Configuring and Troubleshooting Networks

CompTIA®

Configuring and Troubleshooting Networks

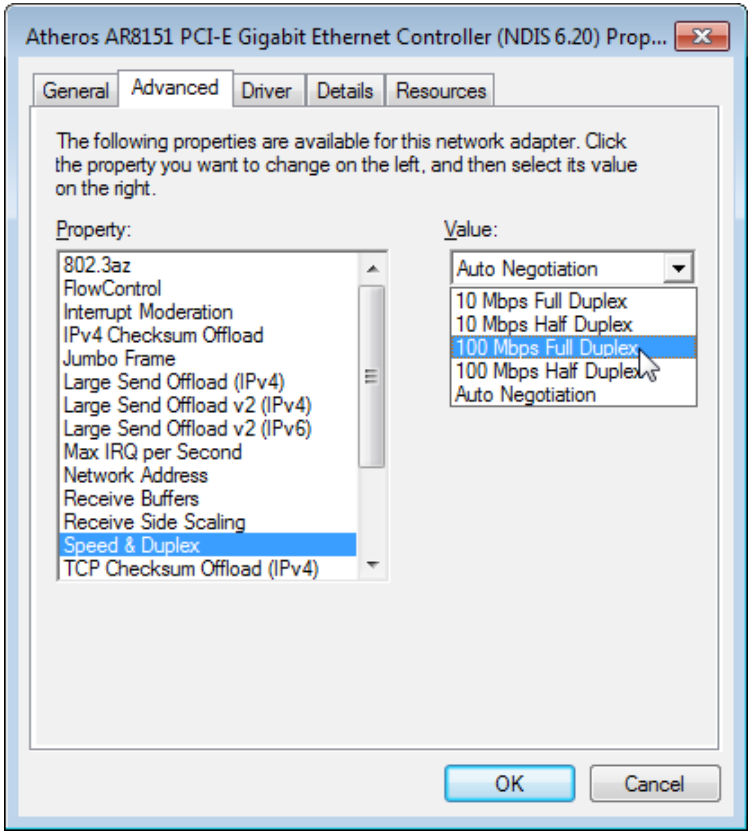
- Configure Network Connection Settings
- Install and Configure SOHO Networks
- Configure SOHO Network Security
- Configure Remote Access
- Troubleshoot Network Connections
- Install and Configure IoT Devices

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

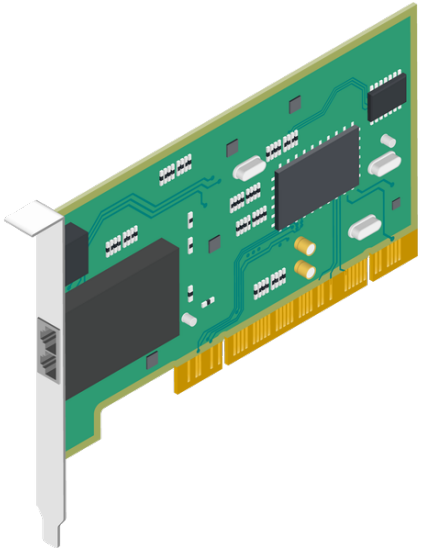


QoS (Quality of Service)

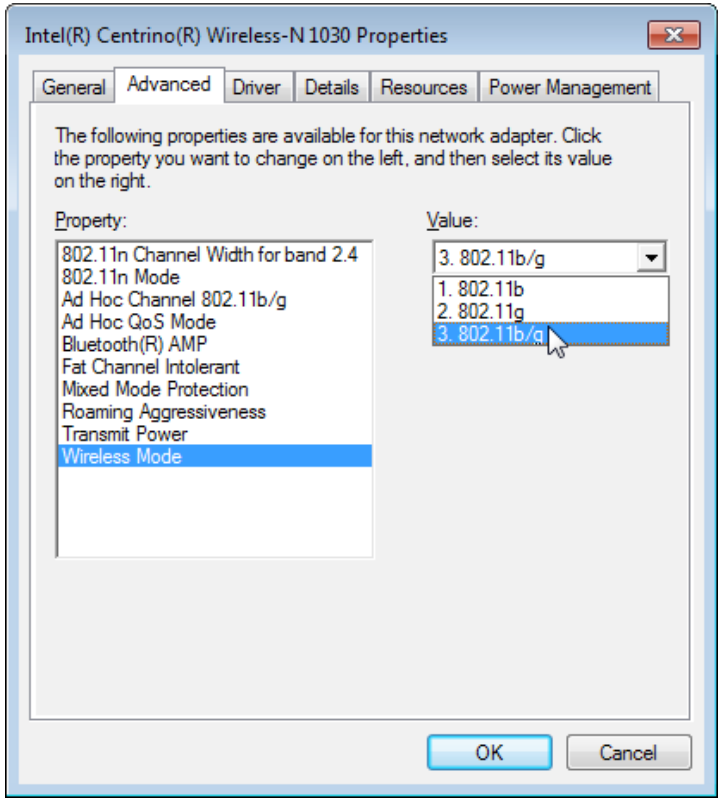
- Network protocol that prioritizes some types of traffic.
- Can help ensure real-time applications such as VoIP or video conference have priority.
- QoS usually configured on managed switches.
- May need to enable QoS protocol on adapter.

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.



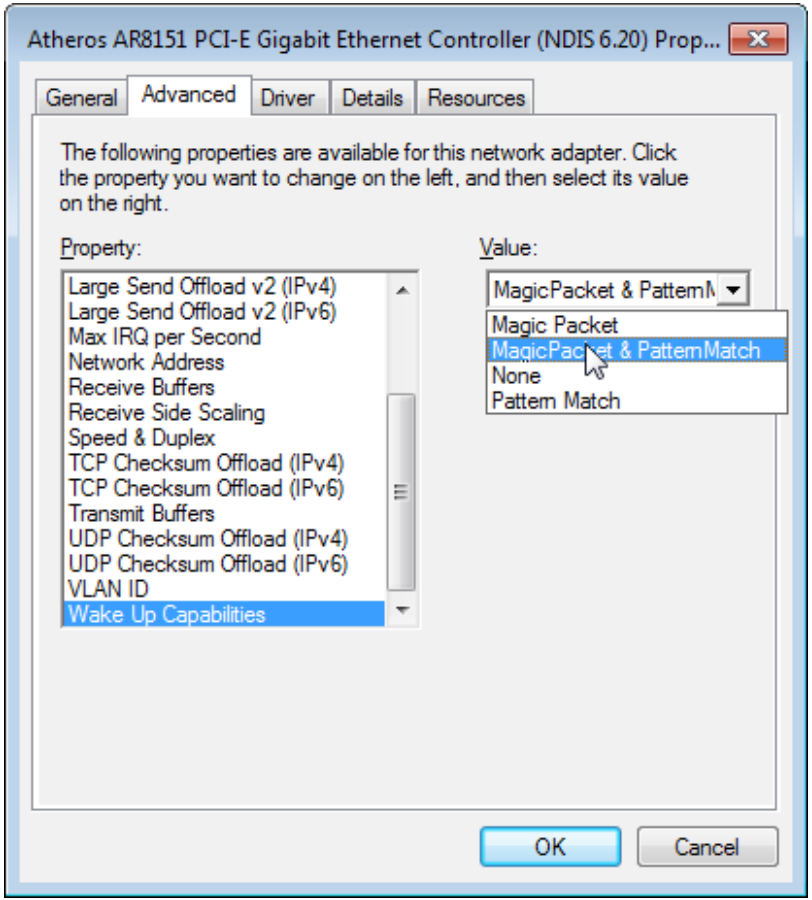
Wireless Network Cards



- 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

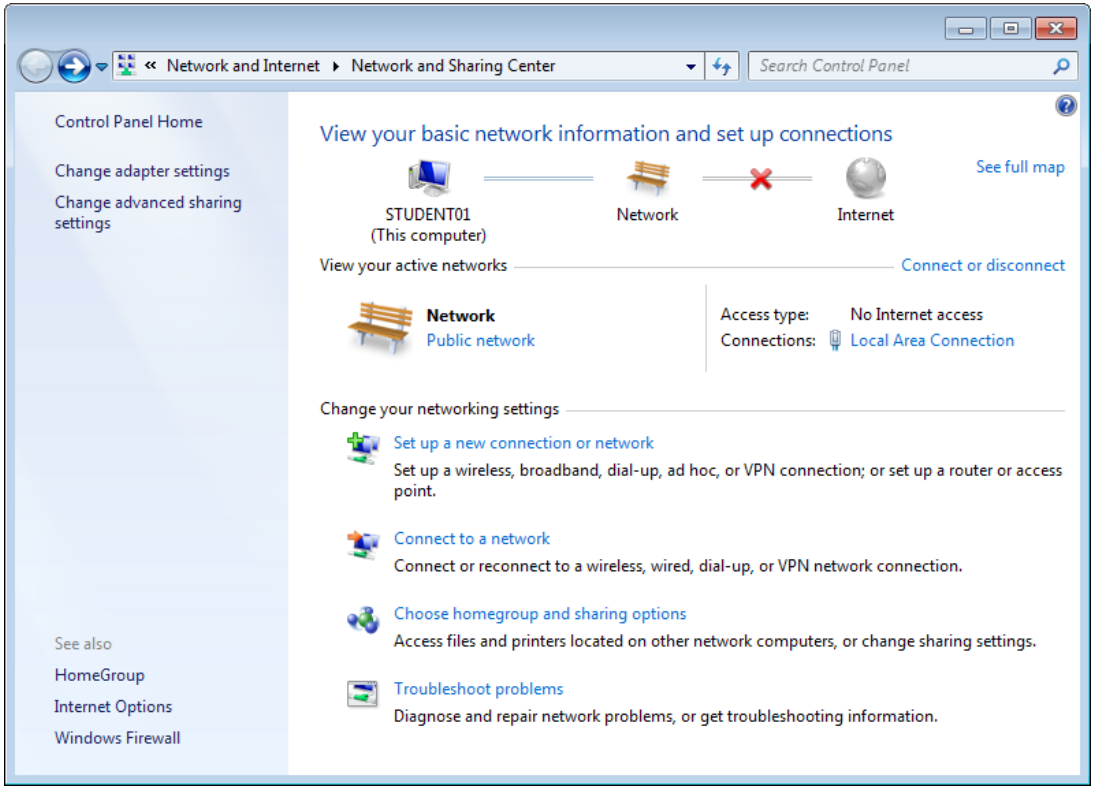
Wake on LAN

- 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



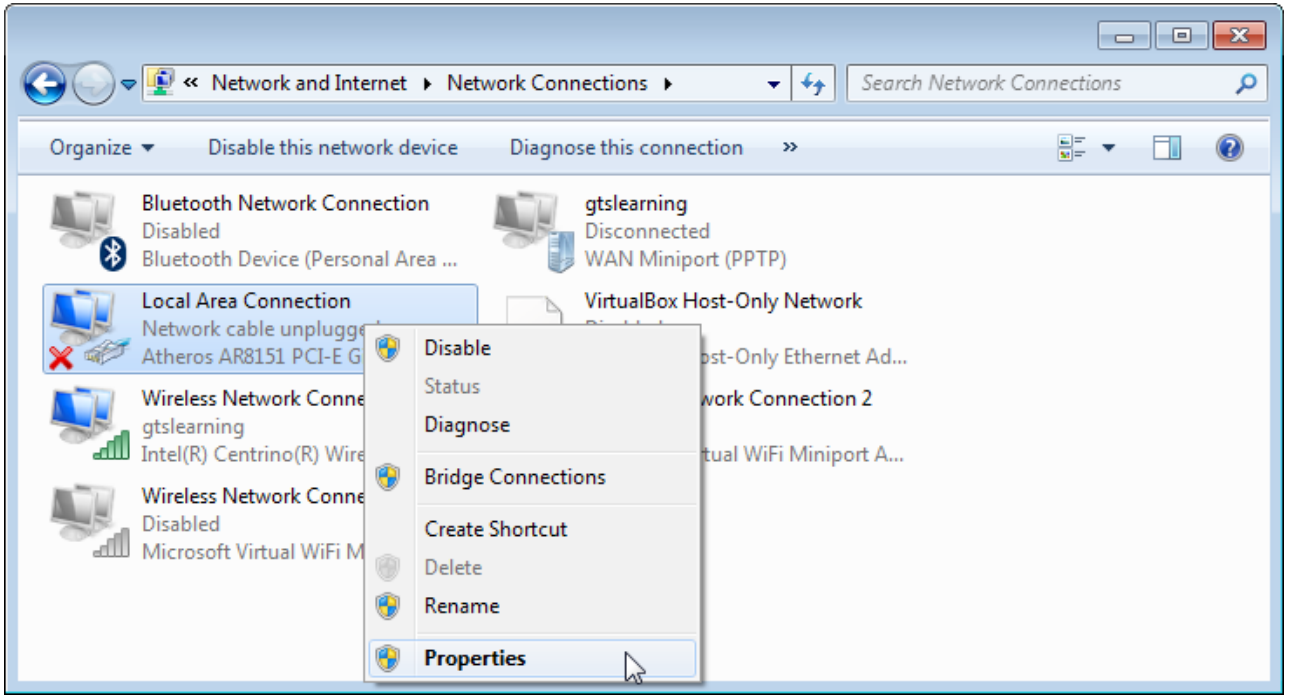
Network Connections in Windows 7 and Windows 8 (Slide 1 of 4)

- Configure network card with client software and protocol
- Use Network and Sharing Center



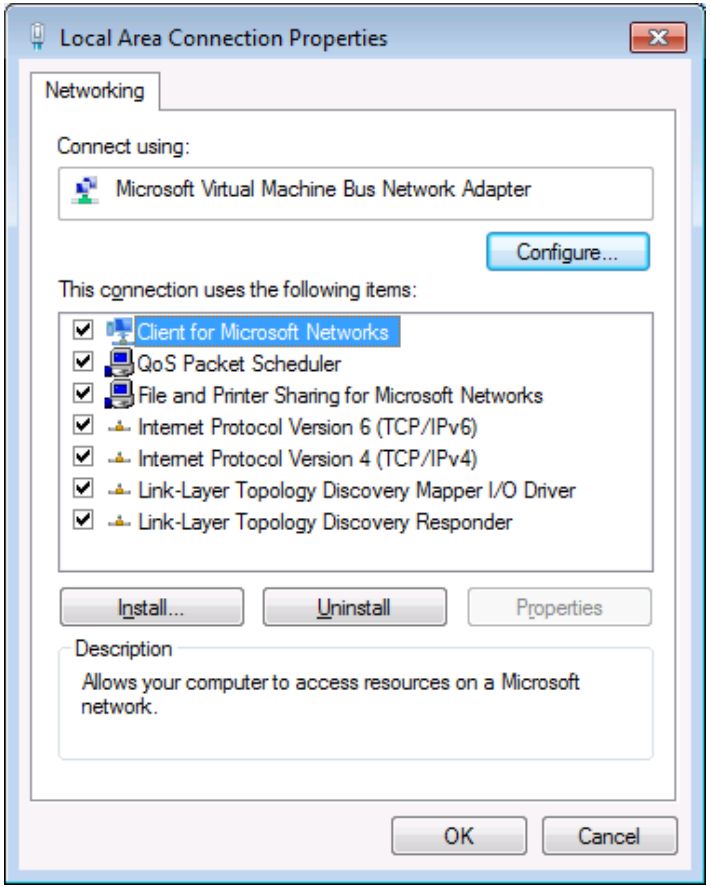
Network Connections in Windows 7 and Windows 8 (Slide 2 of 4)

- Access adapter properties
- Wired/wireless adapter names vary



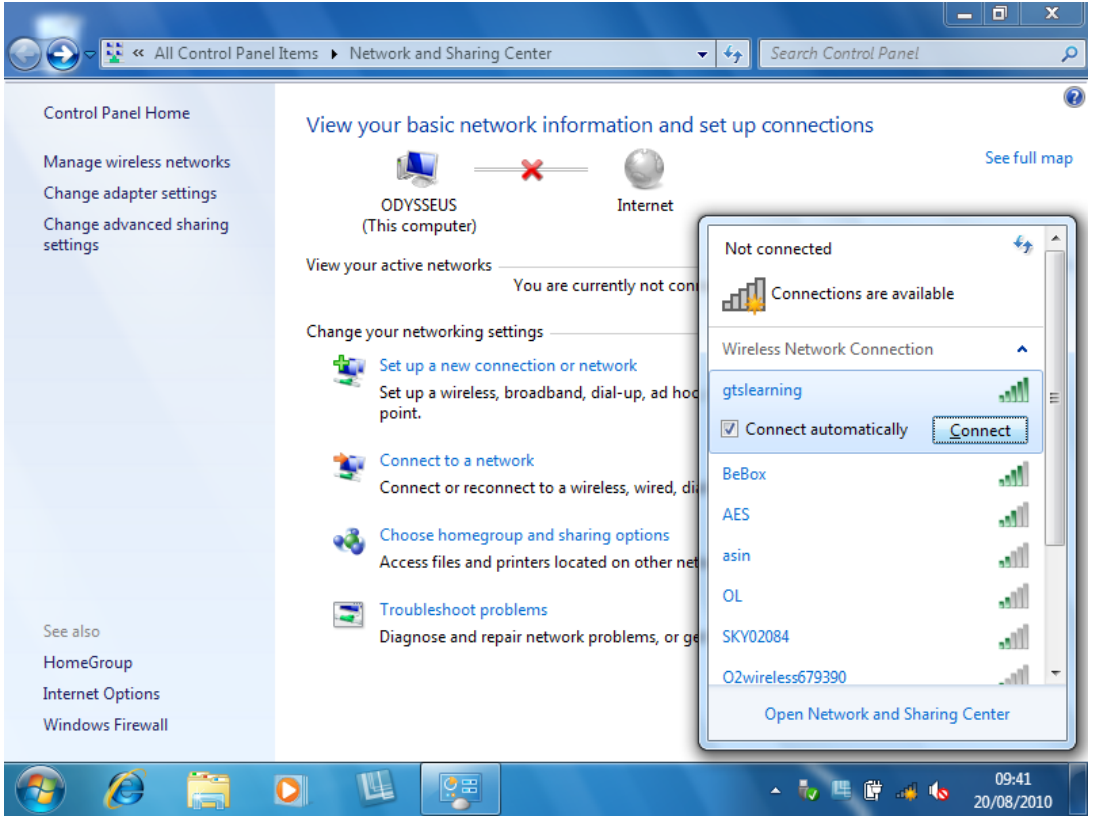
Network Connections in Windows 7 and Windows 8 (Slide 3 of 4)

- Change properties or view status
- Configure client, protocol, service
- Default bindings include Microsoft clients, IPv4 and IPv6, and link-layer discovery

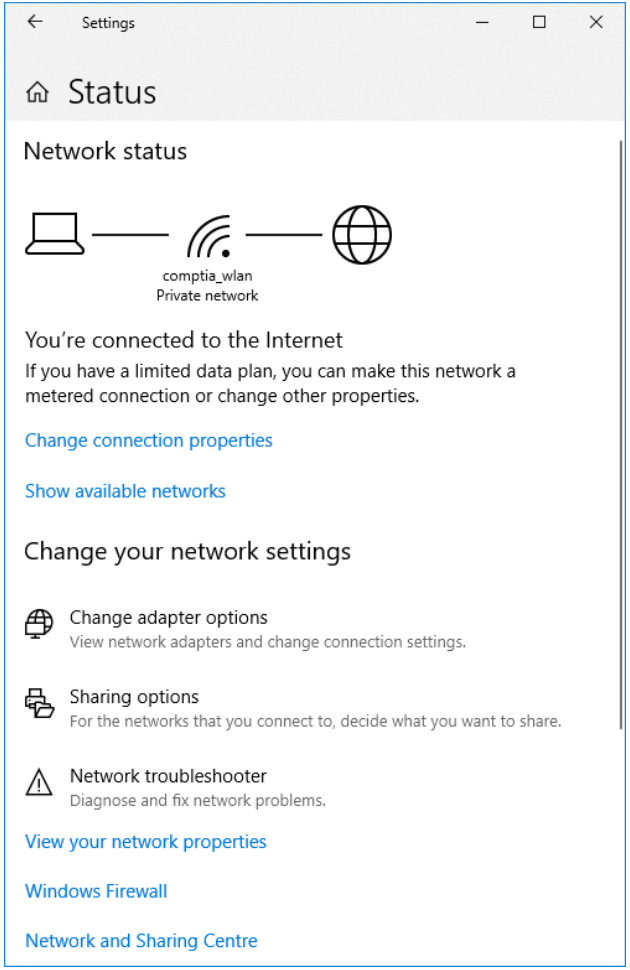


Network Connections in Windows 7 and Windows 8 (Slide 4 of 4)

- To join WLAN, select network from list in notification area
- Can connect automatically
- Can configure manually if network not broadcasting



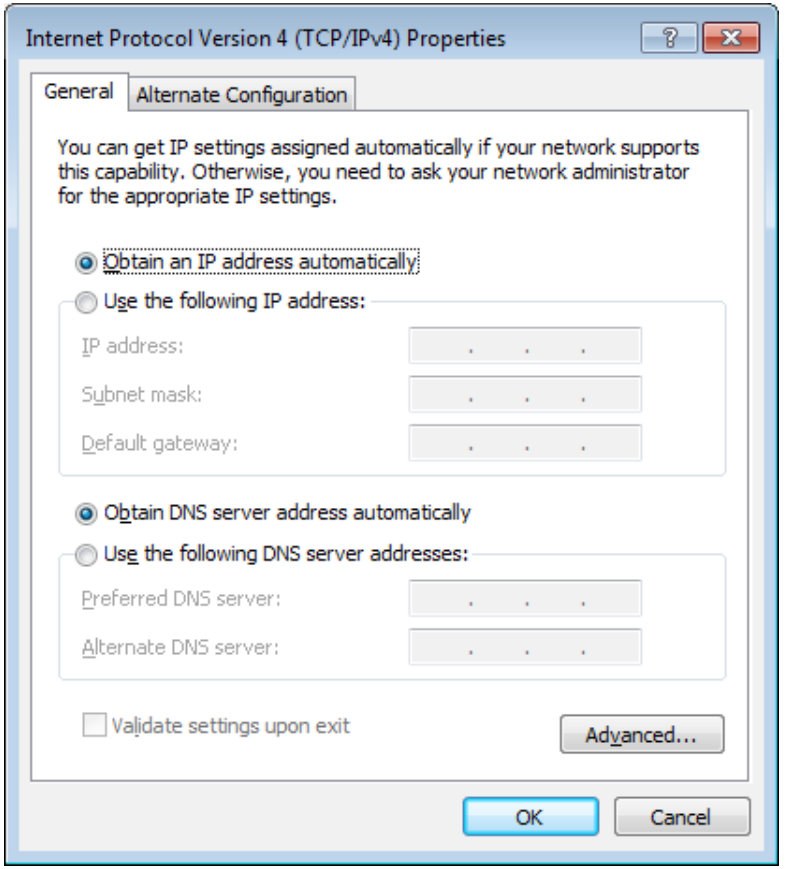
Network Connections in Windows 10



- Settings: Network & Internet
- Use to access Network and Sharing Center and Network Connections applets

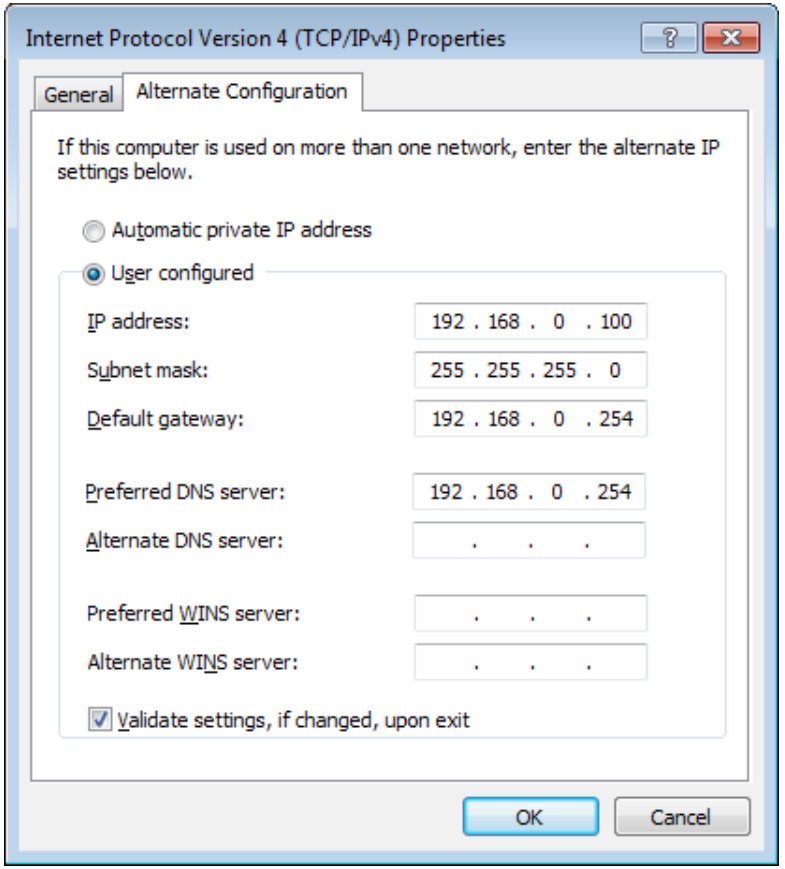
IP Address Configuration (Slide 1 of 2)

- Configure wired and wireless through connection's Properties
- Default is dynamic IP
- Can configure a static IP address manually

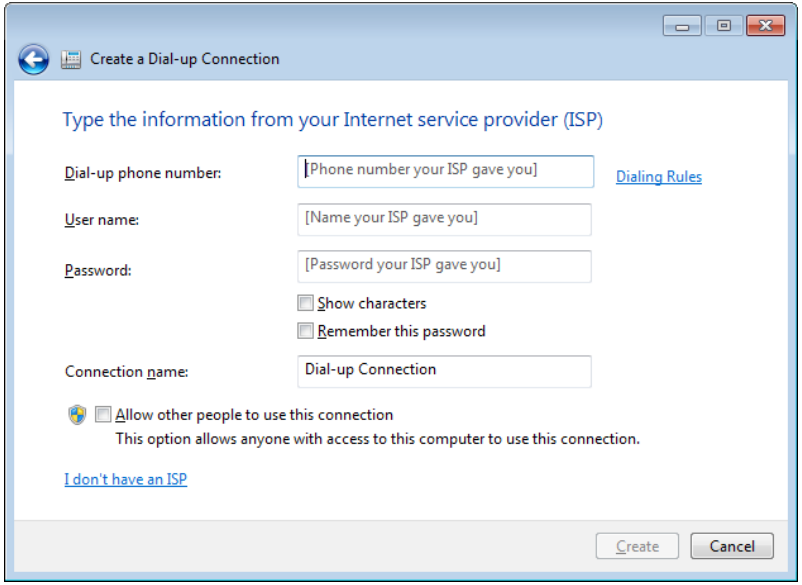


IP Address Configuration (Slide 2 of 2)

- Select “Obtain an IP address automatically” for DHCP/APIPA
- Can set up alternate configuration if desired

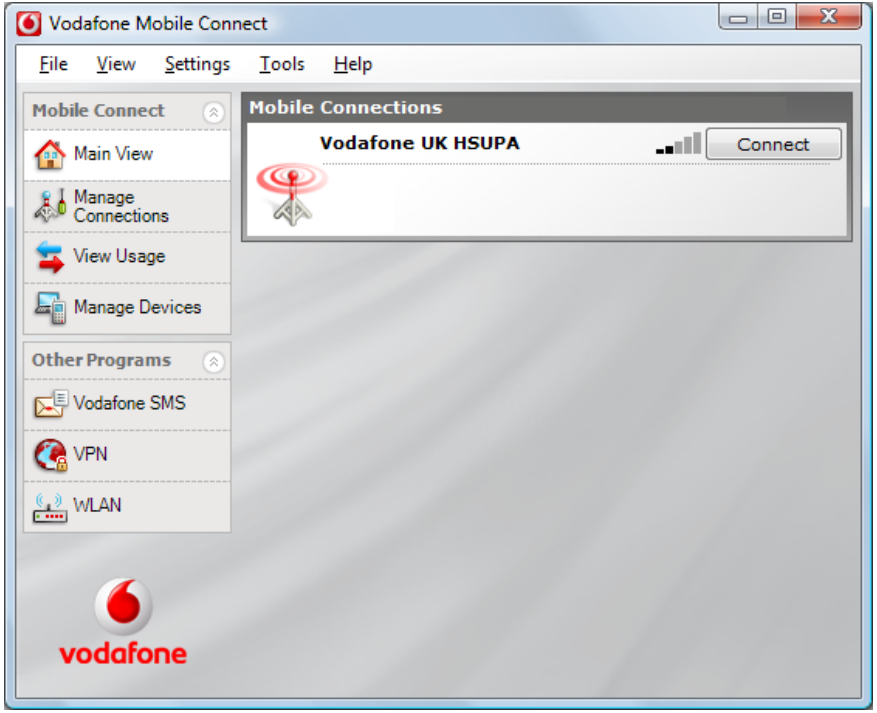


Other Network Connections (Slide 1 of 3)



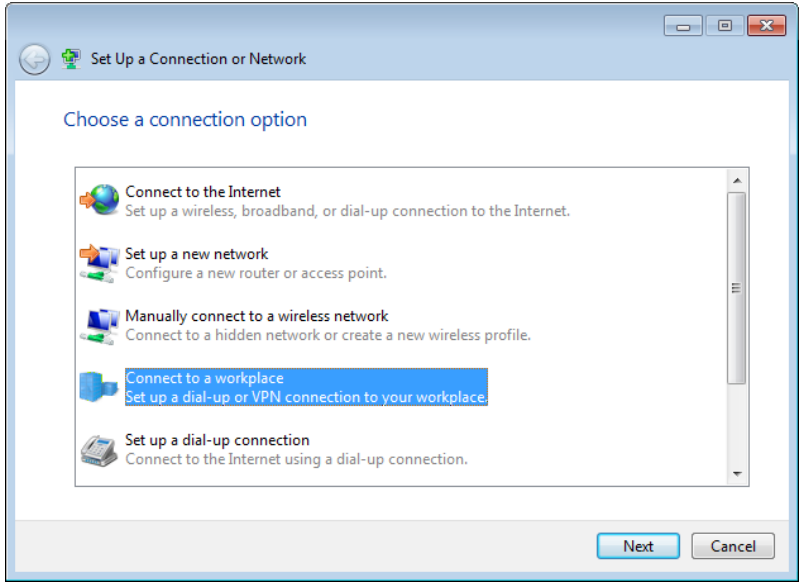
- SOHO router is typical; usually combines several functions
- Other connection options include dial-up
- Analog modem connects to ISP
- Use Set Up a Connection or Network to configure

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

Other Network Connections (Slide 3 of 3)



- VPN tunnels privately through network
- Windows supports several types; can configure in Network Connections
- Click network status icon to access

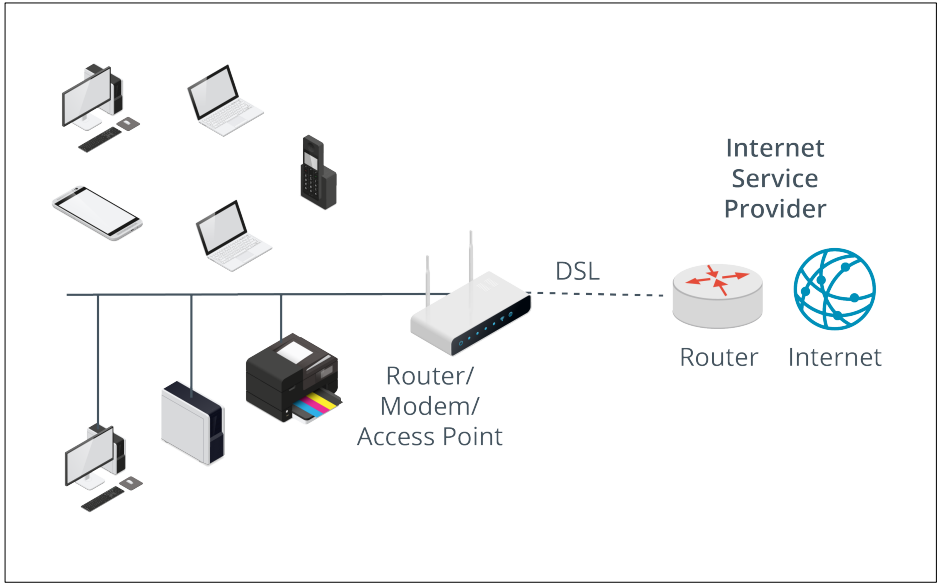
Activity

Discussing Network Connection Configuration Settings

https://www.youtube.com/watch?v=dgKy-mtL6N4

SOHO Networks

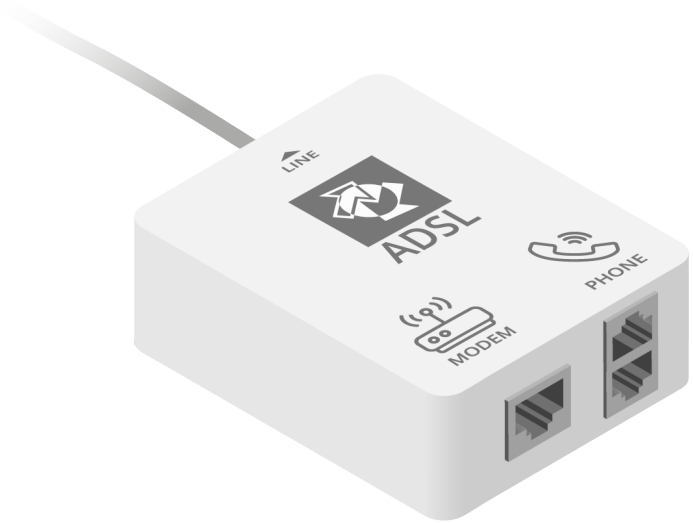
- Business network; may use centralized server as well as clients.
- Often uses single Internet device for connectivity.
- May be home/residential network as well.



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.

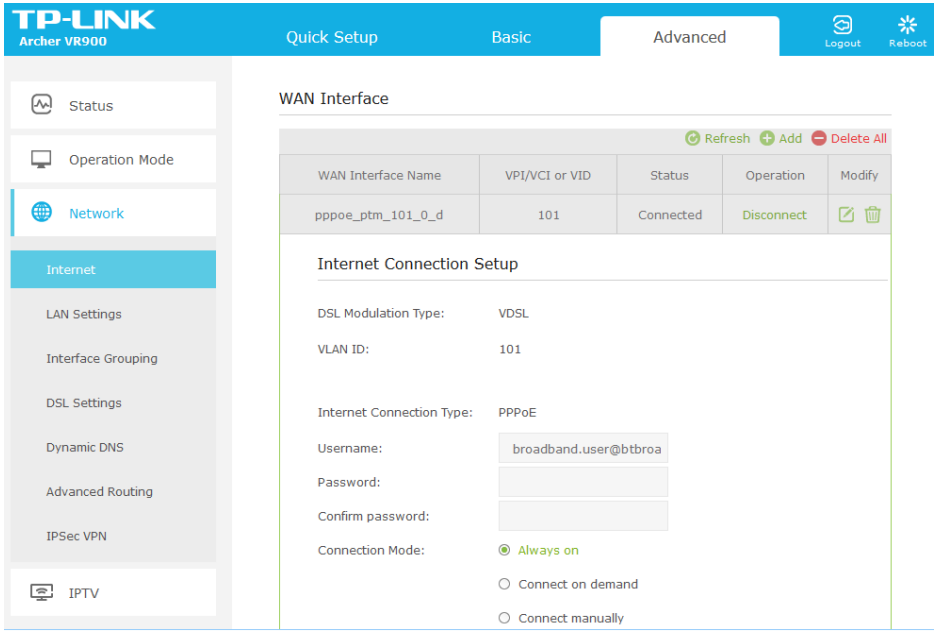
Common SOHO Network Hardware (Slide 2 of 2)



- On DSL, RJ-11 port connects to phone jack.
- Voice/data splitter usually part of modern socket.

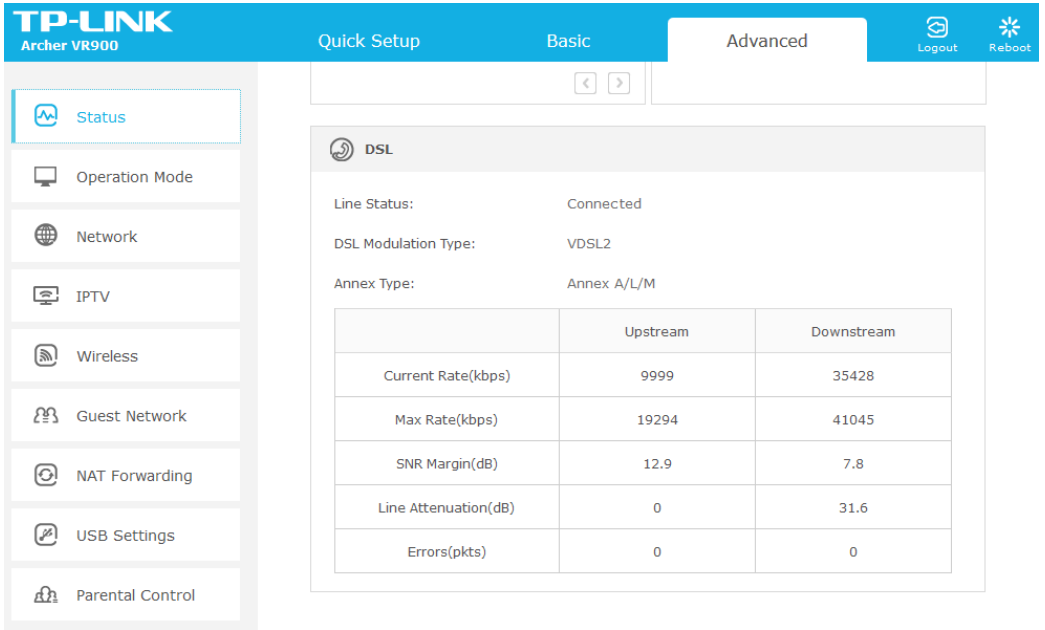
SOHO Network Configuration (Slide 1 of 2)

- Connect device to SOHO appliance to configure.
- Access management interface through browser.
- Change default password!
- Follow wizard interface to configure Internet access.



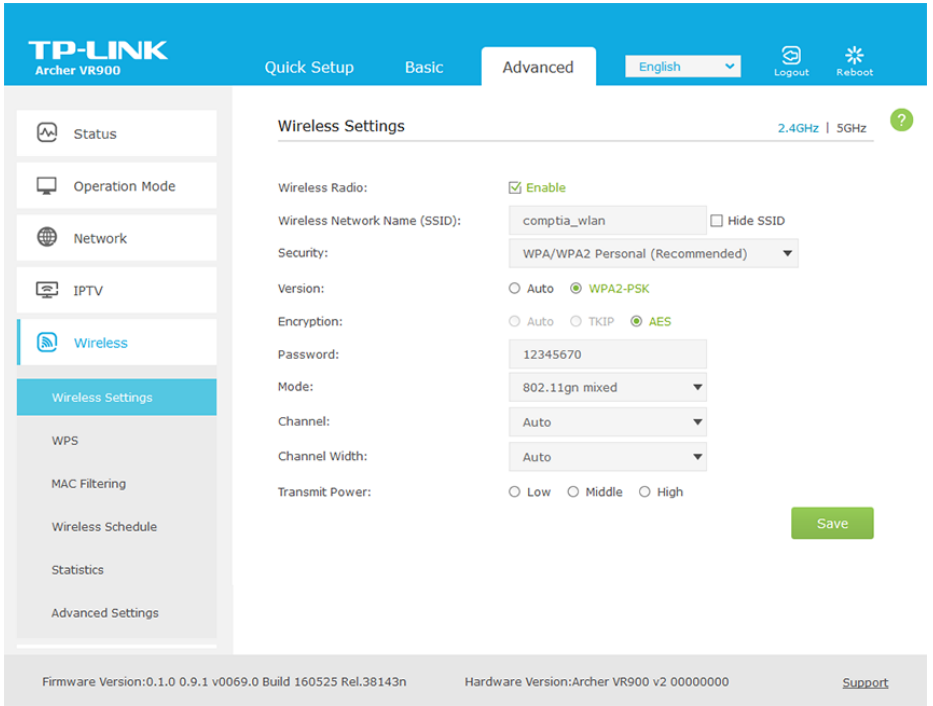
SOHO Network Configuration (Slide 2 of 2)

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

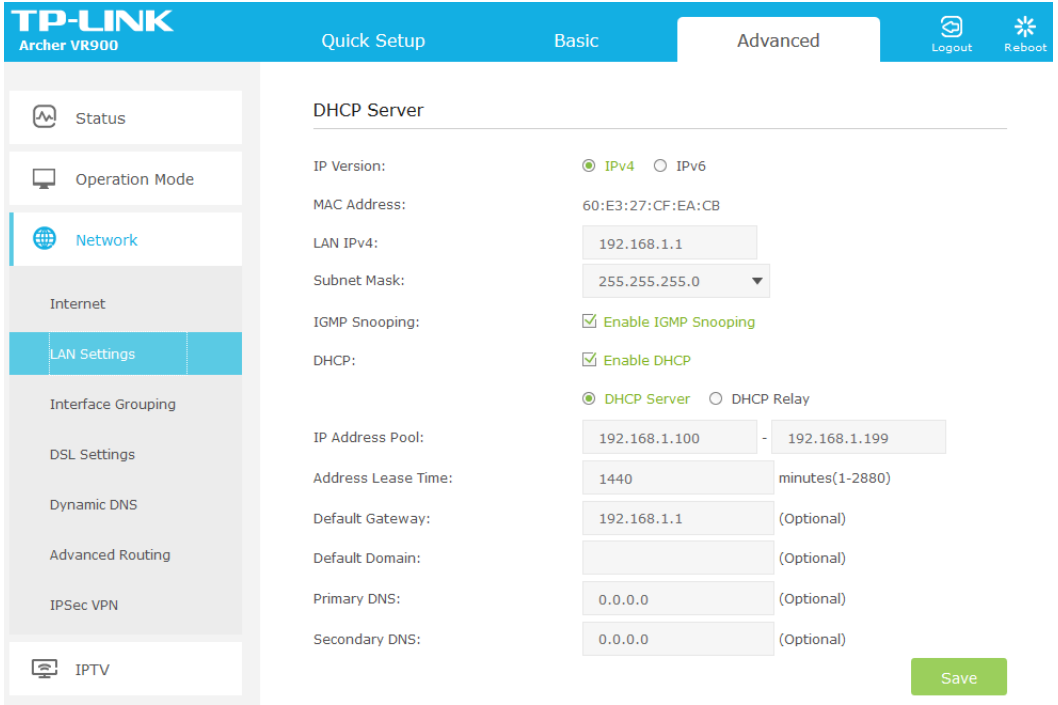


Wireless Settings

- 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

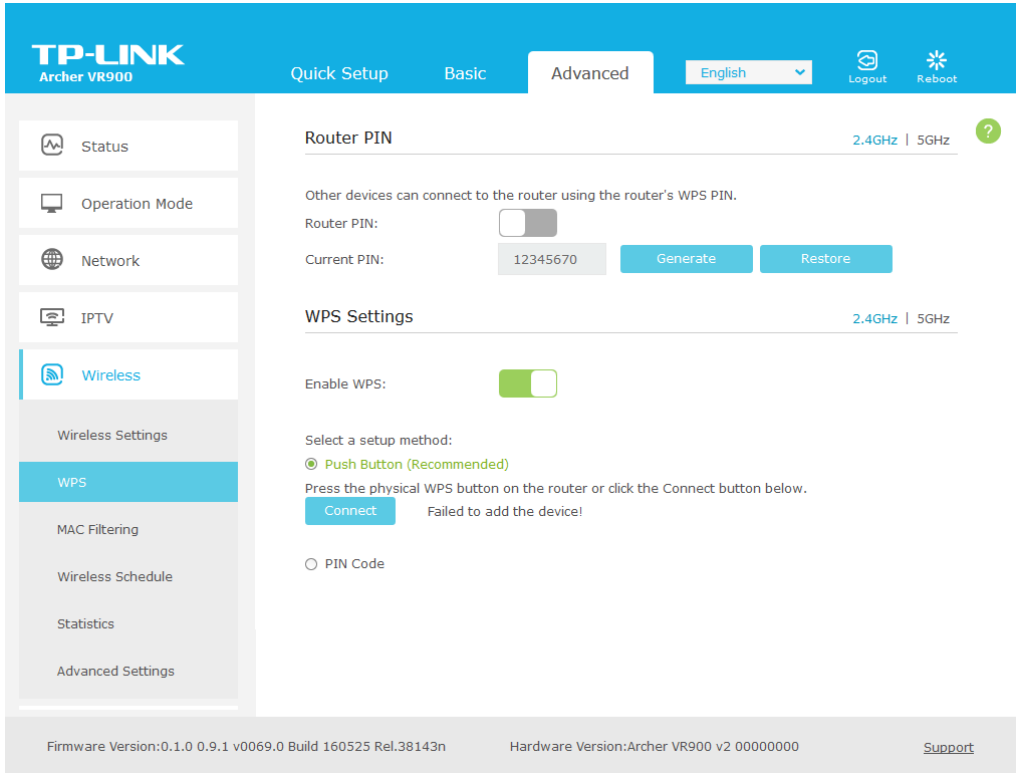


DHCP and IP Address Configuration



- 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



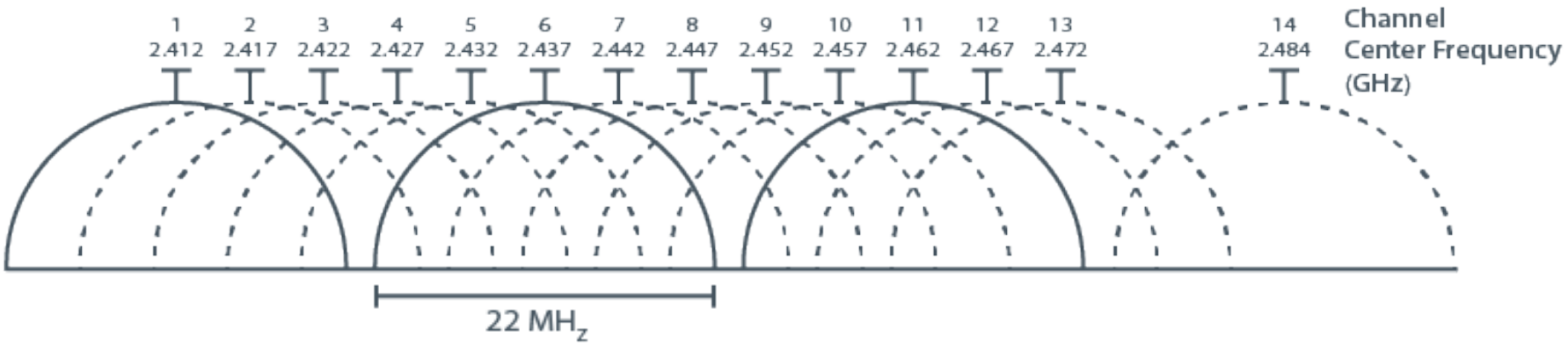
- Simplifies secure access point setup.
- AP and all adapters must be WPS-capable.
- Pushbutton on device typically causes device and AP to associate automatically over WPA2.
- Generates random SSID and passphrase.

Access Point Placement

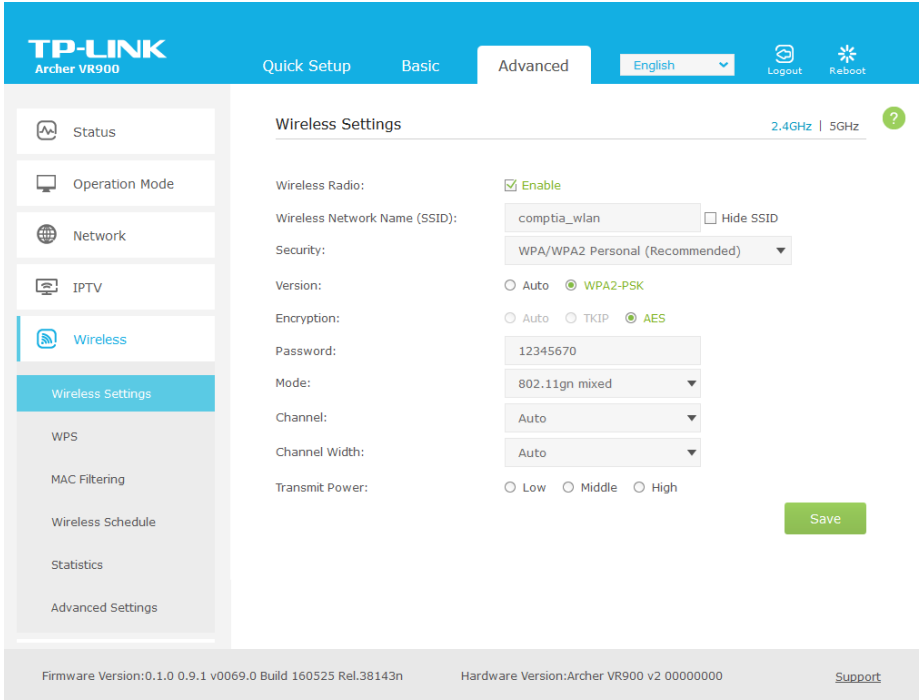
- Correct antenna and access point placement helps ensure robust network.
- AP placement may be constrained by provider's cabling location.
- Can use extenders.
- Site survey can help identify dead zones.

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)

Security Protocol	Description
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 **WPA2**	• 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

Wi-Fi Authentication

Authentication Mode	Description
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

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

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

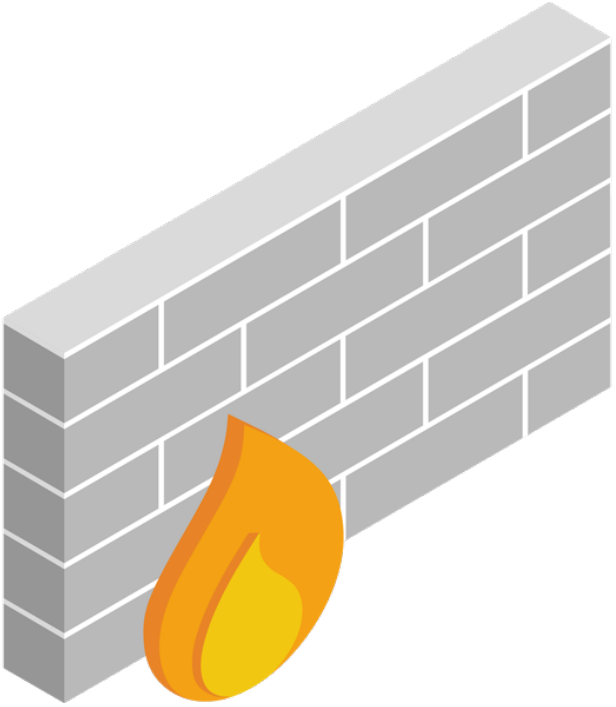
Discussing SOHO Network Installation and Configuration

Activity

Installing and Configuring SOHO Networks

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)

Firewall Type	Description

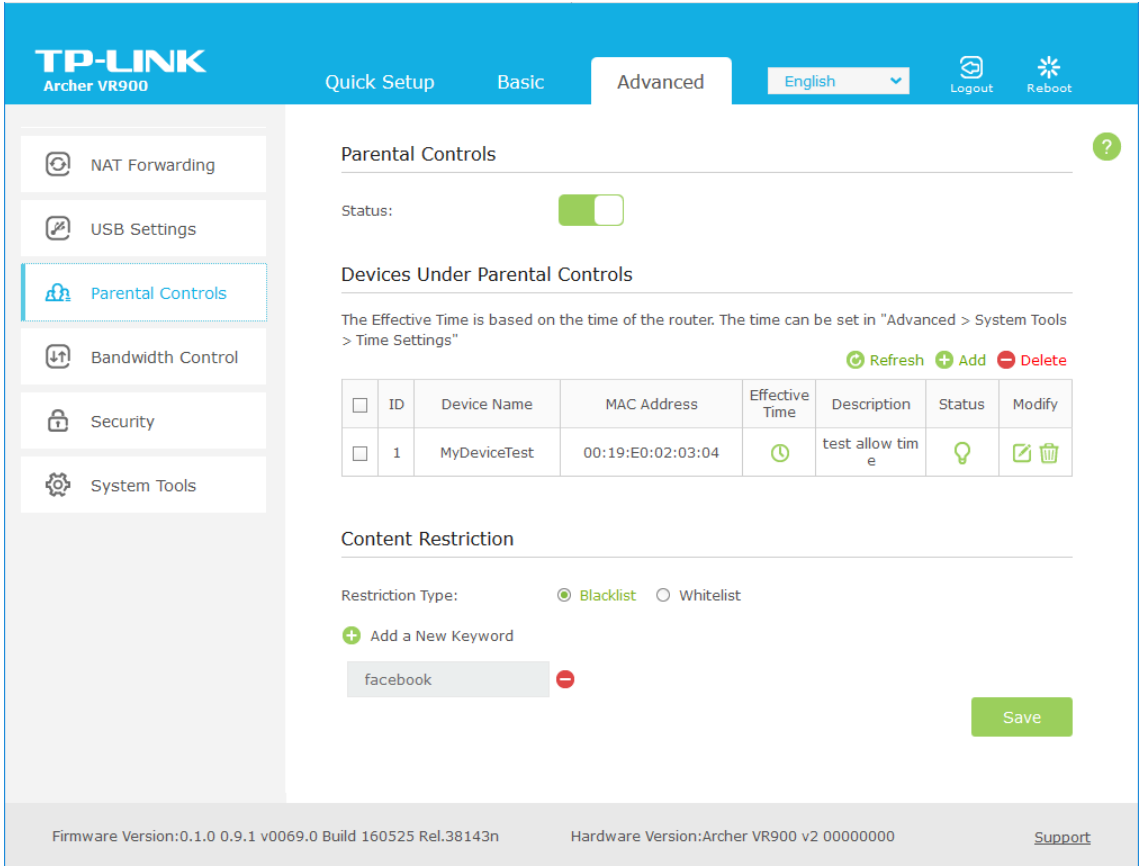
Packet Filtering	• Earliest type; all firewalls capable of this function
	• Inspects IP packet headers, accepts or drops based on rules
	• Filtering rules based on:
	  • IP filtering
	  • Protocol ID/type
	  • Port filtering/security
	• Configure ACL

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)

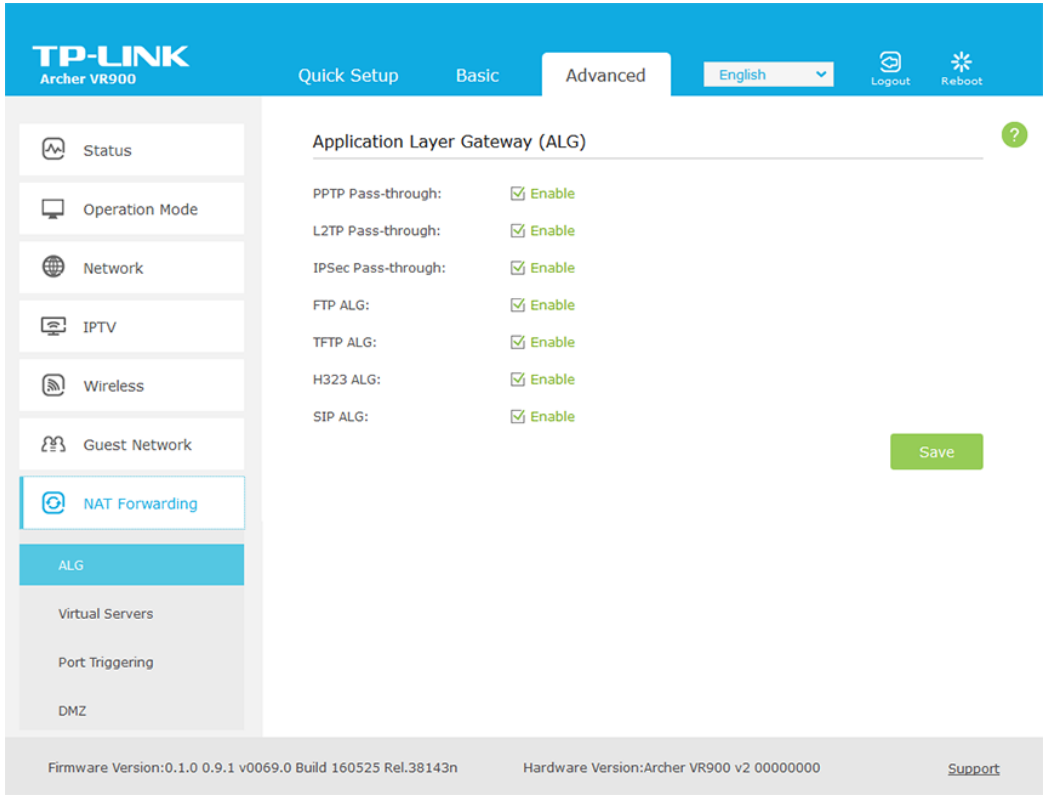
Firewall Setting	Description
Disabling Ports	• Only enable required services; can remove service at the host. • May want service available locally but not on Internet. • Configure firewall ACL to block the port, or block by default rule.
MAC Filtering	• Firewalls, switches, and APs can whitelist/blacklist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

Firewall Settings (Slide 2 of 2)

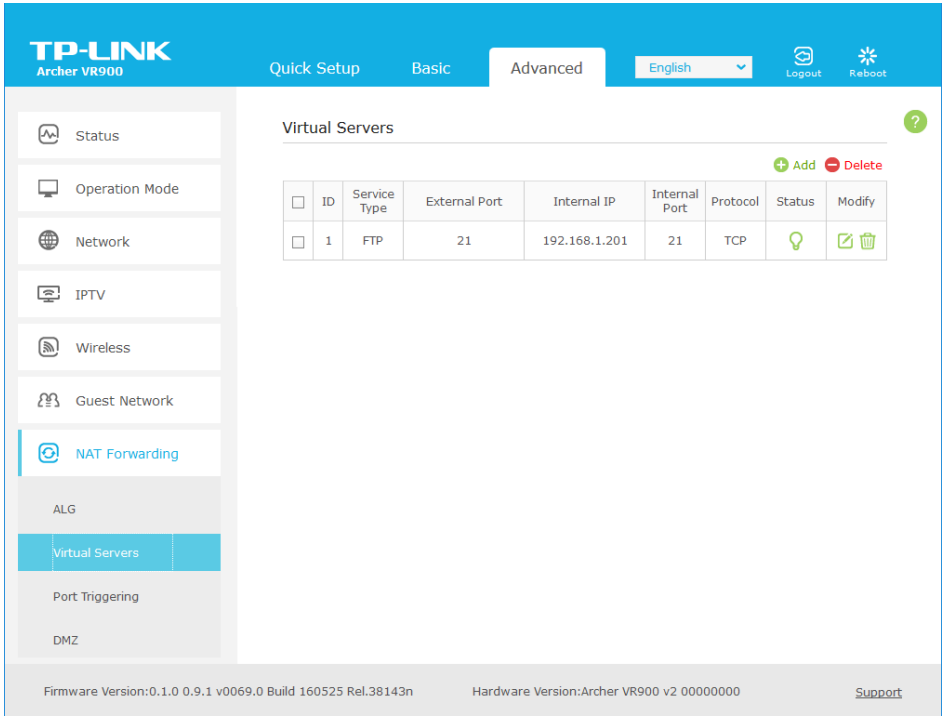


NAT

- 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



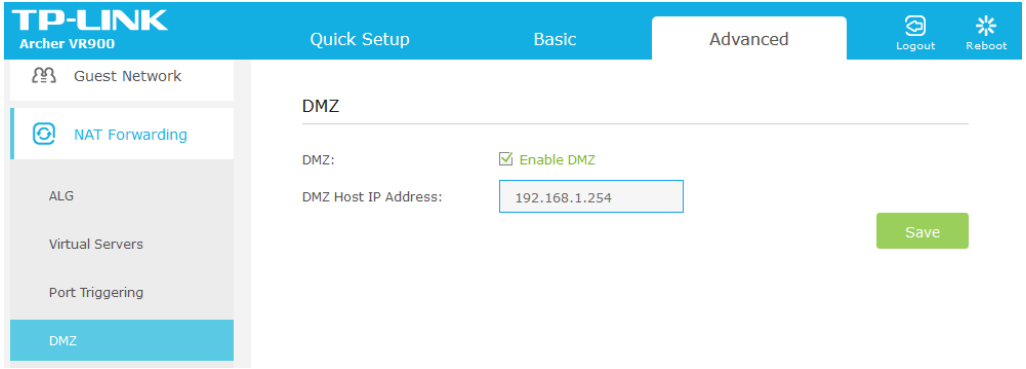
Port Forwarding and Port Triggering



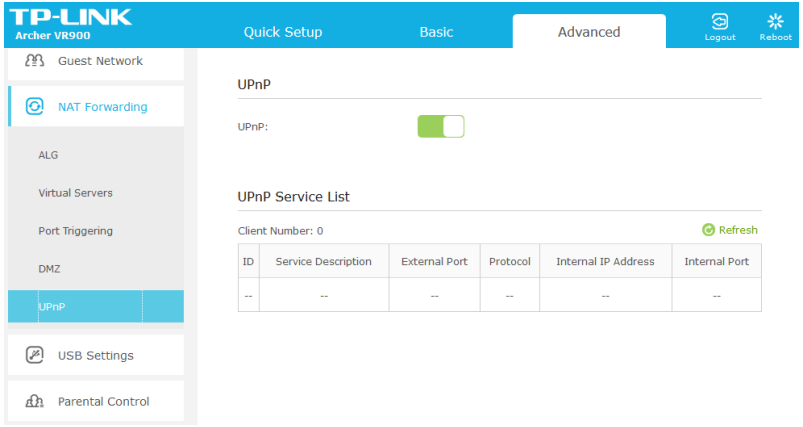
- Internet hosts only see router's public address.
- Configure port forwarding/DNAT if running an Internet-facing service on your internal network.
- Router transmits Internet requests to a given port to a designated internal host.
- Port triggering is for applications using multiple ports.

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.



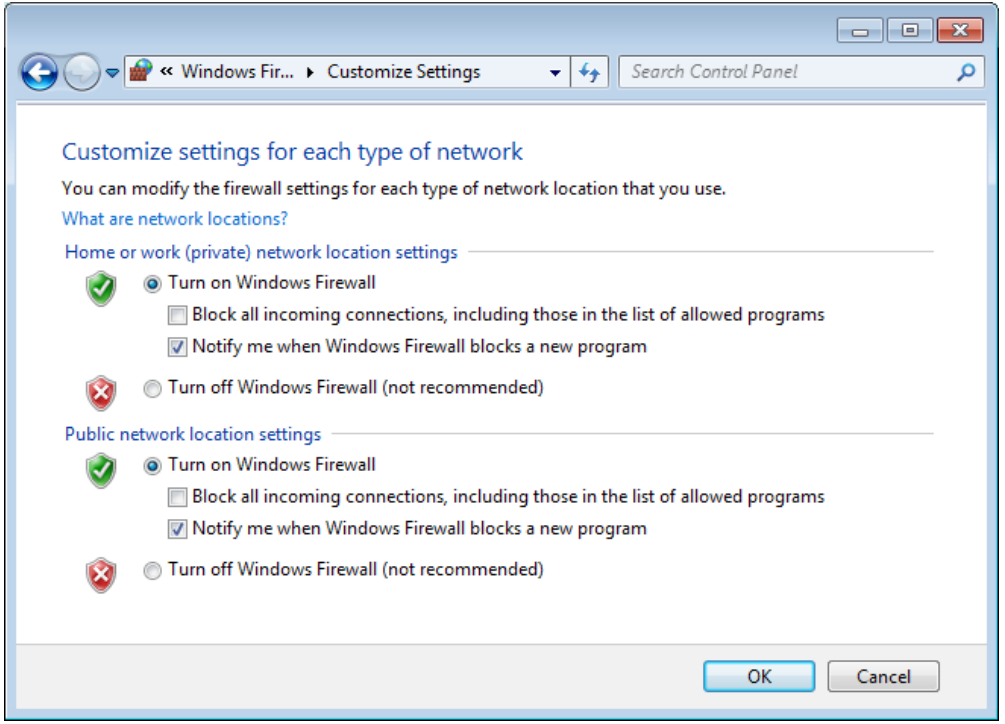
Universal Plug-and-Play



- 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.

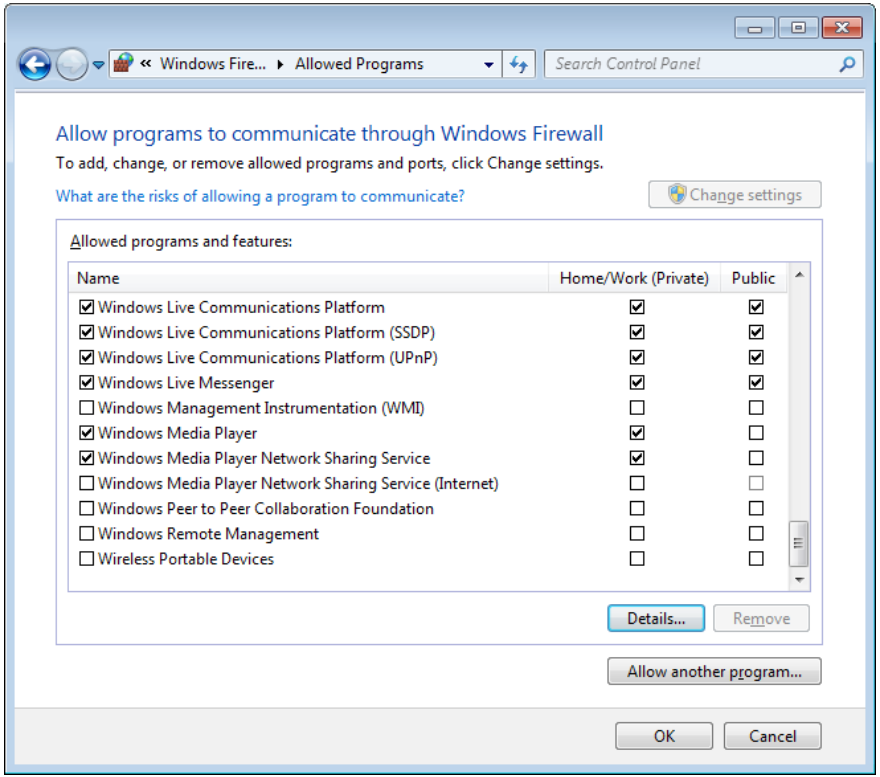
Windows Firewall (Slide 1 of 2)

- Each version has become more advanced
- Configure in Control Panel

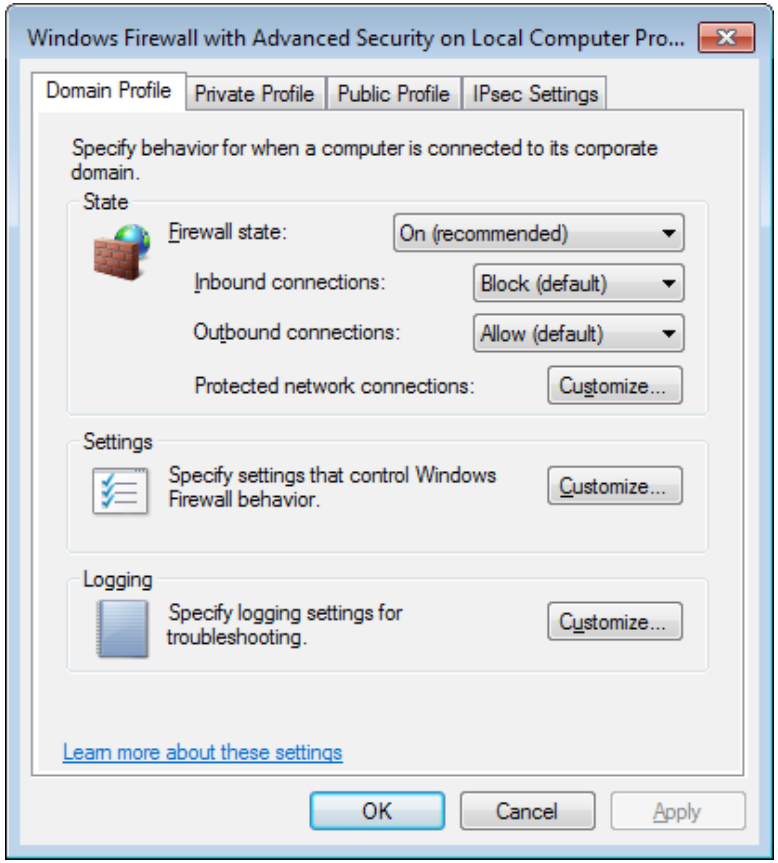


Windows Firewall (Slide 2 of 2)

- Can configure exceptions
- Use Windows Defender Security Center on Windows 10

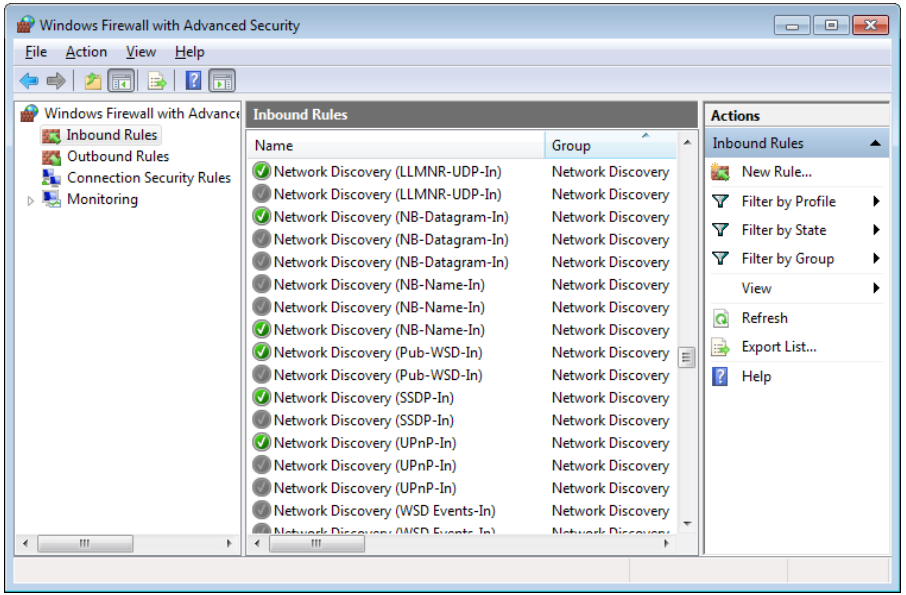


Windows Firewall with Advanced Security (Slide 1 of 2)



- Add-in to basic firewall
- Can configure outbound filtering, IPSec, monitoring
- Configure in Group Policy on domain, in management console in workgroup

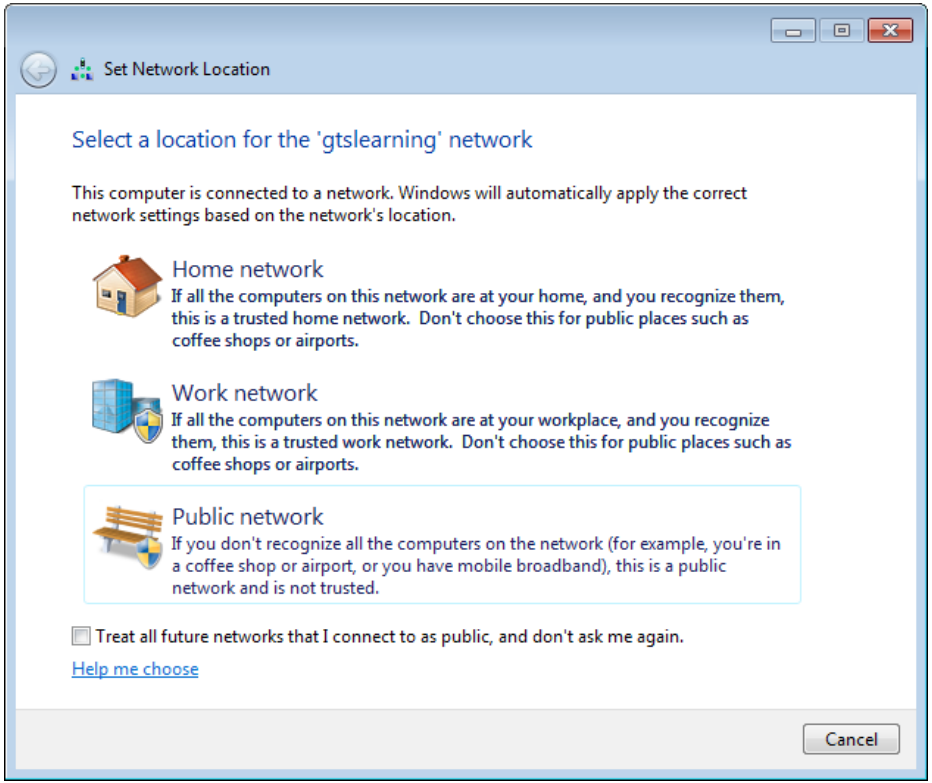
Windows Firewall with Advanced Security (Slide 2 of 2)



- Configure inbound and outbound rules as appropriate
- Rules can use various triggers

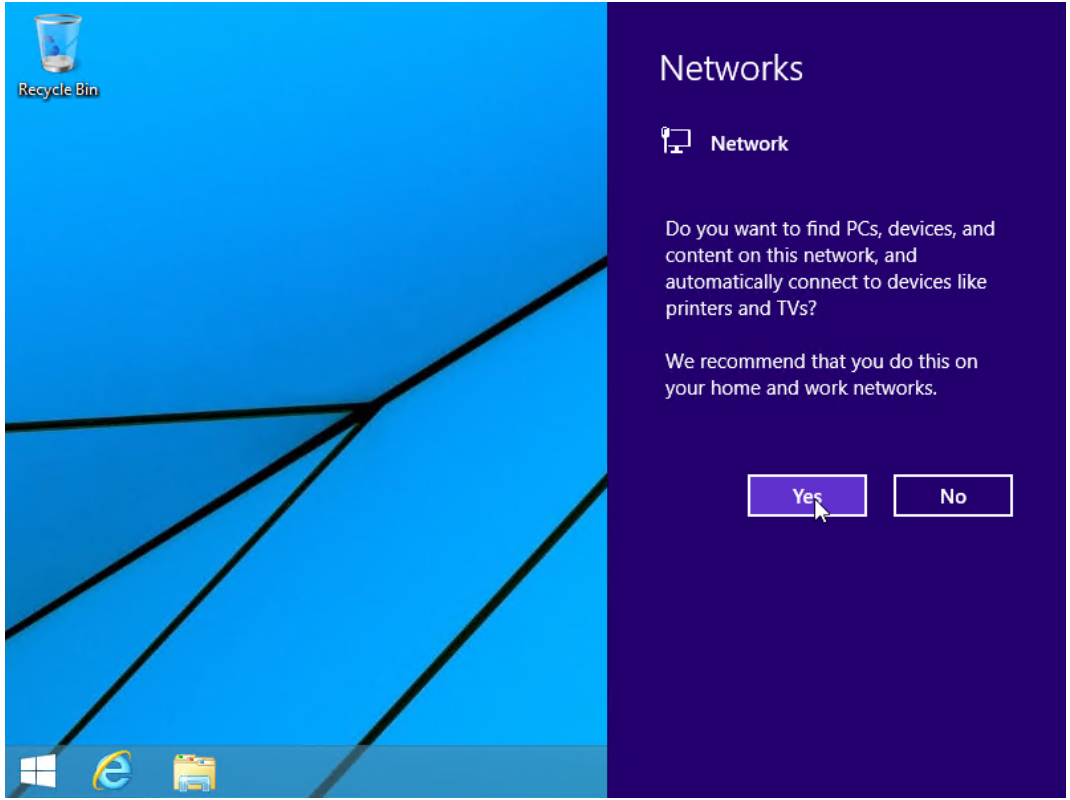
Location Awareness (Slide 1 of 2)

- Firewall settings can be applied depending on connected network.
- Displays dialog when new network is detected.



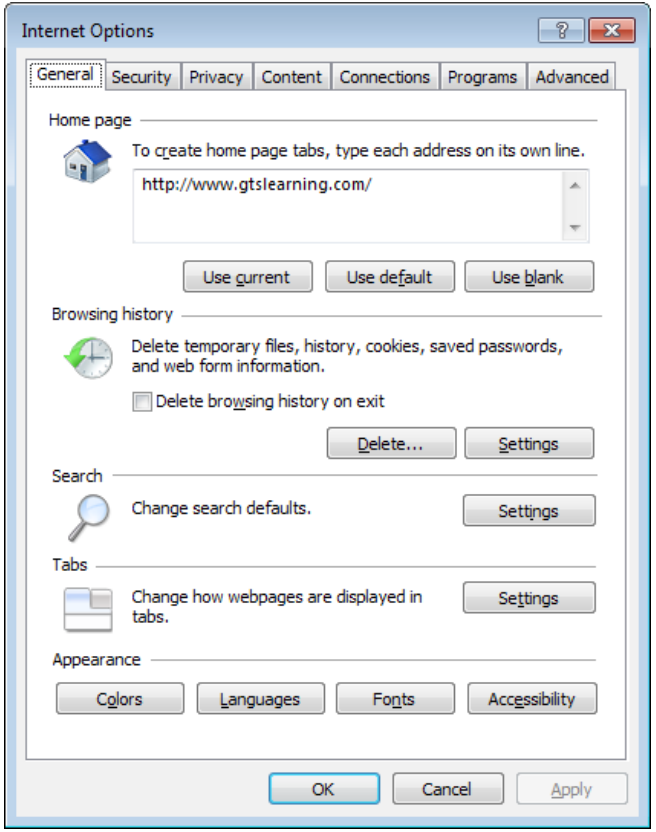
Location Awareness (Slide 2 of 2)

- 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.



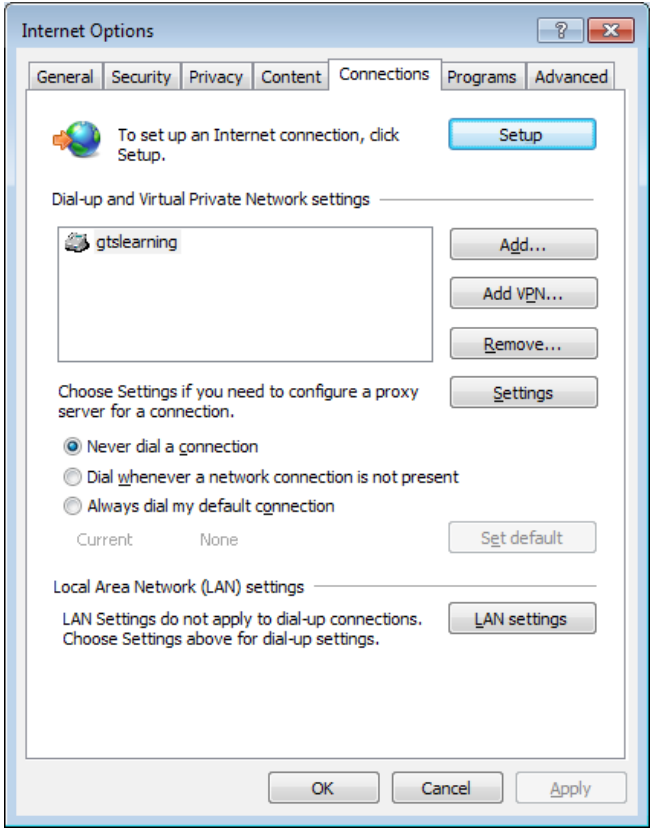
Browser Configuration (Slide 1 of 7)

- 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.



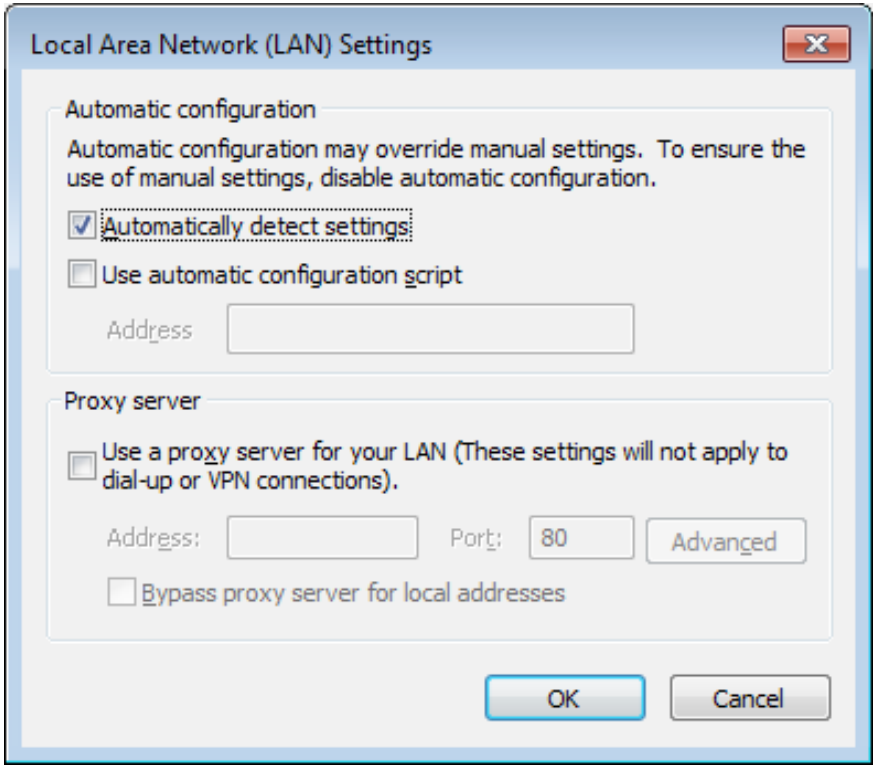
Browser Configuration (Slide 2 of 7)

- Configure connections:
  - Dial-up
  - Router



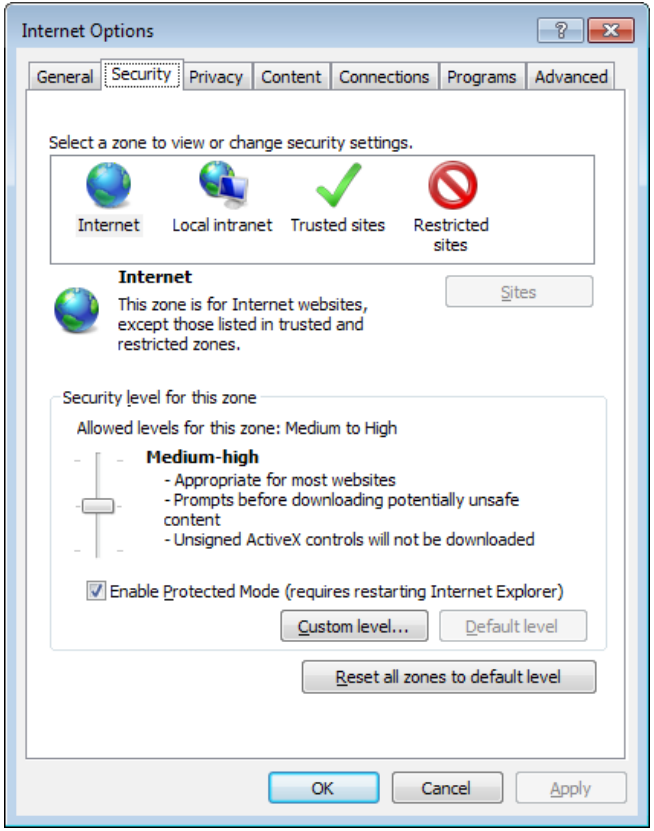
Browser Configuration (Slide 3 of 7)

- 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.



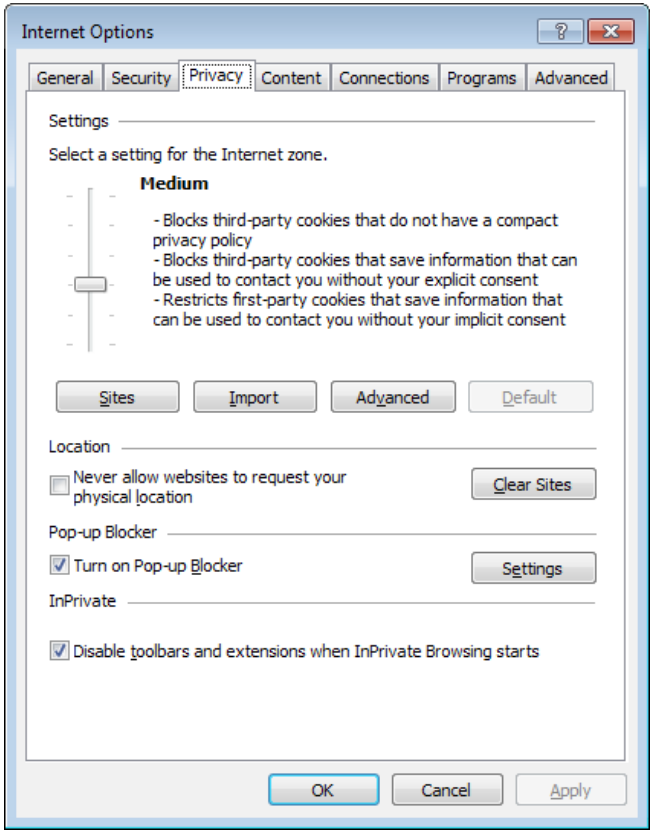
Browser Configuration (Slide 4 of 7)

- Security settings protect system from malicious content on web pages.
- In Windows, configure by security zone.



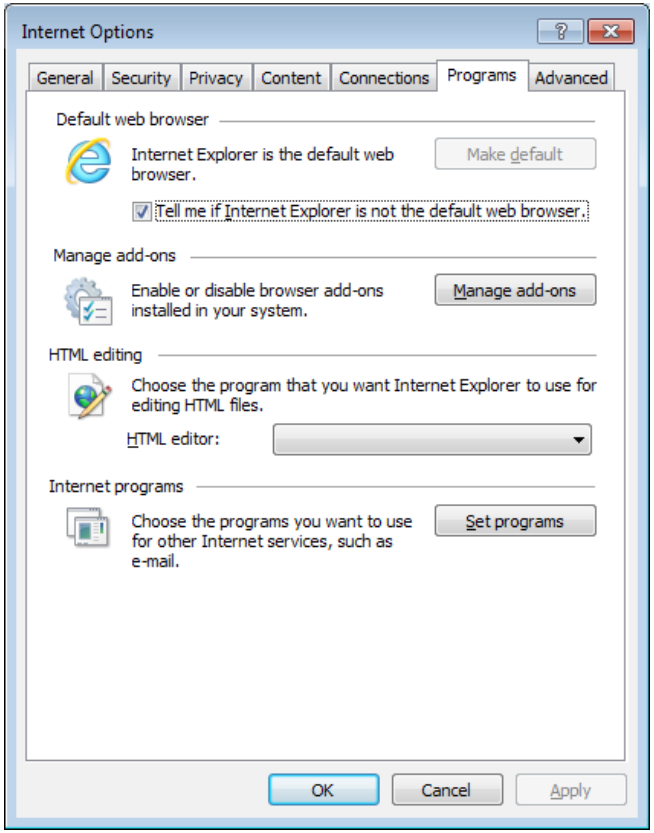
Browser Configuration (Slide 5 of 7)

- Privacy settings control use of cookies
  - Text files containing session data
- Configure pop-up blocker



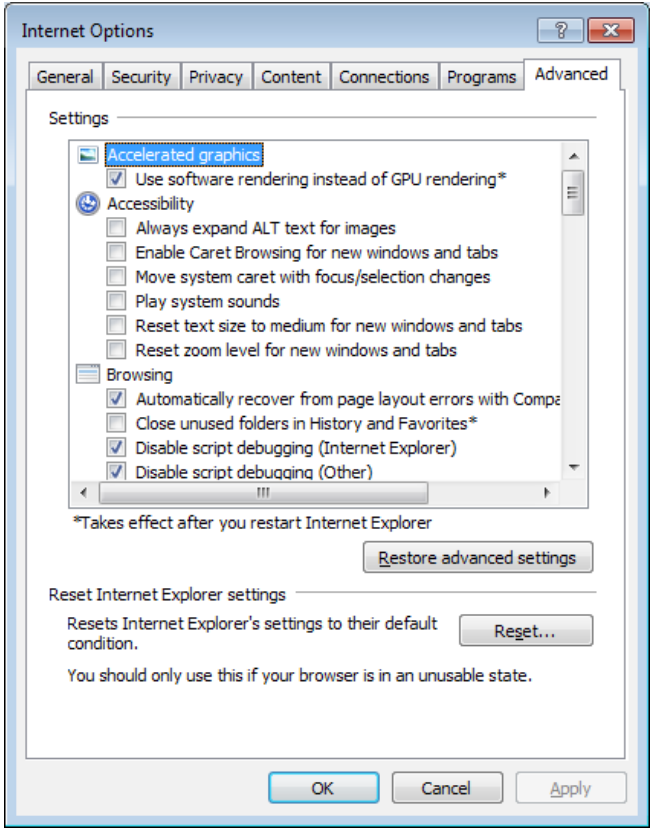
Browser Configuration (Slide 6 of 7)

- Check or set default browser
- Manage add-ons



Browser Configuration (Slide 7 of 7)

- Various advanced settings and options
- Resetting the browser



Activity

Discussing SOHO Network Security

30bird lab 11.2.3