Client Networking Software

With many different software concepts and implementations between a client and a server, there's many different opportunities for failures that can disrupt a connection. This report aims to outline the major steps relating to networking that could impact a connection.

Client Software

For certain applications and workflows, a networking connection can be required for data and functionality. For estate agents in particular, software can be key to the functionality of a workstation, relying on and facilitating network connections for data such as client data management, interaction tracking, workflow automation and performance tracking (Software Advice UK, 2020).

Like with any CRM software, real estate CRM software relies on either client software or a web browser, depending on implementation, either of which have implications when it comes to configuration and functionality.

Operating Systems, Drivers & Protocols

Protocols such as TCP/IP and HTTP provide functionality to software, facilitating network connections. Additionally, workstation networking hardware relies on drivers depending on type, including network interface cards and dongles.

- Device drivers provide communication between software and hardware, providing the core functionality in software of both wired and wireless network interface cards. These drivers are key to the functionality of hardware (TJ, 2017).
- TCP/IP is usually implemented at the driver or kernel level. In windows, this driver is a protocol driver, loaded as a service at boot. Protocol drivers facilitate low-level packet allocation, creation, and transferral. These services communicate with higher level transport protocols and lower level protocol driver interfaces (Hudek, MacMichael, 2019). TCP/IP in particular can be configured within Windows through connection properties (Windows Support, 2020).
- HTTP and FTP are both application protocols, and are implemented within application software like web browsers and file browsers respectively. These protocols rely on transport protocols and drivers to function, being higher level and more focussed around information flow instead of device integration (Tiwari, 2019).

Firewalls

Firewalls are designed to reject networking packets based on firewall rules. These rules can be incredibly helpful for security, blocking unauthorised packets. While this can be useful for security, networking issues can arise should a firewall be misconfigured; packets that are blocked unintentionally can completely prevent the functionality of software (Cisco, 2020).

VPNs

Corporate VPNs rely on client software and server software, built upon standard network infrastructure and protocols. As well as this, some VPN protocols use ports that some firewalls block, which can impact connection and stability. Various protocols have different implications when it comes to speed, security and stability, with some being reliant on single ports being open and others having multiple reserved ports as well as the ability to use non-reserved ports (Phillips, 2017). Some popular protocols include:

- OpenVPN utilises multiple ports, but most commonly uses the reserved port 1194, or the HTTPS port 443, on both TCP and UDP. Since HTTPS is often left unblocked, OpenVPN is unlikely to also be accidentally blocked by a firewall (CRYPTMODE, 2020).
- L2TP/IPSec relies solely on port 1701 on UDP, which is reserved for the protocol. Unless the firewall is configured to allow L2TP traffic, this protocol won't work (SpeedGuide, 2020).
- SSTP, like OpenVPN, utilises port 443 on TCP, meaning that it shouldn't be blocked accidentally under normal conditions (CRYPTMODE, 2020). This protocol is integrated into Microsoft Windows, making it simpler to utilise (Phillips, 2017).
- IKEv2 uses the ports 50 and 51, port 500 on UDP and TCP, as well as port 4500 on UDP. The latter two ports are reserved for IPSec, and so aren't essential for common browsing and networking functionality. Because of this, they may be blocked (SpeedGuide, 2020).
- PPTP, while often not used due to security issues (Bischoff, 2016), utilises the TCP port 1723. This port is reserved for PPTP and as such, may be blocked in some firewall configurations (SpeedGuide, 2020).

Server Software & Operating Systems

While not directly related to client software and hardware, the operating systems and software that a server utilises can impact networking connections in much the same way as software on a client workstation. Because of this, compatible software, drivers, and operating systems should be utilised alongside the software and hardware used in workstations.

Bibliography

Software Advice UK. 2020. Best Real Estate CRM Software - 2020 Reviews & Pricing - Software Advice UK. [ONLINE] Available at: https://www.softwareadvice.com/uk/crm/real-estate-crm-comparison/#buyers-guide. [Accessed 20 March 2020].

Madhur TJ. 2017. What Is a Network Driver, And How To Install It? | DESKDECODE.COM. [ONLINE] Available at: https://www.deskdecode.com/network-driver/. [Accessed 20 March 2020].

Ted Hudek, Duncan MacMichael. 2019. Protocol drivers - Windows drivers | Microsoft Docs. [ONLINE] Available at: https://docs.microsoft.com/en-us/windows-hardware/drivers/network/ndis-protocol-drivers2. [Accessed 20 March 2020].

Windows Support. 2020. Change TCP/IP settings. [ONLINE] Available at: https://support.microsoft.com/en-us/help/15089/windows-change-tcp-ip-settings. [Accessed 20 March 2020].

Richa Tiwari. 2019. Application Layer Protocols (DNS, SMTP, POP, FTP, HTTP) Study Notes. [ONLINE] Available at: https://gradeup.co/application-layer-protocols-dns-smtp-pop-ftp-http-i-ba1194bd-c5ab-11e5-9dcb-5849de73f8e1. [Accessed 20 March 2020].

Cisco. 2020. What Is a Firewall? - Cisco. [ONLINE] Available at: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html. [Accessed 21 March 2020].

Gavin Phillips. 2017. The 5 Major VPN Protocols Explained. [ONLINE] Available at: https://www.makeuseof.com/tag/major-vpn-protocols-explained/. [Accessed 21 March 2020].

CRYPTMODE. 2020. VPN Ports & Port Forwarding. [ONLINE] Available at: https://cryptmode.com/vpn-ports-port-forwarding-tcp-udp-443-80-53-25-22-21/. [Accessed 21 March 2020].

SpeedGuide. 2020. Port 1701 (tcp/udp) :: SpeedGuide. [ONLINE] Available at: https://www.speedguide.net/port.php?port=1701. [Accessed 21 March 2020].

SpeedGuide. 2020. Port 4500 (tcp/udp) :: SpeedGuide. [ONLINE] Available at: https://www.speedguide.net/port.php?port=4500. [Accessed 21 March 2020].

Paul Bischoff. 2016. The PPTP VPN Protocol Is Not Secure Try, These Alternatives Instead. [ONLINE] Available at: https://www.comparitech.com/blog/vpn-privacy/the-pptp-vpn-protocol-is-not-secure-use-these-alternatives-instead/. [Accessed 21 March 2020].

SpeedGuide. 2020. Port 1723 (tcp/udp) :: SpeedGuide. [ONLINE] Available at: https://www.speedguide.net/port.php?port=1723. [Accessed 21 March 2020].