Configuring and Troubleshooting Networks
Configure Network Connection Settings
Configuring and Troubleshooting Networks

- Configure Network Connection Settings
- Install and Configure SOHO Networks
- Configure SOHO Network Security
- Configure Remote Access
- Troubleshoot Network Connections
- Install and Configure IoT Devices
NIC Properties

- Computer’s network adapter connects to a network appliance
- Card settings should be configured to match network
Wired Network Cards

- Ethernet adapter and switch must have same media type:
  - Signaling speed
  - Half/full duplex
- Most will auto-negotiate; can be configured
- Most settings can be left at default
QoS

• Network protocol that prioritizes some types of traffic.
• Can help ensure real-time applications such as VoIP or video conference have priority.
• QoS usually configured on managed switches.
• May need to enable QoS protocol on adapter.
Onboard Network Cards

- Most computers have built-in Gigabit Ethernet adapter.
- Uses RJ-45 port/twisted-pair cabling.
- Check system setup if issues or to disable if installing a plug-in card.
Wireless Network Cards

• Set up 802.11 standard supported by access point
• Card should support any standard available
• Configure Roaming Aggressiveness to adjust for weak signals
• Transmit Power usually set to highest level by default
Wake on LAN

- Start computer remotely
- Network card is active, on standby
- “Magic packet” starts boot
- To set up WoL:
  1. Enable WoL in system setup
  2. Enable WoL on adapter
  3. Configure network to send magic packets
Network Connections in Windows 7 and Windows 8 (Slide 1 of 4)

- Configure network card with client software and protocol
- Use Network and Sharing Center
Network Connections in Windows 7 and Windows 8 (Slide 2 of 4)

• Access adapter properties
• Wired/wireless adapter names vary
Network Connections in Windows 7 and Windows 8 (Slide 3 of 4)

- Change properties or view status
- Configure client, protocol, service
- Default bindings include Microsoft clients, IPv4 and IPv6, and link-layer discovery
Network Connections in Windows 7 and Windows 8 (Slide 4 of 4)

• To join WLAN, select network from list in notification area
• Can connect automatically
• Can configure manually if network not broadcasting
Network Connections in Windows 10

- Settings: Network & Internet
- Use to access Network and Sharing Center and Network Connections applets
IP Address Configuration (Slide 1 of 2)

- Configure wired and wireless through connection’s Properties
- Default is dynamic IP
- Can configure a static IP address manually
• Select “Obtain an IP address automatically” for DHCP/APIPA
• Can set up alternate configuration if desired
Other Network Connections (Slide 1 of 3)

- SOHO router is typical; usually combines several functions
- Other connection options include dial-up
- Analog modem connects to ISP
- Use Set Up a Connection or Network to configure
Other Network Connections (Slide 2 of 3)

- WAN cellular connects to a cell provider’s network
- Can be USB or internal
- Install vendor software, plug in adapter, use software to view and configure
• VPN tunnels privately through network
• Windows supports several types; can configure in Network Connections
• Click network status icon to access
Discussing Network Connection Configuration Settings
Configuring Network Connection Settings
Configuring and Troubleshooting Networks

• Configure Network Connection Settings
• Install and Configure SOHO Networks
• Configure SOHO Network Security
• Configure Remote Access
• Troubleshoot Network Connections
• Install and Configure IoT Devices
SOHO Networks

• Business network; may use centralized server as well as clients.
• Often uses single Internet device for connectivity.
• May be home/residential network as well.
Common SOHO Network Hardware (Slide 1 of 2)

- DSL or cable modem installed on customer premises.
- Bundles several device types: modem, router, switch, access point.
- On DSL, RJ-11 port connects to phone jack; voice/data splitter usually part of modern socket.
Common SOHO Network Hardware (Slide 2 of 2)

- On DSL, RJ-11 port connects to phone jack.
- Voice/data splitter usually part of modern socket.
SOHO Network Configuration (Slide 1 of 2)

- Connect device to SOHO appliance to configure.
- Access management interface through browser.
- Change default password!
- Follow wizard interface to configure Internet access.
SOHO Network Configuration (Slide 2 of 2)

- View line status and system log in management console.
- Helpful for troubleshooting.
Wireless Settings

- Configure wireless settings; most hosts connect wirelessly.
- May be part of setup wizard; can use management software directly.
- Adjust settings as appropriate:
  - Frequency band (2.4 GHz or 5 GHz)
  - SSID (name for WAN)
  - Security and encryption
  - Password (pre-shared key)
  - 802.11 mode
  - Channel/channel width
DHCP and IP Address Configuration

- May need to adjust DHCP server settings
- Enabled by default
- If you disable, IP addresses must be assigned manually
- Easy for attacker to determine scope
WPS

- Simplifies secure access point setup.
- AP and all adapters must be WPS-capable.
- Pushbutton on device typically causes device and AP to associate automatically over WPA2.
- Generates random SSID and passphrase.
Access Point Placement

• Correct antenna and access point placement helps ensure robust network.
• AP placement may be constrained by provider’s cabling location.
• Can use extenders.
• Site survey can help identify dead zones.
Channel Selection

- In US, 2.4 GHz band subdivided into 11 channels at 5 MHz intervals.
- Best to allow 25 MHz spacing for channels in active use.
- No more than 3 nearby APs can have non-overlapping channels.
- Newer APs detect least-congested channel at boot; may need to adjust.
- Use spectrum analyzer to find least busy channels.
Radio Power Levels

- Can turn down AP power to prevent war driving.
- Need to ensure enough coverage for legitimate users.
- May expose to “evil twin” attack if a rogue AP is detected first.
- Increasing power may also cause signal bouncing.
- Client must match AP.
- Best to allow autonegotiation.
Wi-Fi Security Protocols (Slide 1 of 2)

- Wi-Fi requires careful security configuration
- Media “unguided;” RF scanner can intercept signals
- Encryption is crucial
- Cipher scrambles message; key decodes message
- Keep key secure
## Wi-Fi Security Protocols (Slide 2 of 2)

<table>
<thead>
<tr>
<th>Security Protocol</th>
<th>Description</th>
</tr>
</thead>
</table>
| WEP               | • Legacy encryption system based on RC4 cipher  
                    • 64-bit or 128-bit key  
                    • Flaw in key production method; easy for attacker to generate key  
                    • Deprecated and should not be used |
| WPA               | • Based on RC4  
                    • Adds TKIP to fix security problem  
                    • WPA2 developed to meet 802.11i security standards  
                    • Use WPA2 whenever possible  
                    • If not supported by devices, use WPA |
| WPA2              |             |
## Wi-Fi Authentication

<table>
<thead>
<tr>
<th>Authentication Mode</th>
<th>Description</th>
</tr>
</thead>
</table>
| Personal            | • Based on pre-shared key generated from passphrase.  
                       • Cannot completely secure distribution of key; on home network may not be secure passphrase; all users share key (no accounting); hard to change key.  
                       • Simple setup.  
                       • Only choice for WEP; can use with WPA/WPA2 on SOHO networks or workgroups. |
| Enterprise          | • Enterprise mode authentication in WPA/WPA2.  
                       • Authentication passed to RADIUS server.  
                       • Suitable for server-/domain-based networks. |
## Common SOHO Security Issues

<table>
<thead>
<tr>
<th>Security Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSID</strong></td>
<td>• Simple name to identify the WAN&lt;br&gt;• Change default SSID&lt;br&gt;• Do not use personal information&lt;br&gt;• Disable SSID broadcast&lt;br&gt;• Enable encryption</td>
</tr>
<tr>
<td><strong>Physical Security</strong></td>
<td>• Restrict physical access to enterprise routers and switches&lt;br&gt;• Attacker with physical access could reset to defaults, gain access</td>
</tr>
<tr>
<td><strong>Updating Firmware</strong></td>
<td>• Keep Internet appliance firmware and driver up to date&lt;br&gt;• Make sure power stays on during update process</td>
</tr>
<tr>
<td><strong>Static IP Addresses</strong></td>
<td>• Static IP assignments will not deter a determined attack&lt;br&gt;• Router/modem must have static IP to function as DHCP server/default gateway</td>
</tr>
</tbody>
</table>
Latency and Jitter

**Quality of Service (QoS):** Using a network protocol to prioritize types of traffic

- Modern networks provide two-way communications (VoIP, video conferencing, gaming).
- Standard protocols sensitive to data loss, not delivery delay (latency/jitter).
- Real-time data applications sensitive to latency and jitter, not packet loss.
  - Latency: the time for a signal to reach recipient
  - Jitter: variation in delay (congestion, configuration problems).
- QoS:
  - Hard to guarantee on Internet.
  - Can be deployed on enterprise networks.
  - On SOHO network, may be able to configure on router/modem.
Activity

Discussing SOHO Network Installation and Configuration
Installing and Configuring SOHO Networks
Configuring and Troubleshooting Networks

- Configure Network Connection Settings
- Install and Configure SOHO Networks
- **Configure SOHO Network Security**
- Configure Remote Access
- Troubleshoot Network Connections
- Install and Configure IoT Devices
Firewalls (Slide 1 of 2)

- 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
## Firewalls (Slide 2 of 2)

<table>
<thead>
<tr>
<th>Firewall Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Packet Filtering** | • Earliest type; all firewalls capable of this function  
• Inspects IP packet headers, accepts or drops based on rules  
• Filtering rules based on:  
  • IP filtering  
  • Protocol ID/type  
  • Port filtering/security  
• Configure ACL |
| **Host Firewall** | • Software on individual host; may be in addition to network firewall  
• Can do packet filtering  
• Can also grant/deny access based on software programs, services/processes, and users  
• Two firewalls increase security; more complex to configure and troubleshoot |
## Firewall Settings (Slide 1 of 2)

<table>
<thead>
<tr>
<th>Firewall Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Disabling Ports</strong></td>
<td>• Only enable required services; can remove service at the host.</td>
</tr>
<tr>
<td></td>
<td>• May want service available locally but not on Internet.</td>
</tr>
<tr>
<td></td>
<td>• Configure firewall ACL to block the port, or block by default rule.</td>
</tr>
<tr>
<td><strong>MAC Filtering</strong></td>
<td>• Firewalls, switches, and APs can whitelist/blacklist MAC addresses.</td>
</tr>
<tr>
<td></td>
<td>• Can be time-consuming, but good security option for SOHO networks.</td>
</tr>
<tr>
<td><strong>Content Filtering / Parental Controls</strong></td>
<td>• Blocks websites and services based on keywords, ratings, or classification.</td>
</tr>
<tr>
<td></td>
<td>• Can restrict times.</td>
</tr>
<tr>
<td></td>
<td>• ISP-enforced filters cannot distinguish account types.</td>
</tr>
<tr>
<td></td>
<td>• Filters can also be enforced by OS.</td>
</tr>
<tr>
<td><strong>Whitelists / Blacklists</strong></td>
<td>• Blacklists document URLs known to harbor specific undesired content.</td>
</tr>
<tr>
<td></td>
<td>• Whitelists document sites that will be accessible even if filter is applied.</td>
</tr>
</tbody>
</table>
Firewall Settings (Slide 2 of 2)
NAT

- All routers/modems use NAT/NAPT
- Router has single public address; clients use local private addresses
- Router translates between Internet and host
- Usually auto-configured
- Some protocols may need ALG to open ports dynamically
Port Forwarding and Port Triggering

- Internet hosts only see router’s public address.
- Configure port forwarding/DNAT if running an Internet-facing service on your internal network.
- Router transmits Internet requests to a given port to a designated internal host.
- Port triggering is for applications using multiple ports.
DMZ

• If internal server is exposed to Internet, consider local network security; compromised server can expose LAN to attacks.

• Enterprise networks use DMZ; hosts in DMZ are not trusted by local network.

• Traffic from Internet cannot access local network through DMZ.

• SOHO vendors’ “DMZ” = LAN computer that receives all Internet communications not forwarded to other hosts.
Universal Plug-and-Play

- Users may be tempted to turn off firewall if configuration is complex. Services requiring complex configuration can use UPnP to instruct firewall with correct configuration.
- Does have security vulnerabilities:
  - Use only if required.
  - Don’t let UPnP accept Internet requests.
  - Keep firmware, security advisories up to date.
Windows Firewall (Slide 1 of 2)

- Each version has become more advanced
- Configure in Control Panel
Windows Firewall (Slide 2 of 2)

- Can configure exceptions
- Use Windows Defender Security Center on Windows 10
Windows Firewall with Advanced Security (Slide 1 of 2)

- Add-in to basic firewall
- Can configure outbound filtering, IPSec, monitoring
- Configure in Group Policy on domain, in management console in workgroup
• Configure inbound and outbound rules as appropriate
• Rules can use various triggers
Location Awareness (Slide 1 of 2)

- Firewall settings can be applied depending on connected network.
- Displays dialog when new network is detected.
Location Awareness (Slide 2 of 2)

- Set location (Home, Work, Public, Domain).
- Use Network and Sharing Center to change location.
- In Windows 8/Windows 10, networks are either public or private.
- Change using Settings app.
• Browser is very important software, for browsing and as app interface.
• Internet Explorer has been dominant, but other browsers have similar configurations.
• General settings include home pages, browsing history, etc.
• Clear browsing history on public computer.
Browser Configuration (Slide 2 of 7)

- Configure connections:
  - Dial-up
  - Router
Configure proxy:
- User machines send requests to proxy server, which sends to Internet.
- May also perform caching for improved performance.
- Use LAN Settings to configure proxy address.
• Security settings protect system from malicious content on web pages.
• In Windows, configure by security zone.
Browser Configuration (Slide 5 of 7)

- Privacy settings control use of cookies
  - Text files containing session data
- Configure pop-up blocker
Browser Configuration (Slide 6 of 7)

• Check or set default browser
• Manage add-ons
Browser Configuration (Slide 7 of 7)

- Various advanced settings and options
- Resetting the browser
Configuring and Troubleshooting Networks

- Configure Network Connection Settings
- Install and Configure SOHO Networks
- Configure SOHO Network Security
- Configure Remote Access
- Troubleshoot Network Connections
- Install and Configure IoT Devices
# Windows Remote Access Tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
</table>
| Remote Desktop  | • Allows user to connect to desktop remotely<br>
|                 | • Desktop machine = terminal server; connecting machine = Windows terminal<br>
|                 | • Good for home workers<br>
|                 | • Can also be used for troubleshooting<br>
|                 | • TCP port 3389                                                             |
| Remote Assistance | • Allows user to request help from technician<br>
|                 | • Helper can join user session, take control of desktop<br>
|                 | • Port assigned dynamically from ephemeral range; intended for local support, not to pass through firewalls |
Remote Settings Configuration

- Remote Assistance allowed by default; Remote Desktop is not
- Configure in System Properties/Remote Settings
- Choose RDP client options, including NLA
- RDP authentication/session data always encrypted
- Define which users can connect remotely (local or domain accounts)
Remote Credential Guard

- Remote Desktop credentials are vulnerable on machine compromised by malware.
- RDPRA Mode and Remote Credential Guard mitigate this risk.
The Remote Assistance Process

- Remote Assistance request placed with Remote Assistance tool (file, email, or Easy Connect).
- Helper opens invitation file and waits for user to accept offer.
- Remote Desktop window and chat tool open.
- Remote Assistance session encrypted, same as RDP.
Remote Desktop

- Open via the Communications menu in Accessories or by typing `mstsc` at a command prompt.
- Enter the server's computer name or IP address to connect.
- You will need to define logon credentials.
- Use the format `ComputerOrDomainName\UserName`
- No one else can use the target system while in remote mode.
Remote Access Technologies

• Remote Desktop and Remote Assistance are Microsoft technologies.
• Can connect from Linux, macOS, iOS, or Android to Windows RDP server using `mstsc` client.
• Use other protocols and software for incoming connections to non-Windows devices.
Telnet (Slide 1 of 2)

- Command-line terminal emulation protocol and program
- Host runs Telnet Daemon on TCP port 23
- Client uses Telnet program
- Once connected, can use same commands as local user
- Common commands: open HostPort; ?; status; close; quit
- Troubleshooting for SMTP or HTTP
- Remote router or switch configuration
Telnet (Slide 2 of 2)

```
220 vpc01 Microsoft ESMTP MAIL Service, Version: 6.0.2600.2180 ready at Thu, 16 Jul 2009 10:22:00 +0100

hello
250 vpc01 Hello [192.168.1.2]
mail from:test@domain.com
250 2.1.0 test@domain.com...Sender OK
rcpt to:user@myisp.com
250 2.1.5 user@myisp.com
data
354 Start mail input; end with <CRLF>.<CRLF>
subject:test message
Connectivity test

250 2.6.0 <UFC01J5gjo17TdnfmYo00000001@vpc01> Queued mail for delivery
```
SSH (Slide 1 of 2)

• Replaces unsecure administration and file copy programs (Telnet, FTP)
• Uses TCP port 22
• Encrypts each session
• Many commercial products
• SSH servers identified by public/private key pairs
• SSH clients can keep mappings or use commercial SSH key management products
SSH (Slide 2 of 2)

- Server’s host key used to set up secure channel for SSH client authentication
- Various authentication methods possible; can be enabled/disabled as needed:
  - Username/password
  - Kerberos
  - Host-based
  - Public key
Screen Sharing and VNC

• In MacOS, use Screen Sharing for remote desktop
  • Based on VNC
  • Can use any VNC client
  • Encrypted

• VNC itself is freeware
  • Similar to RDP
  • TCP port 5900
  • Freeware versions have no connection security
  • Commercial products include encryption solutions
File Share

- Network file sharing can be complex (file sharing protocol; permissions; user accounts)
- Vendors offer simple file sharing options:
  - AirDrop (Apple iOS/macOS)
  - NearShare (Microsoft)
  - Third-party and open-source alternatives
- Products include security, but always potential for misuse
- Only accept requests from known contacts
- Security vulnerabilities may allow unsolicited transfers
Discussing Remote Access Configuration
Configuring and Troubleshooting Networks

- Configure Network Connection Settings
- Install and Configure SOHO Networks
- Configure SOHO Network Security
- Configure Remote Access
- Troubleshoot Network Connections
- Install and Configure IoT Devices
Common Wired Network Connectivity Issues (Slide 1 of 2)

- Rule out hardware-layer connectivity (cable connection)
- Troubleshoot wired connectivity:
  - Test with `ping`
  - Verify patch cord between host/panel and panel/switch
  - Connect a different host
  - Verify network adapter link properties
  - Connect to a different port
  - Check the switch (if multiple users)
  - Use cable testing tools
Common Wired Network Connectivity Issues (Slide 2 of 2)

• Troubleshoot slow transfer speeds:
  • Check network adapter driver configuration
  • Check setting for switch port
  • Check for:
    • Switch or router congestion or network-wide problem
    • Adapter driver issues
    • Malware
    • Interference on network cabling
Common Wireless Network Connectivity Issues (Slide 1 of 2)

• Consider problems with physical media, configuration:
  • RF signal weakens with distance
  • Check security and authentication configuration

• Configuration issues:
  • If in range, check SSID mismatch or SSID broadcast
  • Standards mismatch
  • Dual-band support

• Low RF/RSSI

• Signal issues:
  • Channel interference
  • Signal blocking
Common Wireless Network Connectivity Issues (Slide 2 of 2)

- Use Wi-Fi analyzer such as inSSIDer to perform site survey
- Site survey can:
  - Identify sources of interference problems
  - Measure signal strength
  - Identify congested channels
IP Configuration Issues (Slide 1 of 2)

- If host IP configuration is incorrect it will not be able to communicate
- View adapter status in Windows
- Use `ipconfig` at command line
- Typical switches:
  - `/all`
  - `/release`
  - `/renew`
  - `/displaydns`
  - `/flushdns`
IP Configuration Issues (Slide 2 of 2)

- **Use `ipconfig` to test adapter configuration:**
  - Static or DHCP? If DHCP, correct parameters?
- **If configuration is correct, check for:**
  - Communication with DHCP server
  - Configuration with DHCP server
  - Multiple conflicting DHCP servers
- **On Linux, use `ifconfig`; some different functionality**
IP Connectivity Issues (Slide 1 of 3)

- If link and IP are correct, problem may be in network topology.
- Test connections by trying to use resources (but doesn’t eliminate application fault).
- Use other connectivity tests:
  - Ping
  - DNS testing
  - IP conflict
IP Connectivity Issues (Slide 2 of 3)

- Use **ping** to test communications.
- Ping loopback, workstation, default gateway, remote host.
- If successful, reply with time in milliseconds.
- If unsuccessful:
  - Destination unreachable
  - No reply (request timed out)
IP Connectivity Issues (Slide 3 of 3)

- Test DNS:
  - Ping DNS names.
  - Try reverse lookup.

- Troubleshoot IP conflicts:
  - Possible configuration error due to static assignment.
  - Windows disables IP.
  - Identify affected machines and resolve duplicate.
Routing Issues

- Use `tracert` to investigate routing problems
- Command will time out if host not located
- Will list:
  - Router hops
  - Ingress interface
  - Response time
  - Asterisk if no response
Unavailable Resources (Slide 1 of 5)

- If not with cabling, switches/routers, or IP, problem is at higher layer
- Failures possible in:
  - Security
  - Name resolution
  - Application/OS
- If Internet access or local resources are unavailable, establish scope by trying a different client:
  - If works, problem with 1\textsuperscript{st} client
  - If fails, problem is with server, device, or infrastructure
Troubleshooting Internet availability:
- If “No Internet access” message, no working Internet connection
- Check local PC settings
- Check ISP’s service status page/helpline
- Restart modem/router
- Suspect security issue (mis-configured proxy, firewall blocking host)
Performing a reset:
- Restart server as stock response to persistent problems
- Restart application
- Run Windows network troubleshooter
- Reset the network stack
  - Windows 10: Network & Internet > Status
  - Windows 7/8: Network Adapter troubleshooter or command-line tools
- Remove network adapters and reboot; update all network settings
Unavailable Resources (Slide 4 of 5)

- Use `netstat` to investigate open ports and connections
- Use `-a`, `-b`, `-n` switches
- Linux has slightly different utility

```
C:\Windows\system32>netstat -b -n
Active Connections

Proto Local Address                      Foreign Address             State
TCP  192.168.1.110:5006                105.41.10.123:80           CLOSE_WAIT
[EXPLOR.EXE]
TCP  192.168.1.110:5007                105.41.10.123:80           CLOSE_WAIT
[EXPLOR.EXE]
TCP  192.168.1.110:5008                216.58.208.40:443          ESTABLISHED
[EXPLOR.EXE]
TCP  192.168.1.110:5009                216.58.208.40:443          ESTABLISHED
[EXPLOR.EXE]
TCP  192.168.1.110:5010                104.27.151.216:80          CLOSE_WAIT
[EXPLOR.EXE]
TCP  192.168.1.110:5011                104.27.151.216:80          CLOSE_WAIT
[EXPLOR.EXE]
TCP  192.168.1.110:5012                104.27.151.216:80          CLOSE_WAIT
[EXPLOR.EXE]
TCP  192.168.1.110:5013                104.27.151.216:80          CLOSE_WAIT
[EXPLOR.EXE]
TCP  192.168.1.110:5014                104.27.151.216:80          CLOSE_WAIT
[EXPLOR.EXE]
TCP  192.168.1.110:5015                104.27.151.216:80          CLOSE_WAIT
[EXPLOR.EXE]
TCP  192.168.1.110:5016                52.28.192.217:443          ESTABLISHED
[EXPLOR.EXE]
TCP  [fe80::5ce9:8be5:bb3e:f341:x4]:2179  [fe80::5ce9:8be5:bb3e:f341:x4]:2179
[fe80::5ce9:8be5:bb3e:f341:x4]:3567  [fe80::5ce9:8be5:bb3e:f341:x4]:3567
[fe80::5ce9:8be5:bb3e:f341:x4]:5519  [fe80::5ce9:8be5:bb3e:f341:x4]:5519
[fe80::5ce9:8be5:bb3e:f341:x4]:59395
[fe80::5ce9:8be5:bb3e:f341:x4]:59395
TCP  [fe80::5ce9:8be5:bb3e:f341:x4]:2179  [fe80::5ce9:8be5:bb3e:f341:x4]:2179

C:\Windows\system32>
```
Unavailable Resources (Slide 5 of 5)

• Use `nslookup` to investigate name resolution problems
• `nslookup -Option Host Server`
• Query a different name server and compare your results

```
C:\Users\James>nslookup -type=mx comptia.org 8.8.8.8
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
comptia.org      MX preference = 10, mail exchanger = comptia-org.mail.protection.outlook.com
```
Activity

Discussing Network Connection Troubleshooting
Troubleshooting Network Connections
Configuring and Troubleshooting Networks

- Configure Network Connection Settings
- Install and Configure SOHO Networks
- Configure SOHO Network Security
- Configure Remote Access
- Troubleshoot Network Connections
- Install and Configure IoT Devices
Internet of Things

- Global network of devices equipped with sensors, software, network connectivity.
- Devices can communicate and pass data M2M.
- “Things” identified with unique numbers/codes.
## IoT Wireless Networking Technologies

<table>
<thead>
<tr>
<th>Technology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bluetooth</strong></td>
<td>• Radio communication speeds up to 3 Mbps; v3 or v4 up to 24 Mbps</td>
</tr>
<tr>
<td><strong>Bluetooth Low Energy</strong></td>
<td>• Maximum range of 10 m/30 ft (signal strength weak at max. distance)</td>
</tr>
<tr>
<td></td>
<td>• Used in many portable/wearable devices</td>
</tr>
<tr>
<td></td>
<td>• Pairing procedure</td>
</tr>
<tr>
<td></td>
<td>• BLE version for low-powered devices that transmit infrequently</td>
</tr>
<tr>
<td><strong>Z-Wave</strong></td>
<td>• Wireless protocol for home automation</td>
</tr>
<tr>
<td></td>
<td>• Mesh topology over low-energy radio waves</td>
</tr>
<tr>
<td></td>
<td>• Can configure repeaters up to four “hops”</td>
</tr>
<tr>
<td></td>
<td>• High 800-low 900 MHz range; runs for years on battery power</td>
</tr>
<tr>
<td><strong>ZigBee</strong></td>
<td>• Similar to/competitive with Z-Wave</td>
</tr>
<tr>
<td></td>
<td>• 2.4 GHz band</td>
</tr>
<tr>
<td></td>
<td>• Up to 65,000 devices in single network (232 for Z-Wave); no hop limit</td>
</tr>
<tr>
<td><strong>RFID and NFC</strong></td>
<td>• Tagging and tracking devices with radio-frequency tags</td>
</tr>
<tr>
<td></td>
<td>• NFC: peer-to-peer version of RFID</td>
</tr>
</tbody>
</table>
IoT Device Configuration

- IoT functionality in home automation/smart home devices
- To interoperate, devices must all share protocol (i.e., Z-Wave or Zigbee) and be compatible with same virtual assistant/hub
- Endpoint devices (thermostats, light switches, etc.)
- Smartphone control (using Wi-Fi, Bluetooth, NFC)
- Smart hub control (Z-Wave, Zigbee, Wi-Fi, Bluetooth, NFC)
  - Dedicated hub from vendor
  - Generic smart speaker/digital assistant
Digital Assistants

• Voice interface responding to natural language
• Smartphones, computers, smart-speaker hubs
• Back-end server processing; raises privacy/security concerns
  • Google Assistant
  • Amazon Alexa
  • Apple Siri
  • Microsoft Cortana
• Device may require “training” to recognize and respond to user’s voice.
Discussing IoT Devices
Activity

Configuring IoT Devices
Reflective Questions

1. What experiences do you have in working with the networking technologies discussed in this lesson?

2. Do you have any experience working with SOHO networks? What do you expect to support in future job functions?