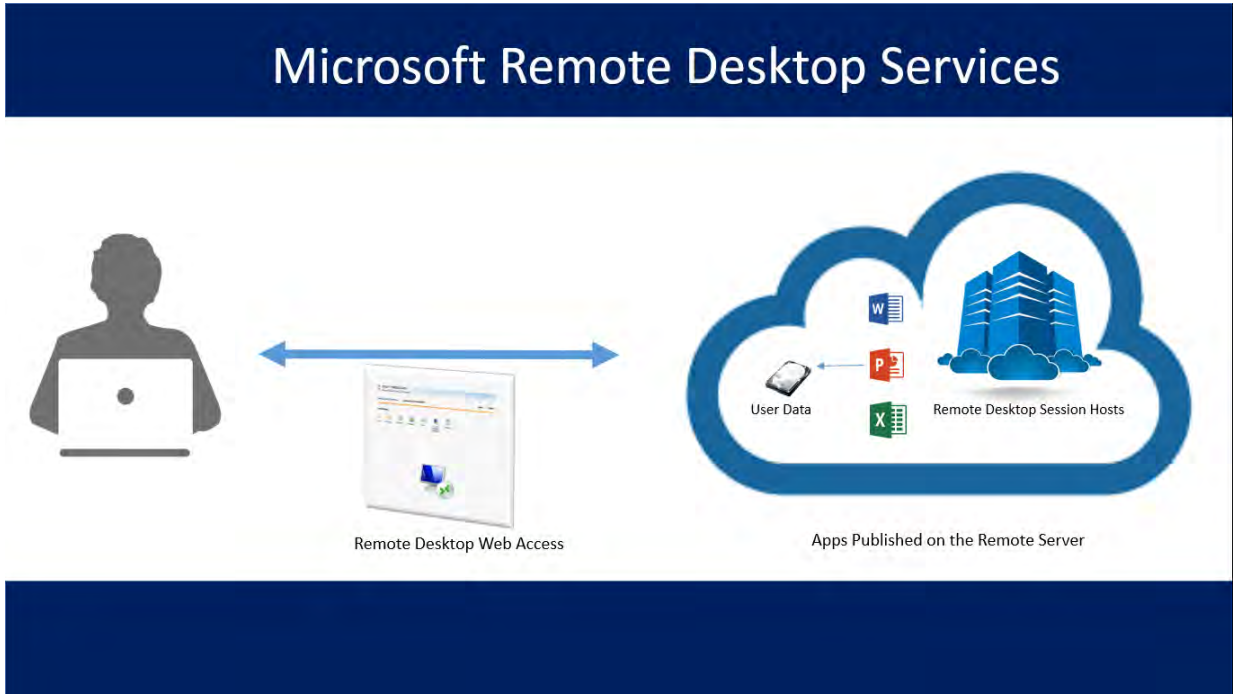
Remote Desktop Tools

- Virtual Network Computing (VNC)
  - macOS Screen Sharing
  - Secure versus unsecure third-party implementations
- Security considerations
  - Granting access
  - Preventing snooping
  - Patching vulnerabilities
- Remote Desktop Protocol (RDP)
  - mstsc.exe client app and session encryption
  - Multi-platform RDP clients



RDP Server and Security Settings

- Security considerations
  - Open-source RDP servers
  - Accounts allowed to connect
  - Network Level Authentication (NLA)
  - RDP Restricted Admin (RDPRA) Mode and Remote Credential Guard
  - TCP/3389 and risks from allowing port forwarding



Microsoft Remote Assistance

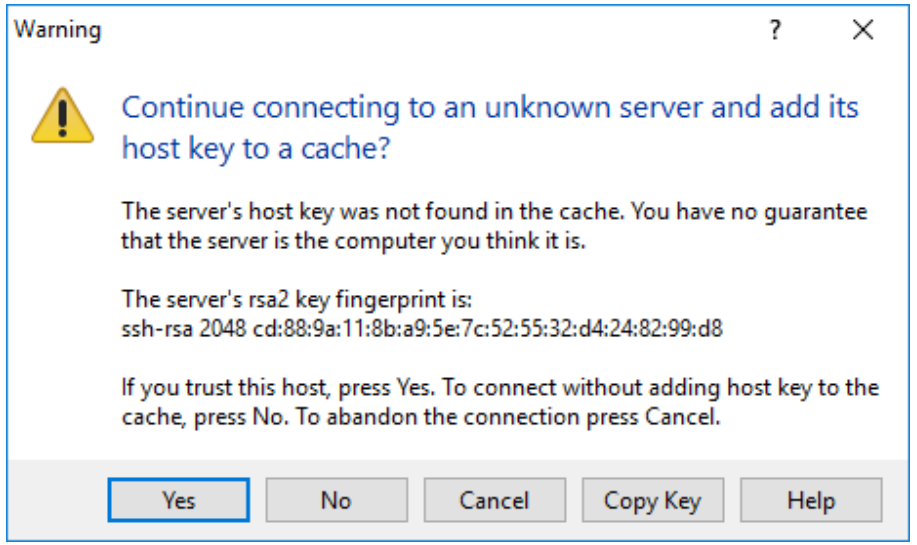
- Allows users to send invite to connect over RDP protected by password
- Chat and request control features
- Quick Assist feature better suited to connections over the Internet

Secure Shell

SSH client

- Password authentication
- Public key authentication

- Remote terminal access to command-line shell
- Secure Shell (SSH) server
  - Server’s host key
  - TCP/22



Desktop Management and Remote Monitoring Tools

- Visibility
  - Remote monitoring and management (RMM)
  - Desktop management and unified endpoint management (UEM)
- Common features
  - Performance monitoring and log collection
  - Security scanning
  - Push deployment
  - Remote support
- Intel vPRO/AMD PRO hardware support for out-of-band (OOB) remote access

Remote Monitoring Tools

- Visibility
  - Remote monitoring and management (RMM)
  - Desktop management and unified endpoint management (UEM)

- Common features
  - Performance monitoring and log collection
  - Security scanning
  - Push deployment
  - Remote support

- Intel vPRO/AMD PRO hardware support for out-of-band (OOB) remote access

Remote Monitoring Tools

- Screen-sharing software
  - Third-party remote desktop tools designed to work over the Internet
- Video-conferencing software
  - Most include a basic screen share client
- File transfer software
  - Easy sharing via Bluetooth
  - Apple AirDrop, Windows Nearby Sharing, and Android Nearby Shar
- Virtual private network (VPN)
  - Connect the remote host to the local network over a secure tunnel
  - Can be more secure than opening or port forwarding remote desktop/SSH ports