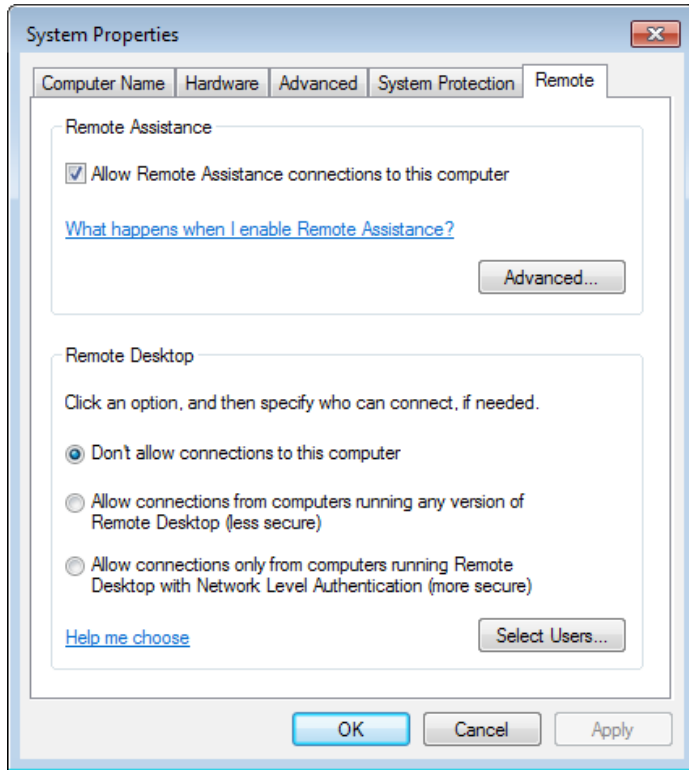


Windows Remote Access Tools

| Tool | Description |
|--------------------------|--|
| Remote Desktop | <ul style="list-style-type: none">• Allows user to connect to desktop remotely• Desktop machine = terminal server; connecting machine = Windows terminal• Good for home workers• Can also be used for troubleshooting• TCP port 3389 |
| Remote Assistance | <ul style="list-style-type: none">• Allows user to request help from technician• Helper can join user session, take control of desktop• Port assigned dynamically from ephemeral range; intended for local support, not to pass through firewalls |

Remote Settings Configuration



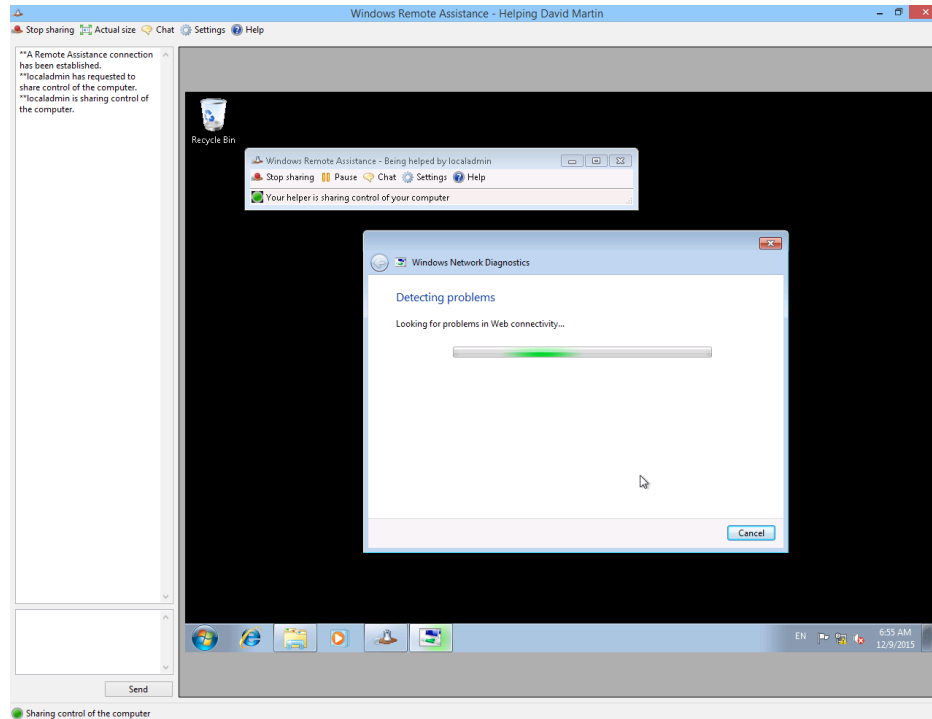
- Remote Assistance allowed by default; Remote Desktop is not
- Configure in System Properties/Remote Settings
- Choose RDP client options, including NLA
- RDP authentication/session data always encrypted
- Define which users can connect remotely (local or domain accounts)

Remote Credential Guard

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

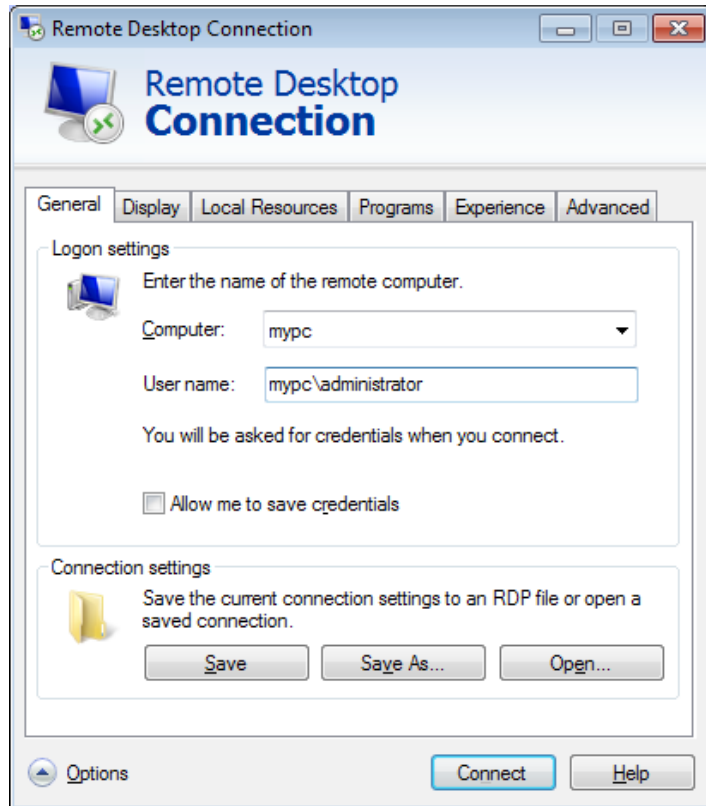


The Remote Assistance Process



- 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.

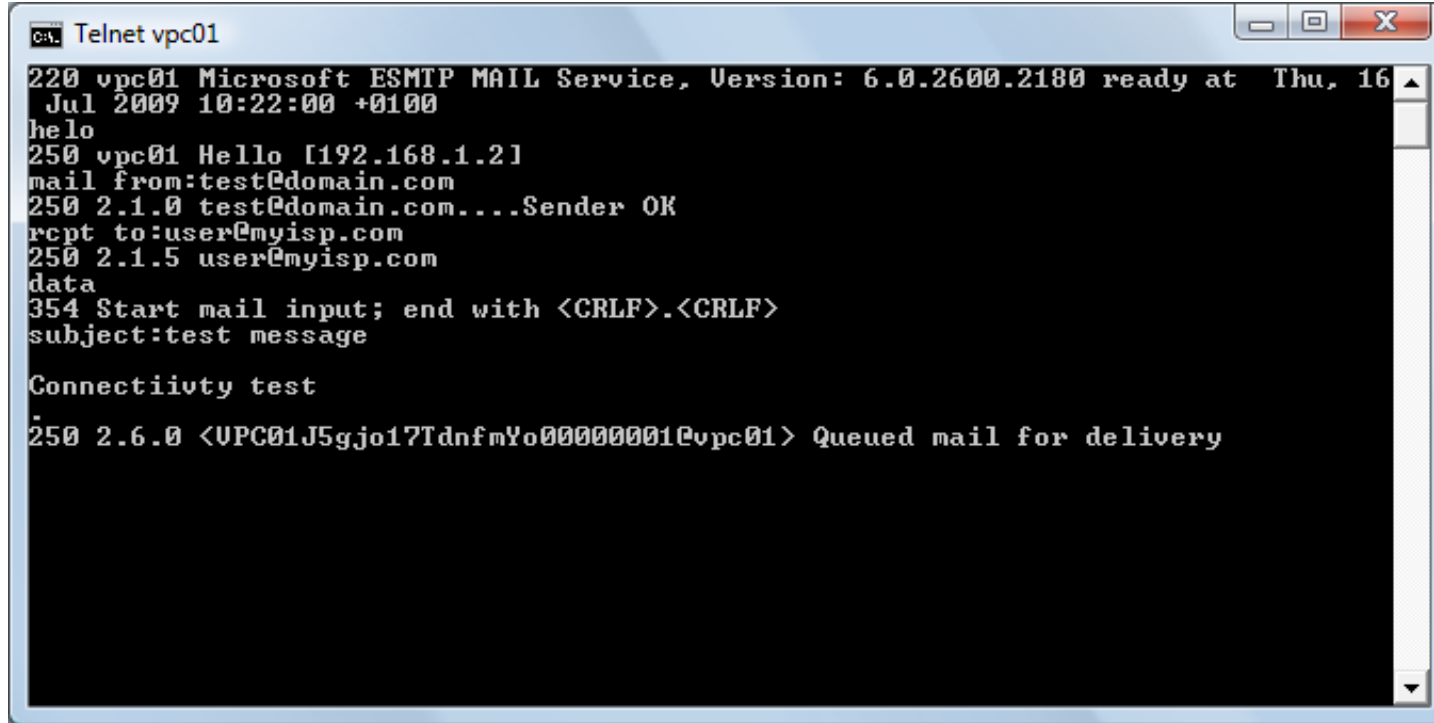
Remote Access Technologies

- 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)



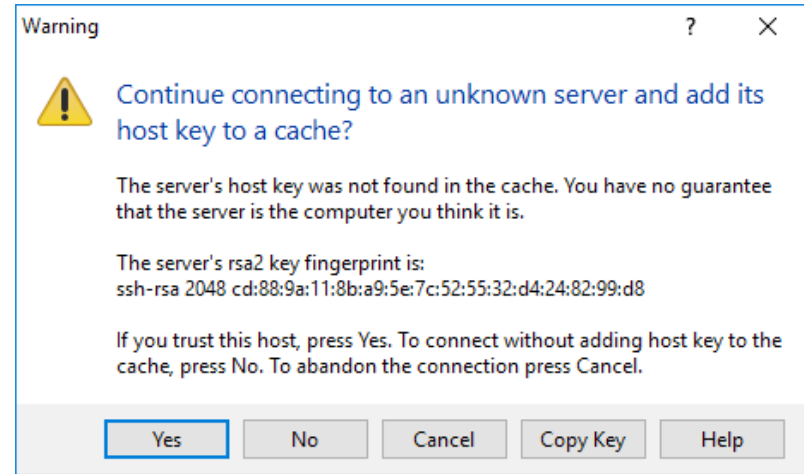
```
CA: Telnet vpc01
220 vpc01 Microsoft ESMTIP MAIL Service, Version: 6.0.2600.2180 ready at Thu, 16
Jul 2009 10:22:00 +0100
helo
250 vpc01 Hello [192.168.1.21]
mail from:test@domain.com
250 2.1.0 test@domain.com....Sender OK
rcpt to:user@myisp.com
250 2.1.5 user@myisp.com
data
354 Start mail input; end with <CRLF>.<CRLF>
subject:test message

Connectiivty test

250 2.6.0 <VPC01J5gjo17TdnfmYo00000001@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



Activity



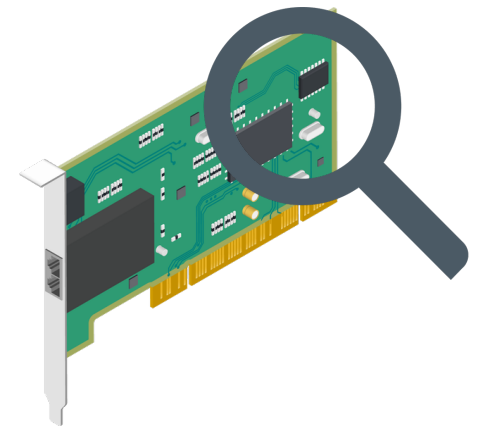
Discussing Remote Access Configuration

30bird 10.2.5

What is SSH? https://www.youtube.com/watch?v=qWKK_PNHnnA

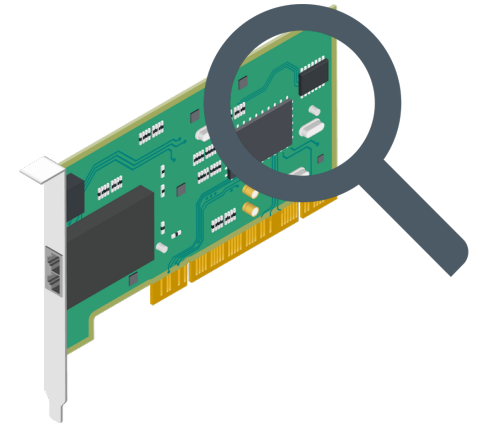
Common Wired Network Connectivity Issues (Slide 1 of 2)

- 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



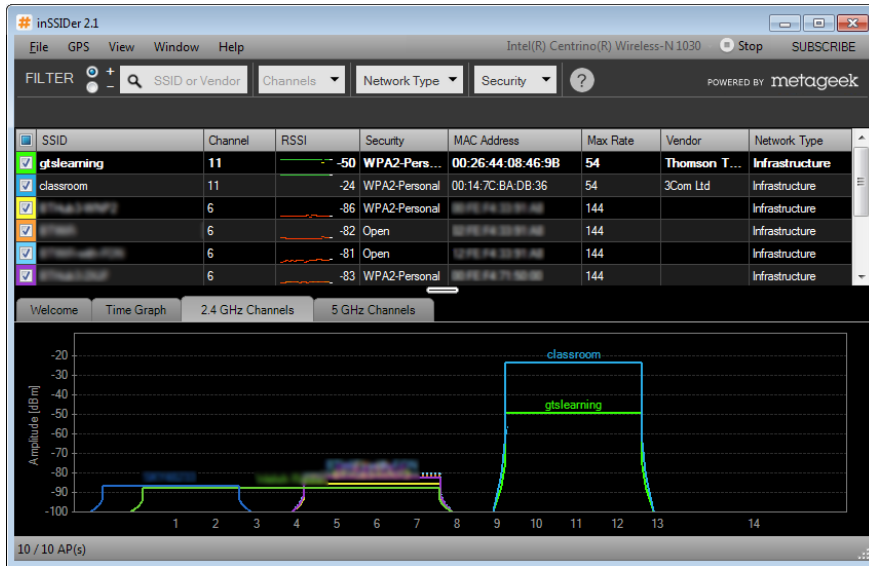
Common Wireless Network Connectivity Issues

(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)

```
C:\Users\Admin>ipconfig /all

Windows IP Configuration

Host Name . . . . . : ROGUE
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : classroom.local

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . : classroom.local
Description . . . . . : Microsoft Hyper-U Network Adapter
Physical Address. . . . . : 00-15-5D-01-CA-0E
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv4 Address. . . . . : 10.1.0.131<Preferred>
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Wednesday, January 4, 2017 2:40:05 AM
Lease Expires . . . . . : Thursday, January 12, 2017 2:40:03 AM
Default Gateway . . . . . : 10.1.0.254
DHCP Server . . . . . : 10.1.0.1
DNS Servers . . . . . : 10.1.0.1
NetBIOS over Tcpip. . . . . : Enabled
```

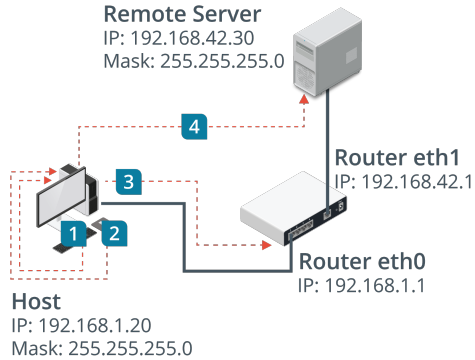
- Use `ipconfig` to test adapter configuration:
 - Static or DHCP? If DHCP, correct parameters?
- If configuration is correct, check for:
 - Communication with DHCP server
 - Configuration with DHCP server
 - Multiple conflicting DHCP servers
- On Linux, use `ifconfig`; some different functionality

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)



```
C:\>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% lost),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.101.100

Pinging 192.168.101.100 with 32 bytes of data:
Reply from 192.168.101.100: bytes=32 time<1ms TTL=128
Reply from 192.168.101.100: bytes=32 time<1ms TTL=128
Reply from 192.168.101.100: bytes=32 time<1ms TTL=128
Reply from 192.168.101.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.101.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% lost),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.200

Pinging 192.168.1.200 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.200:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% lost),
```

- 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 (IP address already in use)
 - 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

```
C:\Users\localadmin>tracert 10.0.0.1
Tracing route to 10.0.0.1 over a maximum of 30 hops
  1  HOST [192.168.1.110]  reports: Destination host unreachable.
Trace complete.
C:\Users\localadmin>tracert gtslearning.com
Tracing route to gtslearning.com [185.41.10.123]
over a maximum of 30 hops:
  1  <1 ms    <1 ms    <1 ms    ARCHER_UR900 [192.168.1.1]
  2  *         *         *         Request timed out.
  3  *         11 ms    11 ms    31.55.187.181
  4  11 ms    11 ms    11 ms    31.55.187.188
  5  12 ms    11 ms    11 ms    core2-hu0-17-0-1.southbank.ukcore.bt.net [195.99
.127.188]
  6  12 ms    12 ms    12 ms    195.99.127.70
  7  13 ms    13 ms    13 ms    peer2-et-9-1-0.redbus.ukcore.bt.net [62.172.103.
43]
  8  13 ms    13 ms    18 ms    linx2.ixreach.com [195.66.236.217]
  9  20 ms    20 ms    20 ms    r1.tcw.man.ixreach.com [91.196.184.181]
 10  19 ms    23 ms    20 ms    rt1-tjh-ixr.as200083.net [46.18.174.222]
 11  20 ms    20 ms    20 ms    server1.gtslearning.com [185.41.10.123]
Trace complete.
C:\Users\localadmin>_
```

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 1st client
 - If fails, problem is with server, device, or infrastructure



Unavailable Resources (Slide 2 of 5)

- 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)



Unavailable Resources (Slide 3 of 5)

- 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    192.168.1.110:5806     185.41.10.123:80      CLOSE_WAIT
[IEXPLORE.EXE]
TCP    192.168.1.110:5807     185.41.10.123:80      CLOSE_WAIT
[IEXPLORE.EXE]
TCP    192.168.1.110:5808     216.58.208.40:443     ESTABLISHED
[IEXPLORE.EXE]
TCP    192.168.1.110:5809     216.58.208.40:443     ESTABLISHED
[IEXPLORE.EXE]
TCP    192.168.1.110:5810     104.27.151.216:80     CLOSE_WAIT
[IEXPLORE.EXE]
TCP    192.168.1.110:5811     104.27.151.216:80     CLOSE_WAIT
[IEXPLORE.EXE]
TCP    192.168.1.110:5812     104.27.151.216:80     CLOSE_WAIT
[IEXPLORE.EXE]
TCP    192.168.1.110:5813     104.27.151.216:80     CLOSE_WAIT
[IEXPLORE.EXE]
TCP    192.168.1.110:5814     104.27.151.216:80     CLOSE_WAIT
[IEXPLORE.EXE]
TCP    192.168.1.110:5815     104.27.151.216:80     CLOSE_WAIT
[IEXPLORE.EXE]
TCP    192.168.1.110:5816     52.28.192.217:443     ESTABLISHED
[IEXPLORE.EXE]
TCP    [fe80::5c9e:8be5:bb3e:f341%4]:2179 [fe80::5c9e:8be5:bb3e:f341%4]:5519
ESTABLISHED
[onms.exe]
TCP    [fe80::5c9e:8be5:bb3e:f341%4]:3587 [fe80::5cf0:94fe:4f4:a8a%4]:57395
ESTABLISHED
p2psvc
[svchost.exe]
TCP    [fe80::5c9e:8be5:bb3e:f341%4]:5519 [fe80::5c9e:8be5:bb3e:f341%4]:2179
ESTABLISHED
[UmConnect.exe]
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.c
om
```

Activity



Discussing Network Connection Troubleshooting
<https://www.youtube.com/watch?v=vJV-GBZ6PeM>

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

| Technology | Description |
|---|---|
| Bluetooth Bluetooth Low Energy | <ul style="list-style-type: none">• Radio communication speeds up to 3 Mbps; v3 or v4 up to 24 Mbps• Maximum range of 10 m/30 ft (signal strength weak at max. distance)• Used in many portable/wearable devices• Pairing procedure• BLE version for low-powered devices that transmit infrequently |
| Z-Wave | <ul style="list-style-type: none">• Wireless protocol for home automation• Mesh topology over low-energy radio waves• Can configure repeaters up to four “hops”• High 800-low 900 MHz range; runs for years on battery power |
| ZigBee | <ul style="list-style-type: none">• Similar to/competitive with Z-Wave• 2.4 GHz band• Up to 65,000 devices in single network (232 for Z-Wave); no hop limit |
| RFID and NFC | <ul style="list-style-type: none">• Tagging and tracking devices with radio-frequency tags• NFC: peer-to-peer version of RFID |

IoT Device Configuration

- IoT functionality in home automation/smart home devices
- To interoperate, devices must all share protocol (i.e., Z-Wave or Zigbee mesh protocols) 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

Activity



Discussing IoT Devices

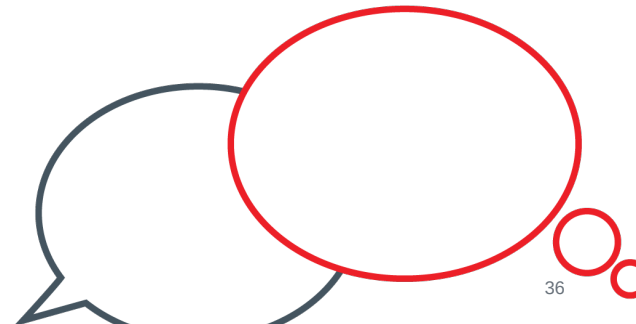
Activity



Configuring IoT Devices PBQ Activity

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?



Reflective Questions

Read Chapter 11, 12, 13

