

# 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

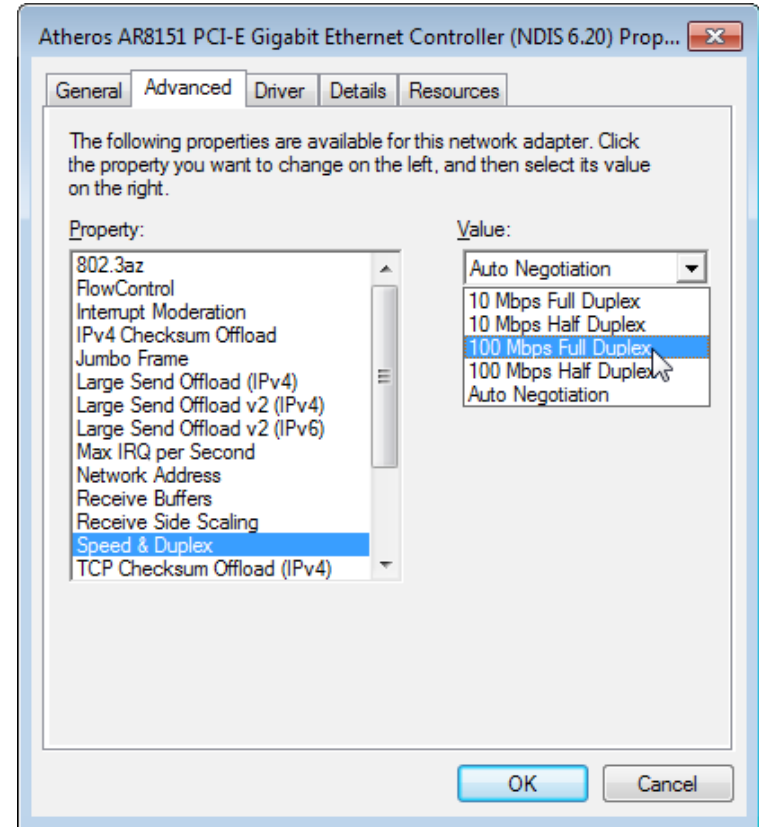
# NIC Properties

- 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

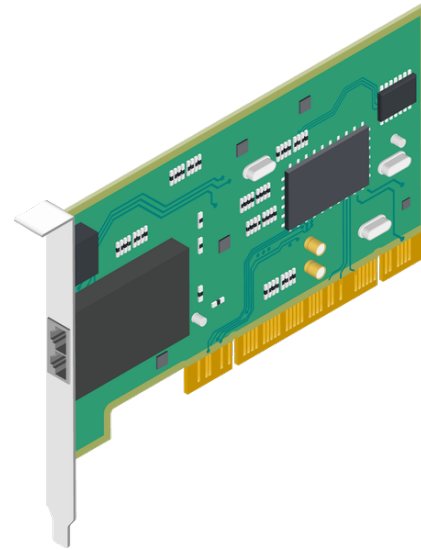


# QoS (Quality of Service)

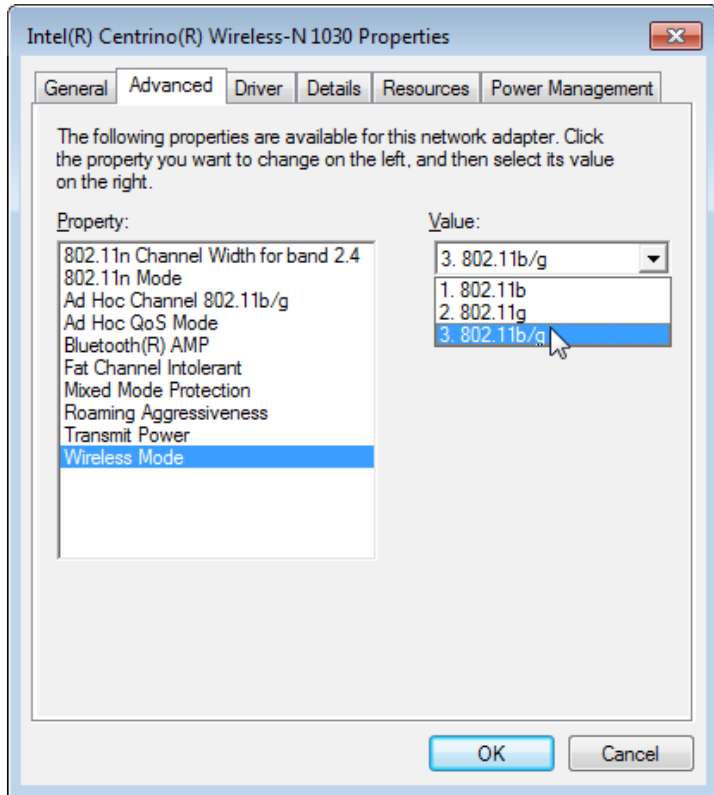
- Network protocol that prioritizes some types of traffic.
- Can help ensure real-time applications such as VoIP or video conference have priority.
- QoS usually configured on managed switches.
- May need to enable QoS protocol on adapter.

# 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.



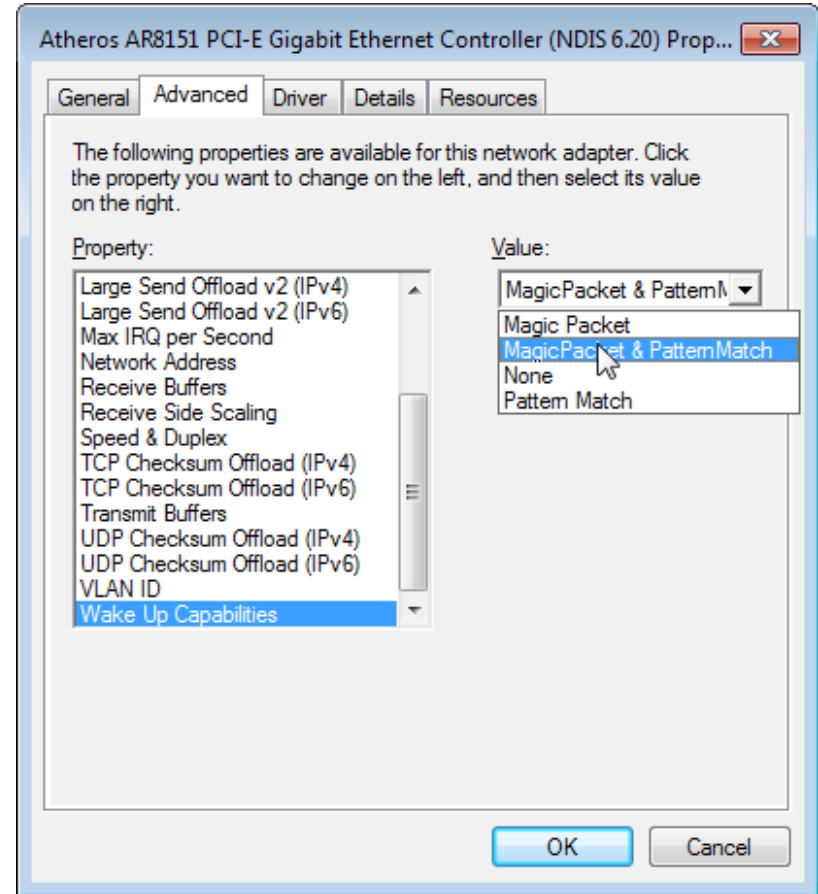
# Wireless Network Cards



- 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

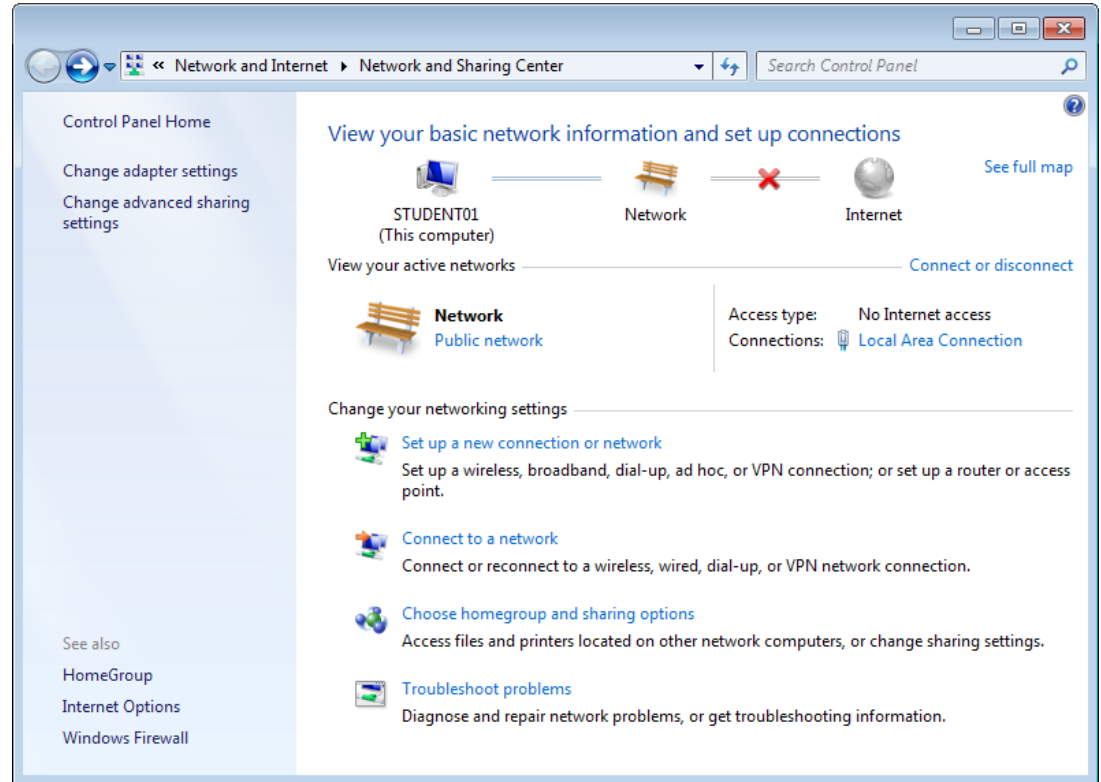
- Start computer remotely
- Network card is active, on standby
- “Magic packet” starts boot
- To set up WoL:
  1. Enable WoL in system setup
  2. Enable WoL on adapter
  3. Configure network to send magic packets





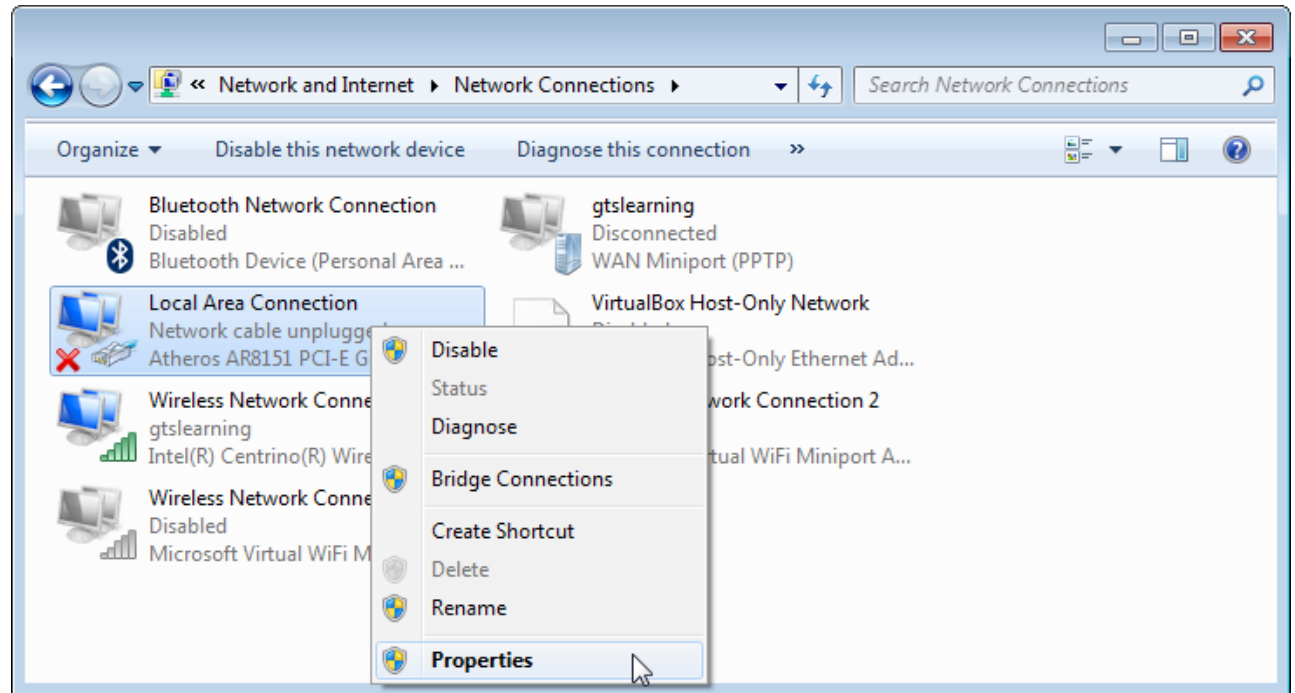
# Network Connections in Windows 7 and Windows 8 (Slide 1 of 4)

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



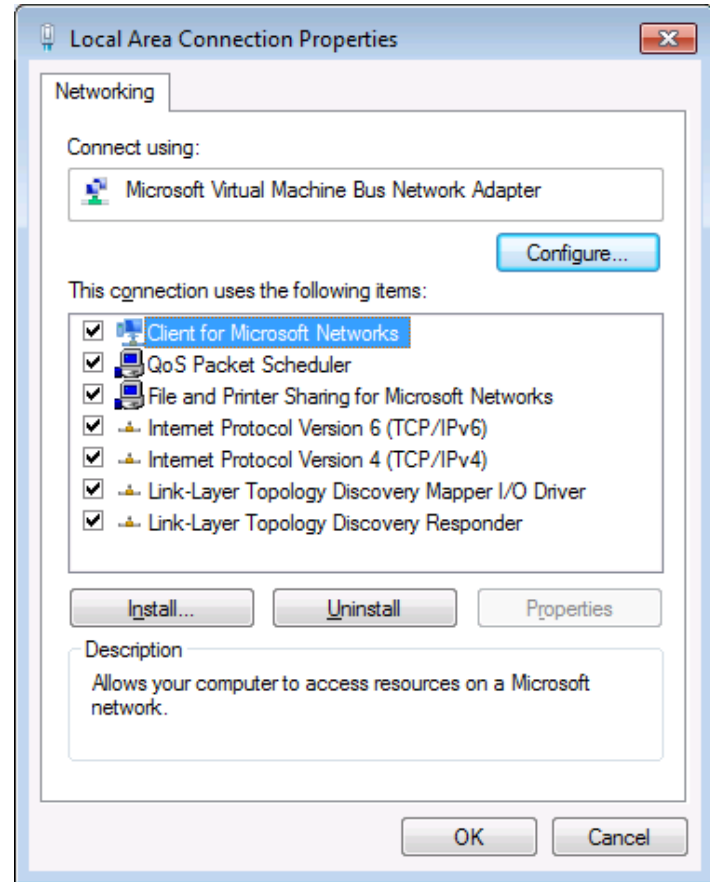
# Network Connections in Windows 7 and Windows 8 (Slide 2 of 4)

- Access adapter properties
- Wired/wireless adapter names vary



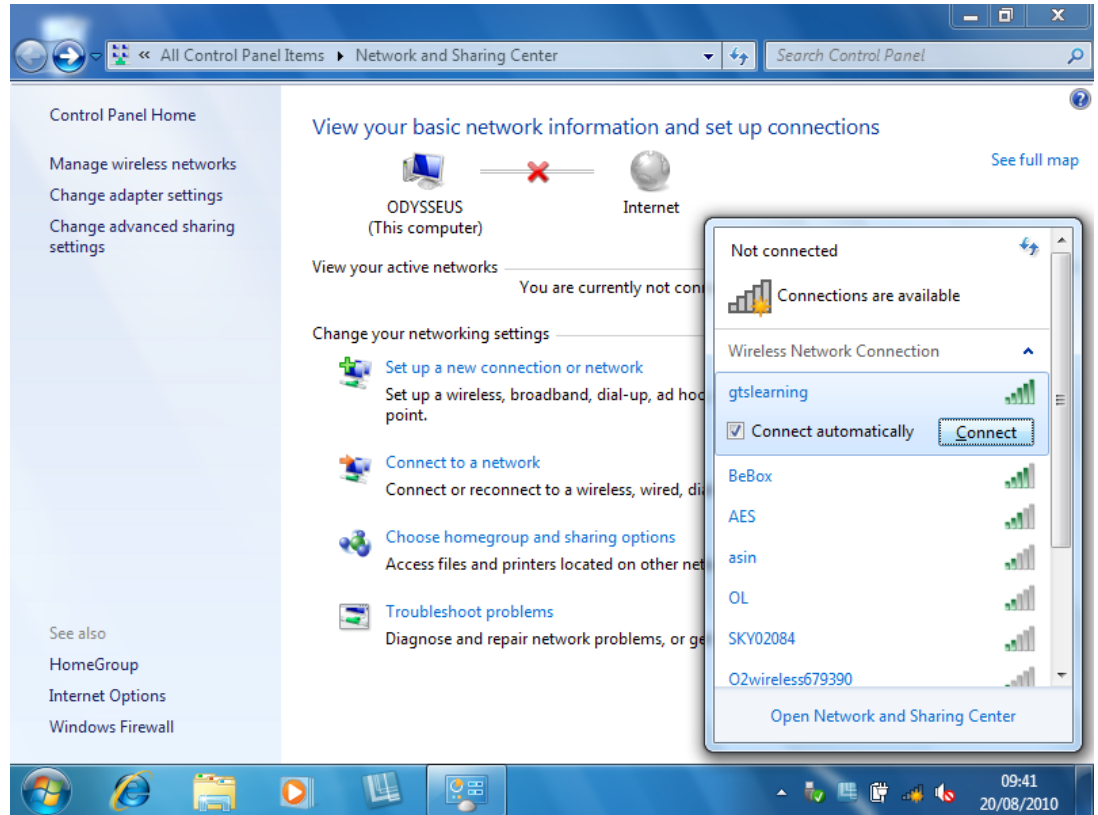
# Network Connections in Windows 7 and Windows 8 (Slide 3 of 4)

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

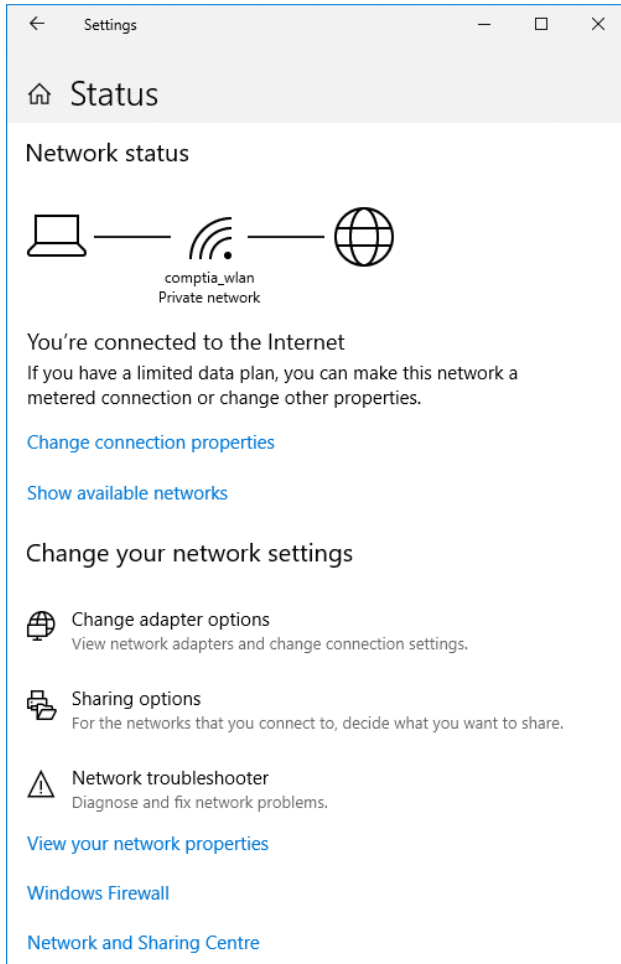


# Network Connections in Windows 7 and Windows 8 (Slide 4 of 4)

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



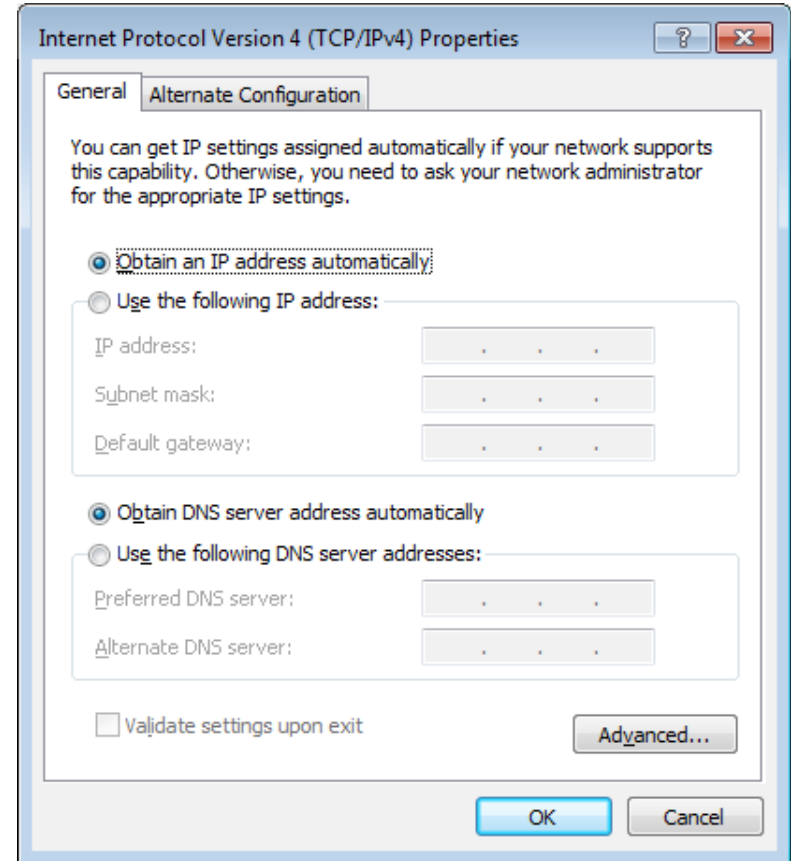
# Network Connections in Windows 10



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

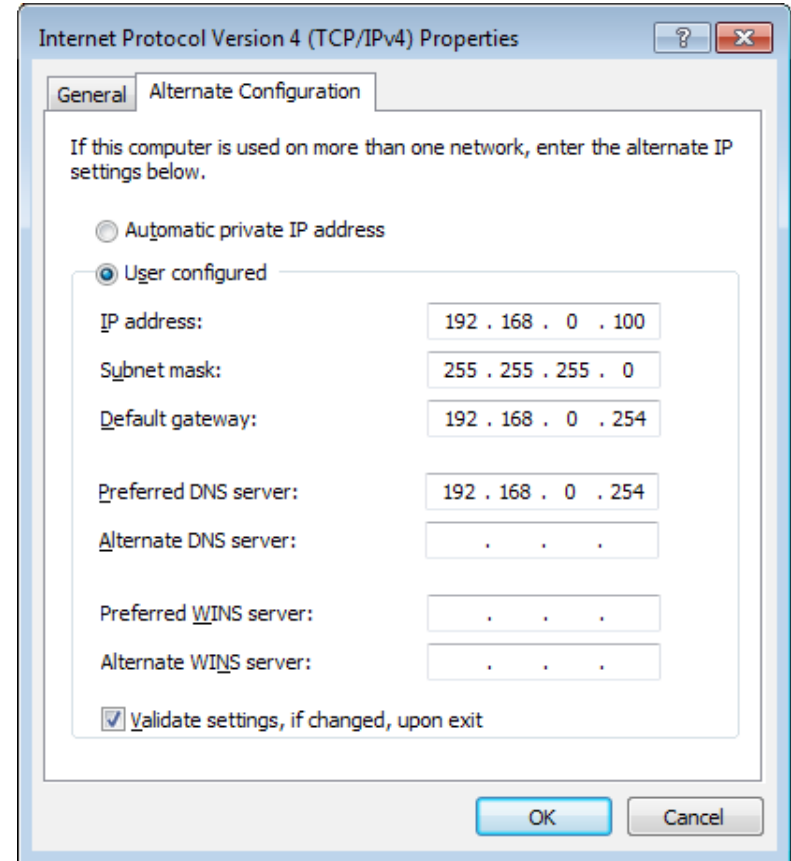
# IP Address Configuration (Slide 1 of 2)

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

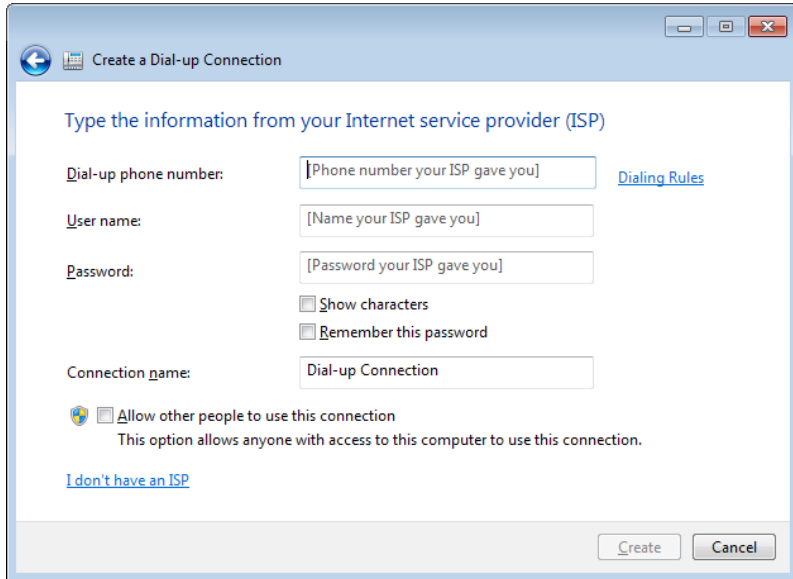


# IP Address Configuration (Slide 2 of 2)

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



# Other Network Connections (Slide 1 of 3)



Create a Dial-up Connection

Type the information from your Internet service provider (ISP)

Dial-up phone number: [Phone number your ISP gave you] [Dialing Rules](#)

User name: [Name your ISP gave you]

Password: [Password your ISP gave you]

Show characters

Remember this password

Connection name: Dial-up Connection

Allow other people to use this connection  
This option allows anyone with access to this computer to use this connection.

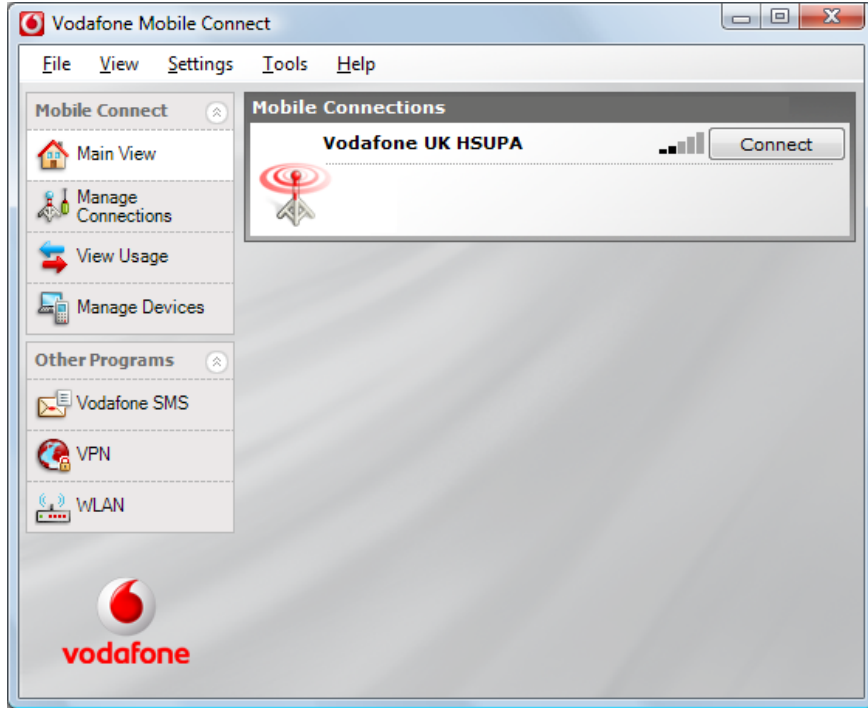
[I don't have an ISP](#)

Create Cancel

- 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

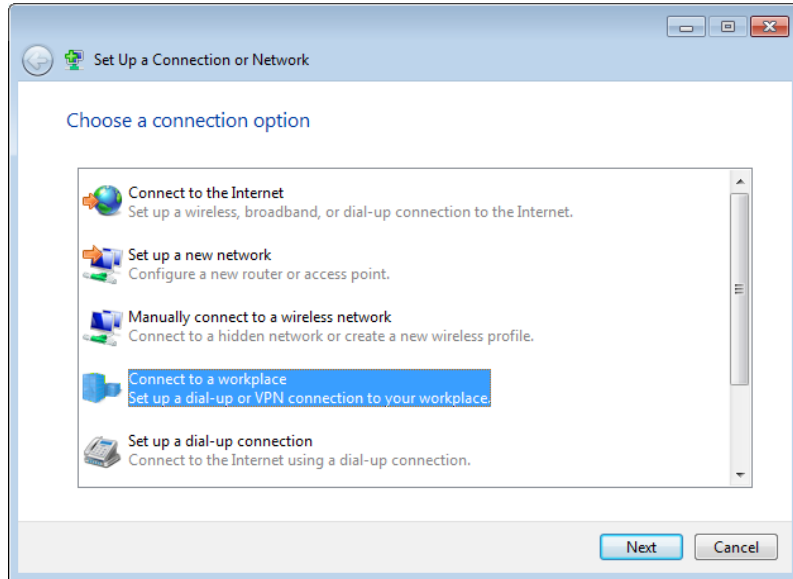


# Other Network Connections (Slide 2 of 3)



- 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

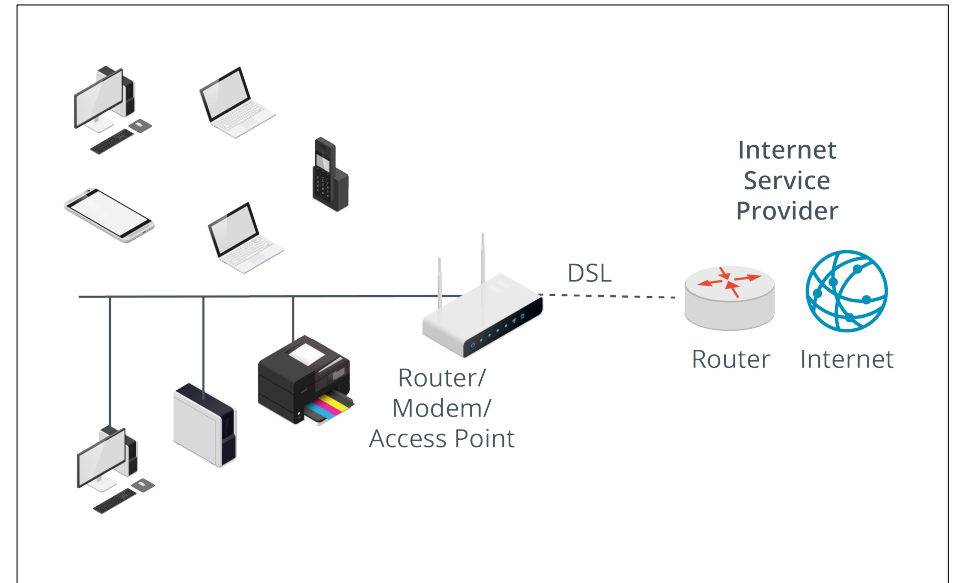


Discussing Network Connection Configuration Settings

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

# SOHO Networks

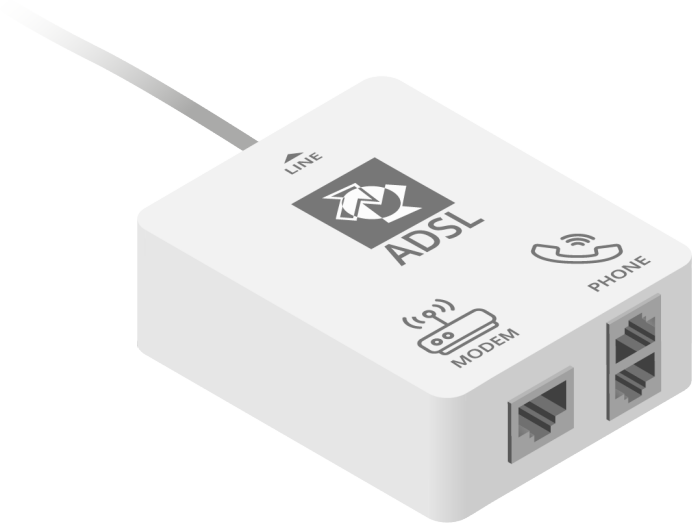
- Business network; may use centralized server as well as clients.
- Often uses single Internet device for connectivity.
- May be home/residential network as well.



# 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.

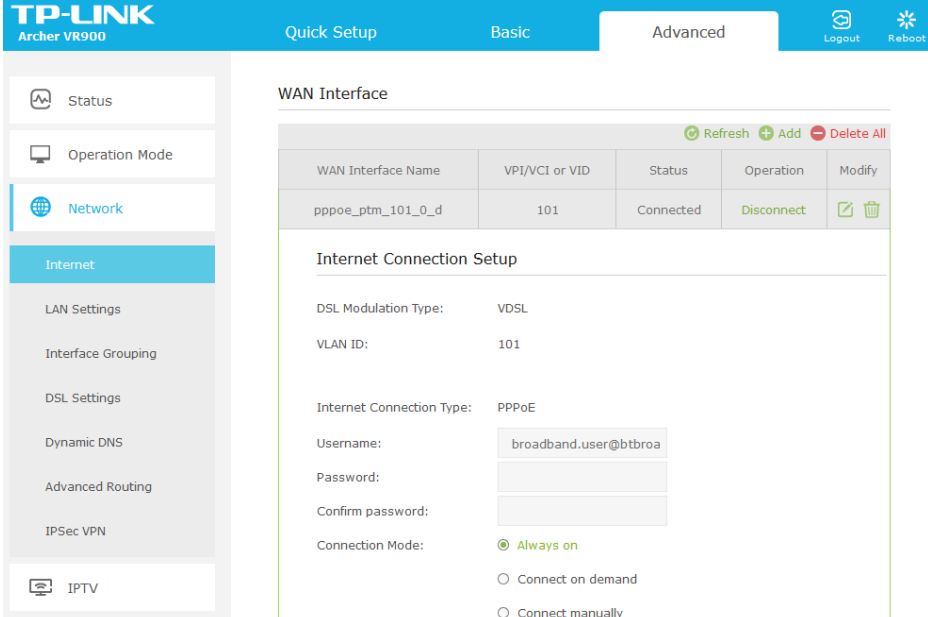
# Common SOHO Network Hardware (Slide 2 of 2)





- 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.



The screenshot displays the TP-LINK Archer VR900 web interface. The top navigation bar includes 'Quick Setup', 'Basic', and 'Advanced' tabs, with 'Advanced' selected. A sidebar on the left contains menu items: Status, Operation Mode, Network (highlighted), Internet (sub-menu), LAN Settings, Interface Grouping, DSL Settings, Dynamic DNS, Advanced Routing, IPsec VPN, and IPTV. The main content area is titled 'WAN Interface' and features a table with columns for WAN Interface Name, VPI/VCI or VID, Status, Operation, and Modify. A single entry is shown with 'pppoe\_ptm\_101\_0\_d', '101', and 'Connected' status. Below the table is the 'Internet Connection Setup' section, which includes fields for DSL Modulation Type (VDSL), VLAN ID (101), Internet Connection Type (PPPoE), Username (broadband.user@btbroa), Password, Confirm password, and Connection Mode (radio buttons for 'Always on', 'Connect on demand', and 'Connect manually').

WAN Interface Name	VPI/VCI or VID	Status	Operation	Modify
pppoe_ptm_101_0_d	101	Connected	Disconnect	 

**Internet Connection Setup**

DSL Modulation Type: VDSL

VLAN ID: 101

Internet Connection Type: PPPoE

Username:

Password:

Confirm password:

Connection Mode:

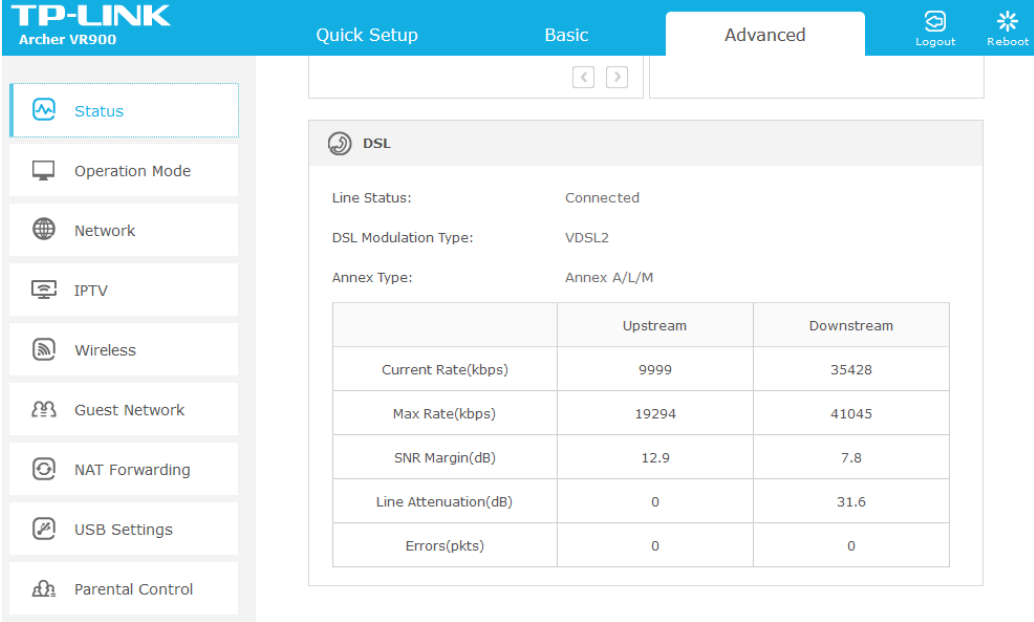
Always on

Connect on demand

Connect manually

# SOHO Network Configuration (Slide 2 of 2)

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



The screenshot displays the TP-LINK Archer VR900 management console. The top navigation bar includes 'Quick Setup', 'Basic', and 'Advanced' tabs, with 'Advanced' selected. A sidebar on the left lists various settings: Status (selected), Operation Mode, Network, IPTV, Wireless, Guest Network, NAT Forwarding, USB Settings, and Parental Control. The main content area shows the 'DSL' configuration page. It indicates the line status is 'Connected', the modulation type is 'VDSL2', and the annex type is 'Annex A/L/M'. A table provides performance metrics for upstream and downstream connections.

	Upstream	Downstream
Current Rate(kbps)	9999	35428
Max Rate(kbps)	19294	41045
SNR Margin(dB)	12.9	7.8
Line Attenuation(dB)	0	31.6
Errors(pkts)	0	0



# 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

The screenshot shows the TP-Link Archer VR900 web interface. The top navigation bar includes 'Quick Setup', 'Basic', and 'Advanced' tabs, with 'Advanced' selected. The 'Wireless Settings' page is displayed, showing various configuration options. The 'Wireless Radio' is enabled. The SSID is 'comptia\_wlan'. Security is set to 'WPA/WPA2 Personal (Recommended)'. The encryption is 'AES'. The password is '12345670'. The mode is '802.11gn mixed'. The channel is 'Auto' and the channel width is 'Auto'. The transmit power is set to 'Low'. A 'Save' button is visible at the bottom right. The footer shows the firmware version '0.1.0 0.9.1 v0069.0 Build 160525 Rel.38143n' and hardware version 'Archer VR900 v2 00000000'.

TP-LINK  
Archer VR900

Quick Setup Basic **Advanced** English Logout Reboot

Status  
Operation Mode  
Network  
IPTV  
Wireless  
Wireless Settings  
WPS  
MAC Filtering  
Wireless Schedule  
Statistics  
Advanced Settings

Wireless Settings 2.4GHz | 5GHz ?

Wireless Radio:  Enable

Wireless Network Name (SSID): comptia\_wlan  Hide SSID

Security: WPA/WPA2 Personal (Recommended)

Version:  Auto  WPA2-PSK

Encryption:  Auto  TKIP  AES

Password: 12345670

Mode: 802.11gn mixed

Channel: Auto

Channel Width: Auto

Transmit Power:  Low  Middle  High

Save

Firmware Version:0.1.0 0.9.1 v0069.0 Build 160525 Rel.38143n Hardware Version:Archer VR900 v2 00000000 Support

# DHCP and IP Address Configuration

The screenshot displays the TP-Link Archer VR900 web interface. The top navigation bar includes 'Quick Setup', 'Basic', and 'Advanced' tabs, with 'Advanced' selected. The left sidebar shows a menu with 'LAN Settings' highlighted. The main content area is titled 'DHCP Server' and contains the following configuration options:

- IP Version:  IPv4  IPv6
- MAC Address: 60:E3:27:CF:EA:CB
- LAN IPv4:
- Subnet Mask:
- IGMP Snooping:  Enable IGMP Snooping
- DHCP:  Enable DHCP
- DHCP Mode:  DHCP Server  DHCP Relay
- IP Address Pool:  -
- Address Lease Time:  minutes(1-2880)
- Default Gateway:  (Optional)
- Default Domain:  (Optional)
- Primary DNS:  (Optional)
- Secondary DNS:  (Optional)

A green 'Save' button is located at the bottom right of the configuration area.

- 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

The screenshot displays the TP-Link Archer VR900 web interface. The top navigation bar includes 'Quick Setup', 'Basic', and 'Advanced' tabs, with 'Advanced' selected. A language dropdown is set to 'English'. The left sidebar shows a menu with 'Wireless' selected, and 'WPS' highlighted under 'Wireless Settings'. The main content area is titled 'Router PIN' and 'WPS Settings'. Under 'Router PIN', there is a toggle for 'Router PIN' (currently off), a 'Current PIN' field showing '12345670', and 'Generate' and 'Restore' buttons. Under 'WPS Settings', the 'Enable WPS' toggle is turned on. The 'Select a setup method' section has 'Push Button (Recommended)' selected, with a 'Connect' button and a 'Failed to add the device!' message. The 'PIN Code' option is also visible but unselected. The footer shows firmware and hardware versions and a 'Support' link.

- 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.

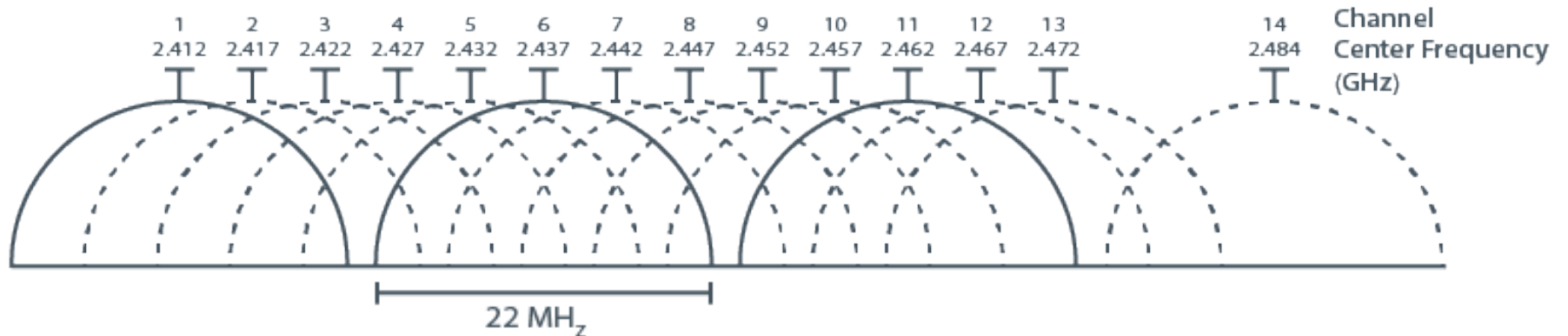
# Access Point Placement

- 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

The screenshot displays the TP-Link Archer VR900 web interface. The top navigation bar includes 'Quick Setup', 'Basic', and 'Advanced' tabs, with 'Advanced' selected. The 'Wireless' section is active in the left sidebar. The main content area is titled 'Wireless Settings' and shows the following configuration:

- Wireless Radio:  Enable
- Wireless Network Name (SSID):   Hide SSID
- Security:  (dropdown)
- Version:  Auto  WPA2-PSK
- Encryption:  Auto  TKIP  AES
- Password:
- Mode:  (dropdown)
- Channel:  (dropdown)
- Channel Width:  (dropdown)
- Transmit Power:  Low  Middle  High

A green 'Save' button is located at the bottom right of the settings area. The footer of the page shows the firmware version (0.1.0 0.9.1 v0069.0 Build 160525 Rel.38143n), hardware version (Archer VR900 v2 00000000), and a 'Support' link.

- 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
<b>WEP</b>	<ul style="list-style-type: none"><li>• Legacy encryption system based on RC4 cipher</li><li>• 64-bit or 128-bit key</li><li>• Flaw in key production method; easy for attacker to generate key</li><li>• Deprecated and should not be used</li></ul>
<b>WPA</b> <b>WPA2</b>	<ul style="list-style-type: none"><li>• Based on RC4</li><li>• Adds TKIP to fix security problem</li><li>• WPA2 developed to meet 802.11i security standards</li><li>• Use WPA2 whenever possible</li><li>• If not supported by devices, use WPA</li></ul>



# Wi-Fi Authentication

Authentication Mode	Description
<b>Personal</b>	<ul style="list-style-type: none"><li>• Based on pre-shared key generated from passphrase.</li><li>• Cannot completely secure distribution of key; on home network may not be secure passphrase; all users share key (no accounting); hard to change key.</li><li>• Simple setup.</li><li>• Only choice for WEP; can use with WPA/WPA2 on SOHO networks or workgroups.</li></ul>
<b>Enterprise</b>	<ul style="list-style-type: none"><li>• Enterprise mode authentication in WPA/WPA2.</li><li>• Authentication passed to RADIUS server.</li><li>• Suitable for server-/domain-based networks.</li></ul>

# Common SOHO Security Issues

Security Issue	Description
<b>SSID</b>	<ul style="list-style-type: none"><li>• Simple name to identify the WAN</li><li>• Change default SSID</li><li>• Do not use personal information</li><li>• Disable SSID broadcast</li><li>• Enable encryption</li></ul>
<b>Physical Security</b>	<ul style="list-style-type: none"><li>• Restrict physical access to enterprise routers and switches</li><li>• Attacker with physical access could reset to defaults, gain access</li></ul>
<b>Updating Firmware</b>	<ul style="list-style-type: none"><li>• Keep Internet appliance firmware and driver up to date</li><li>• Make sure power stays on during update process</li></ul>
<b>Static IP Addresses</b>	<ul style="list-style-type: none"><li>• Static IP assignments will not deter a determined attack</li><li>• Router/modem must have static IP to function as DHCP server/default gateway</li></ul>

# 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

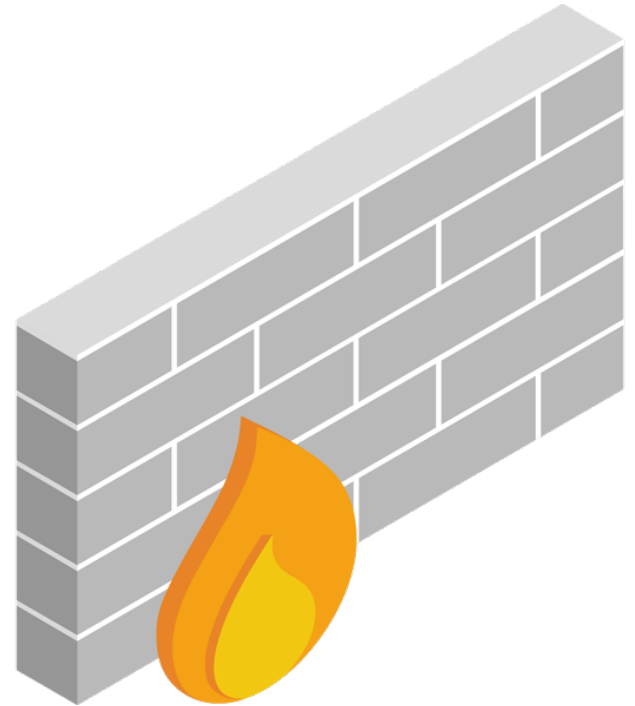
# Activity



## 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
<b>Packet Filtering</b>	<ul style="list-style-type: none"><li>• Earliest type; all firewalls capable of this function</li><li>• Inspects IP packet headers, accepts or drops based on rules</li><li>• Filtering rules based on:<ul style="list-style-type: none"><li>• IP filtering</li><li>• Protocol ID/type</li><li>• Port filtering/security</li></ul></li><li>• Configure ACL</li></ul>
<b>Host Firewall</b>	<ul style="list-style-type: none"><li>• Software on individual host; may be in addition to network firewall</li><li>• Can do packet filtering</li><li>• Can also grant/deny access based on software programs, services/processes, and users</li><li>• Two firewalls increase security; more complex to configure and troubleshoot</li></ul>

# Firewall Settings (Slide 1 of 2)

Firewall Setting	Description
<b>Disabling Ports</b>	<ul style="list-style-type: none"><li>• Only enable required services; can remove service at the host.</li><li>• May want service available locally but not on Internet.</li><li>• Configure firewall ACL to block the port, or block by default rule.</li></ul>
<b>MAC Filtering</b>	<ul style="list-style-type: none"><li>• Firewalls, switches, and APs can whitelist/blacklist MAC addresses.</li><li>• Can be time-consuming, but good security option for SOHO networks.</li></ul>
<b>Content Filtering / Parental Controls</b>	<ul style="list-style-type: none"><li>• Blocks websites and services based on keywords, ratings, or classification.</li><li>• Can restrict times.</li><li>• ISP-enforced filters cannot distinguish account types.</li><li>• Filters can also be enforced by OS.</li></ul>
<b>Whitelists / Blacklists</b>	<ul style="list-style-type: none"><li>• Blacklists document URLs known to harbor specific undesired content.</li><li>• Whitelists document sites that will be accessible even if filter is applied.</li></ul>



# Firewall Settings (Slide 2 of 2)

The screenshot shows the TP-Link Archer VR900 web interface. The top navigation bar includes 'Quick Setup', 'Basic', 'Advanced' (selected), 'English', 'Logout', and 'Reboot'. The left sidebar contains menu items: NAT Forwarding, USB Settings, Parental Controls (highlighted), Bandwidth Control, Security, and System Tools.

### Parental Controls

Status:

### Devices Under Parental Controls

The Effective Time is based on the time of the router. The time can be set in "Advanced > System Tools > Time Settings"

[Refresh](#) [+ Add](#) [- Delete](#)

<input type="checkbox"/>	ID	Device Name	MAC Address	Effective Time	Description	Status	Modify
<input type="checkbox"/>	1	MyDeviceTest	00:19:E0:02:03:04		test allow time		

### Content Restriction

Restriction Type:  Blacklist  Whitelist

[+ Add a New Keyword](#)

facebook [-](#)

[Save](#)

Firmware Version:0.1.0 0.9.1 v0069.0 Build 160525 Rel.38143n      Hardware Version:Archer VR900 v2 00000000      [Support](#)

# NAT

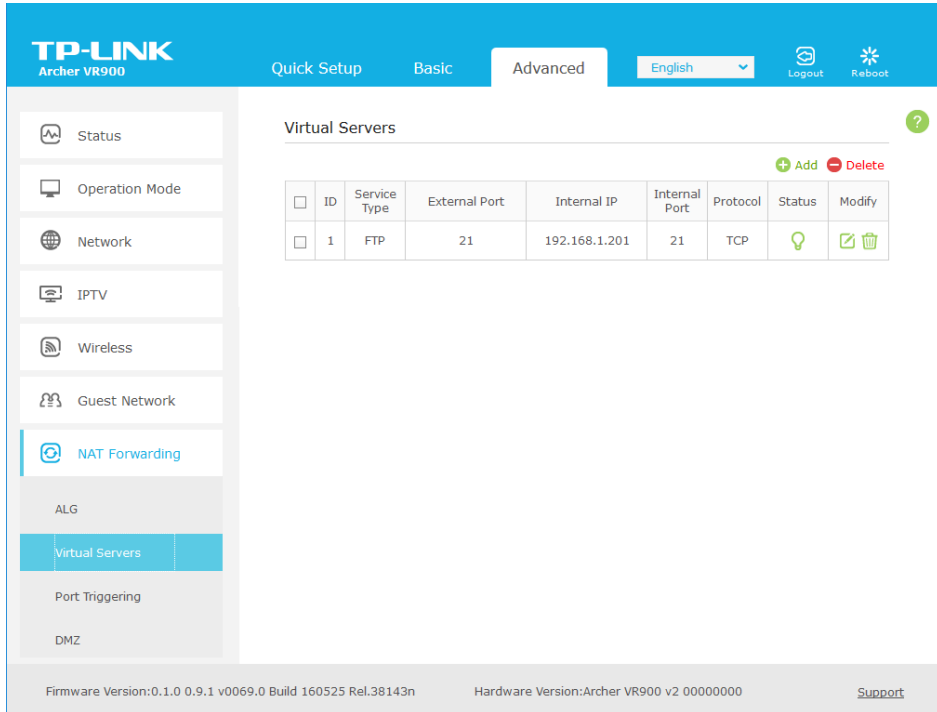
- All routers/modems use NAT/NAPT
- Router has single public address; clients use local private addresses
- Router translates between Internet and host
- Usually auto-configured
- Some protocols may need ALG to open ports dynamically

The screenshot displays the TP-Link Archer VR900 web management interface. The top navigation bar includes 'Quick Setup', 'Basic', and 'Advanced' tabs, with 'Advanced' selected. A language dropdown is set to 'English', and there are 'Logout' and 'Reboot' buttons. The left sidebar contains a menu with options: Status, Operation Mode, Network, IPTV, Wireless, Guest Network, NAT Forwarding (highlighted), ALG, Virtual Servers, Port Triggering, and DMZ. The main content area is titled 'Application Layer Gateway (ALG)' and lists several protocols with their status:

Protocol	Status
PPTP Pass-through:	<input checked="" type="checkbox"/> Enable
L2TP Pass-through:	<input checked="" type="checkbox"/> Enable
IPSec Pass-through:	<input checked="" type="checkbox"/> Enable
FTP ALG:	<input checked="" type="checkbox"/> Enable
TFTP ALG:	<input checked="" type="checkbox"/> Enable
H323 ALG:	<input checked="" type="checkbox"/> Enable
SIP ALG:	<input checked="" type="checkbox"/> Enable

A green 'Save' button is located at the bottom right of the settings area. The footer of the interface shows the firmware version (0.1.0 0.9.1 v0069.0 Build 160525 Rel.38143n) and hardware version (Archer VR900 v2 00000000), along with a 'Support' link.

# Port Forwarding and Port Triggering



The screenshot shows the TP-Link Archer VR900 web interface. The top navigation bar includes 'Quick Setup', 'Basic', and 'Advanced' tabs, with 'Advanced' selected. The language is set to 'English'. The left sidebar contains various settings categories: Status, Operation Mode, Network, IPTV, Wireless, Guest Network, NAT Forwarding (highlighted), ALG, Virtual Servers (highlighted), Port Triggering, and DMZ. The main content area is titled 'Virtual Servers' and contains a table with one entry:

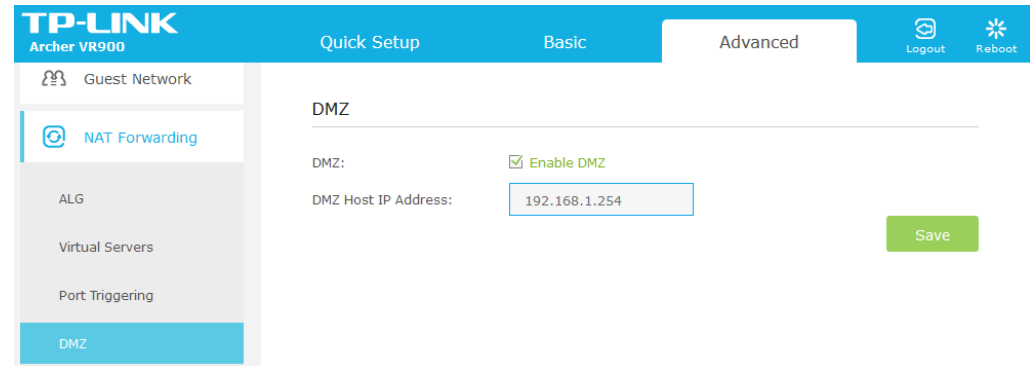
ID	Service Type	External Port	Internal IP	Internal Port	Protocol	Status	Modify
1	FTP	21	192.168.1.201	21	TCP	On	[Edit] [Delete]

At the bottom of the interface, the firmware version is 0.1.0 0.9.1 v0069.0 Build 160525 Rel.38143n and the hardware version is Archer VR900 v2 00000000. A 'Support' link is also present.

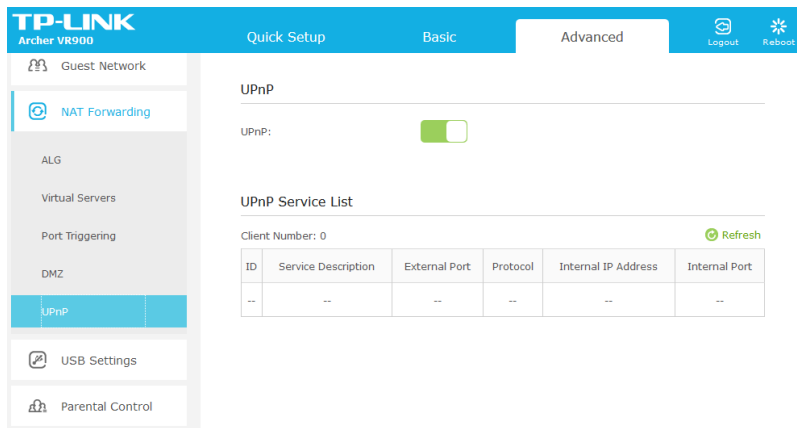
- Internet hosts only see router's public address.
- Configure port forwarding/DNAT if running an Internet-facing service on your internal network.
- Router transmits Internet requests to a given port to a designated internal host.
- Port triggering is for applications using multiple ports.

# 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.



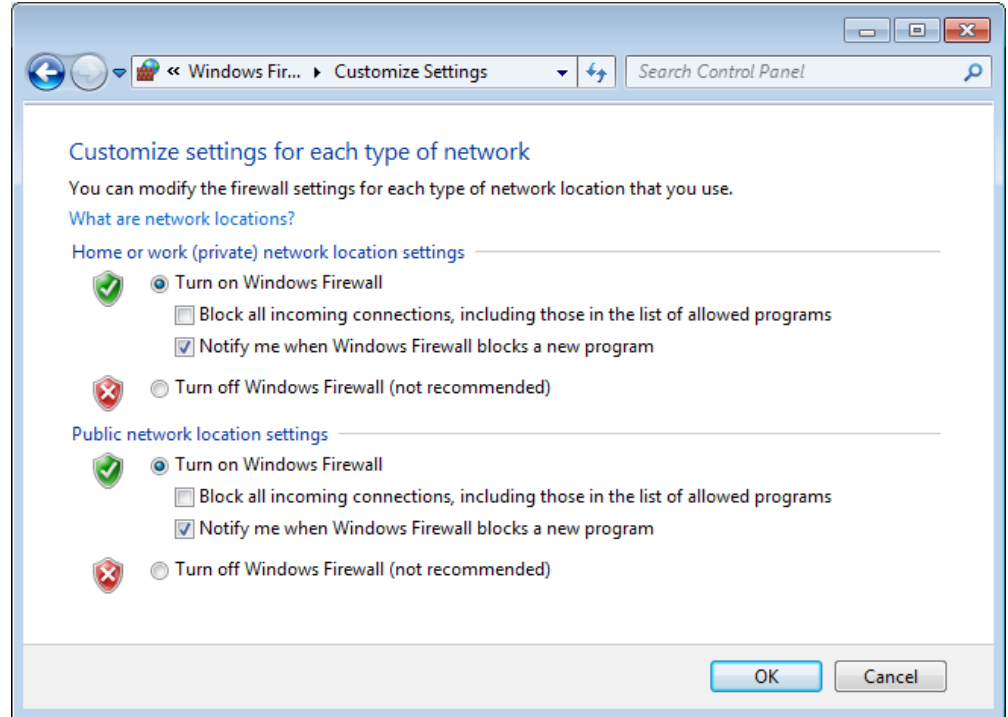
# Universal Plug-and-Play



- 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.

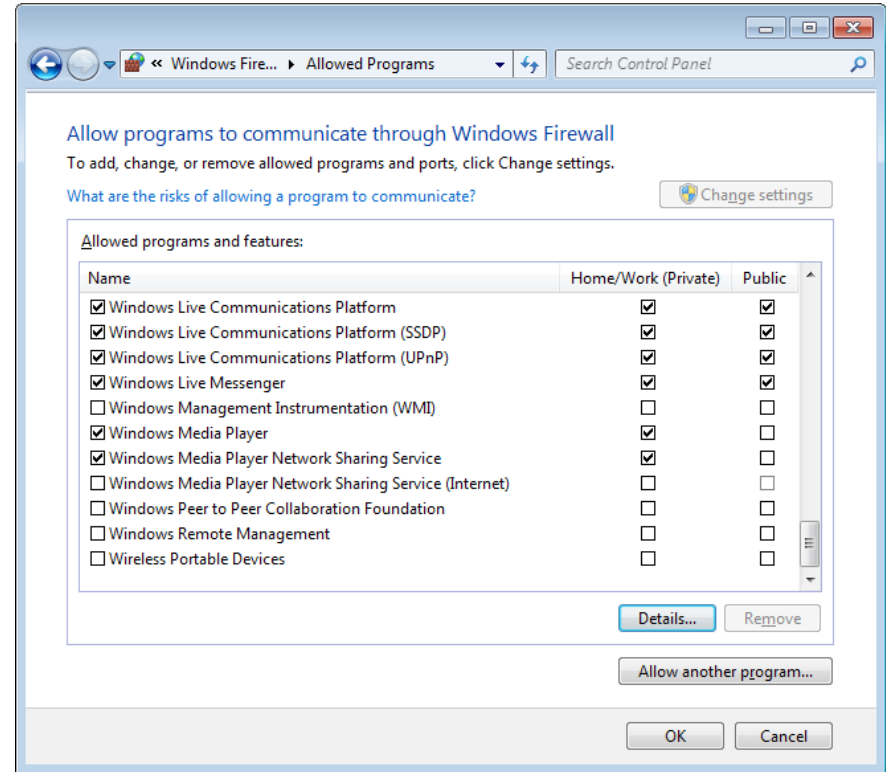
# Windows Firewall (Slide 1 of 2)

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

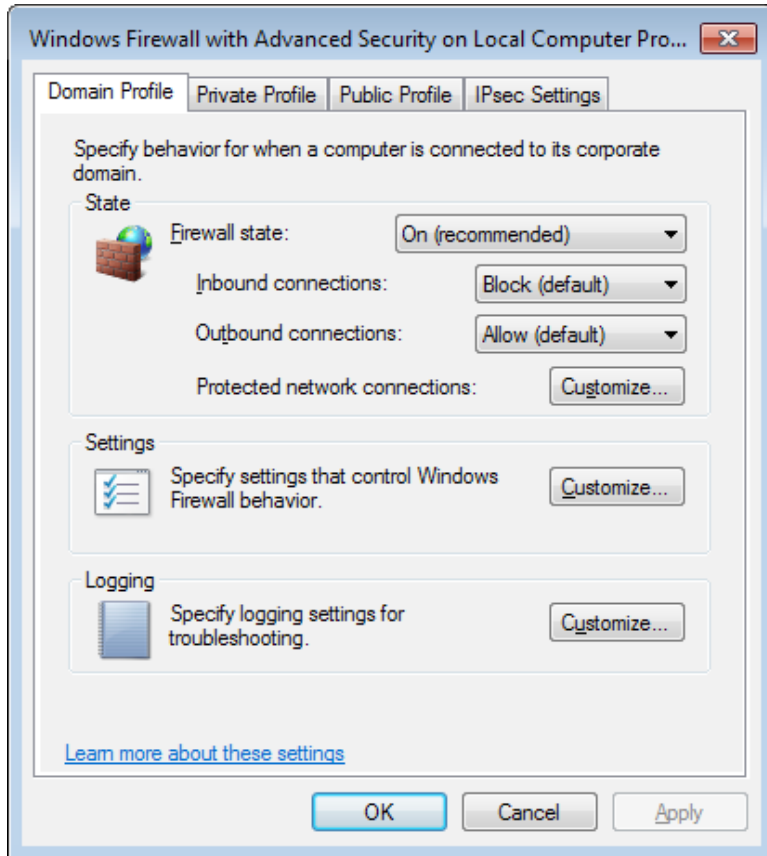


# Windows Firewall (Slide 2 of 2)

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



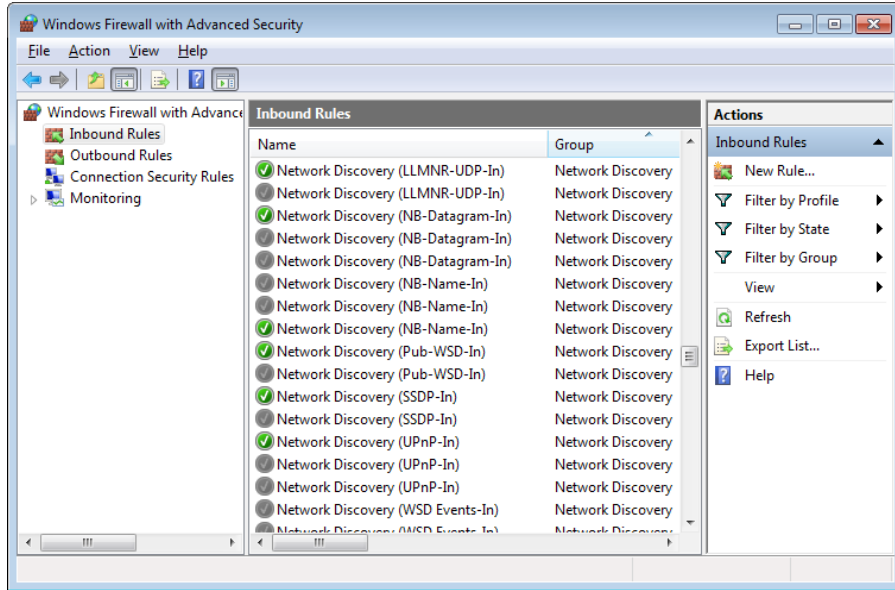
# Windows Firewall with Advanced Security (Slide 1 of 2)



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



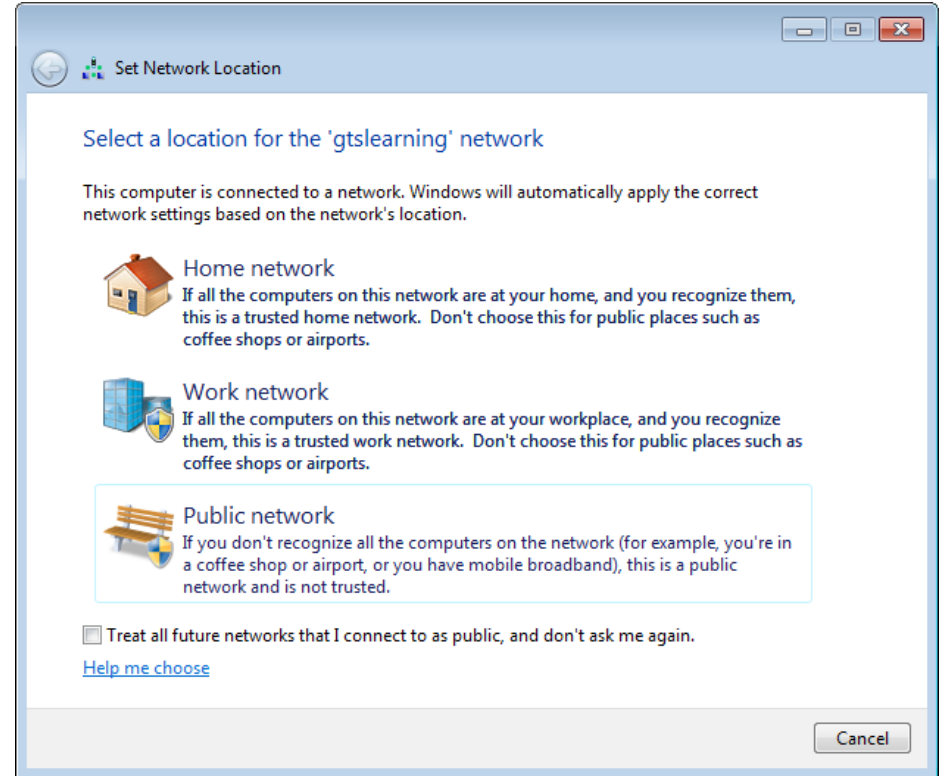
# Windows Firewall with Advanced Security (Slide 2 of 2)



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

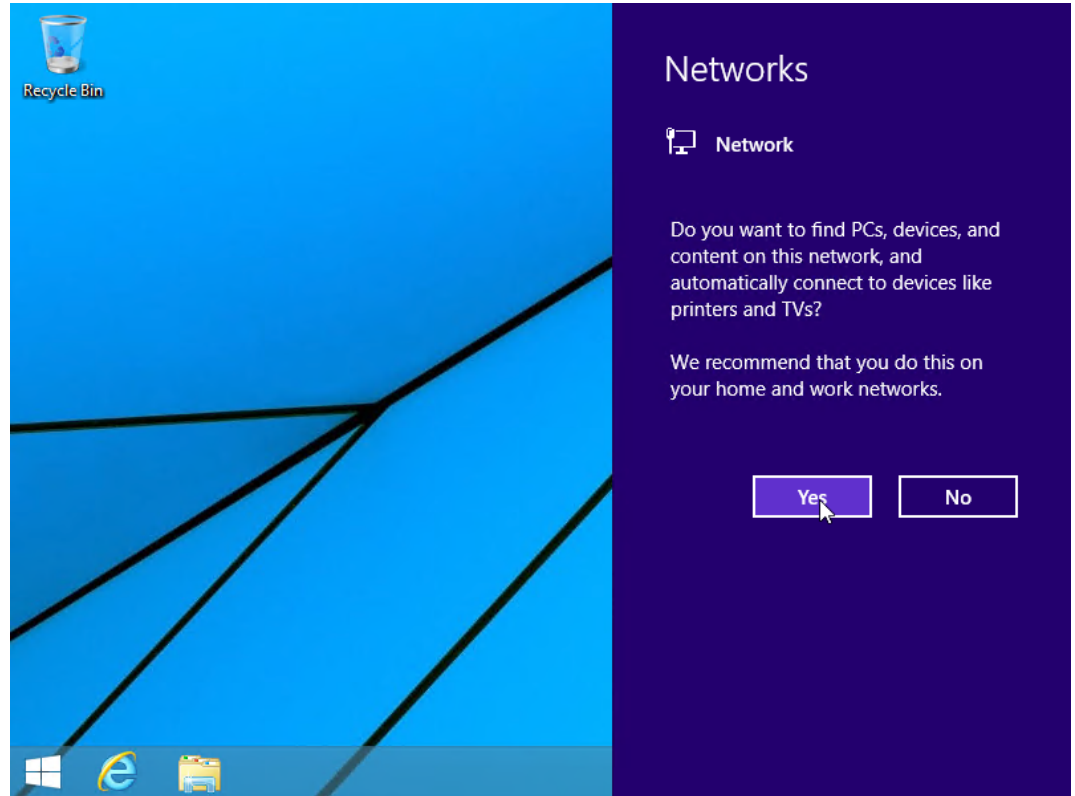
# Location Awareness (Slide 1 of 2)

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



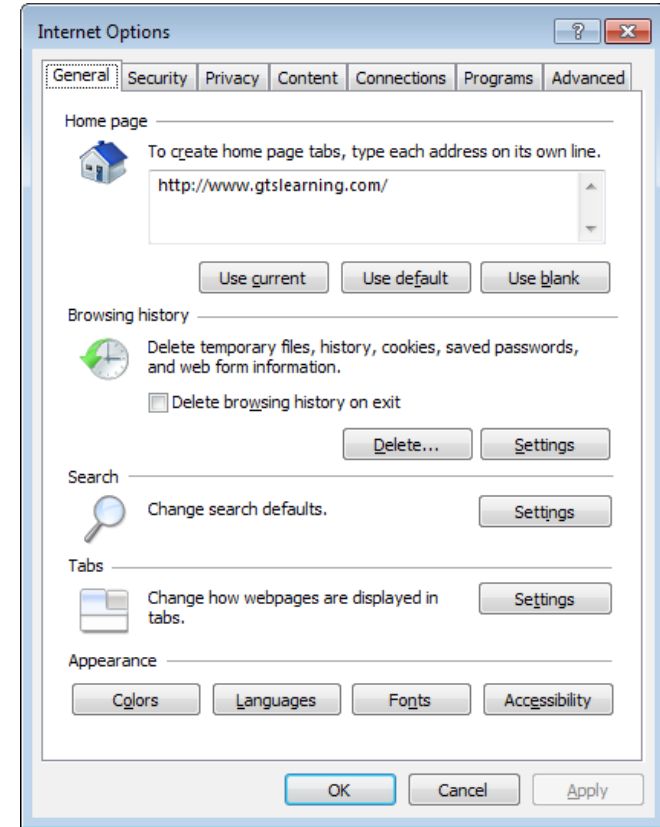
# Location Awareness (Slide 2 of 2)

- 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.



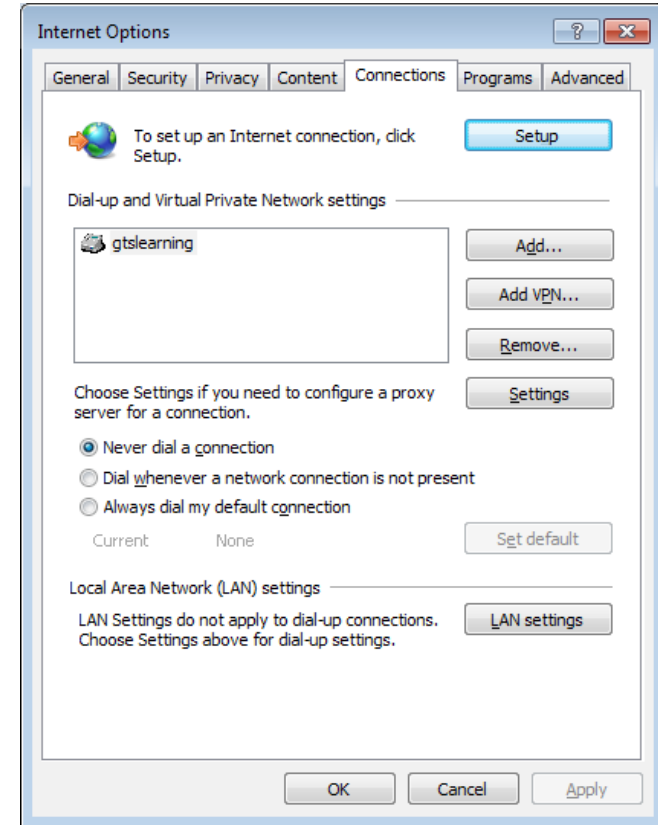
# Browser Configuration (Slide 1 of 7)

- 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.



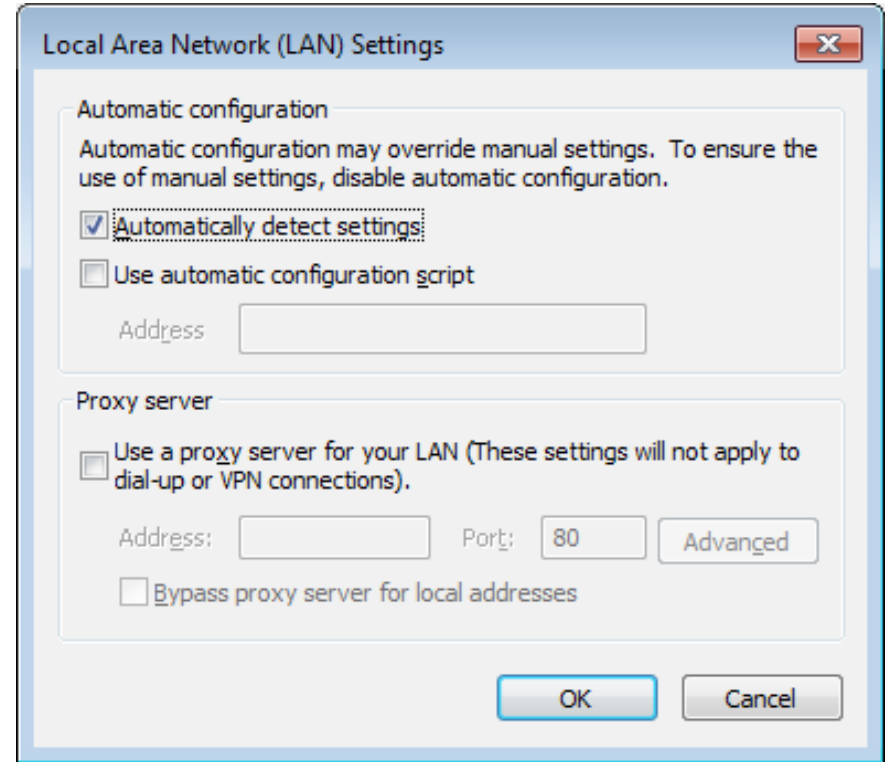
# Browser Configuration (Slide 2 of 7)

- Configure connections:
  - Dial-up
  - Router



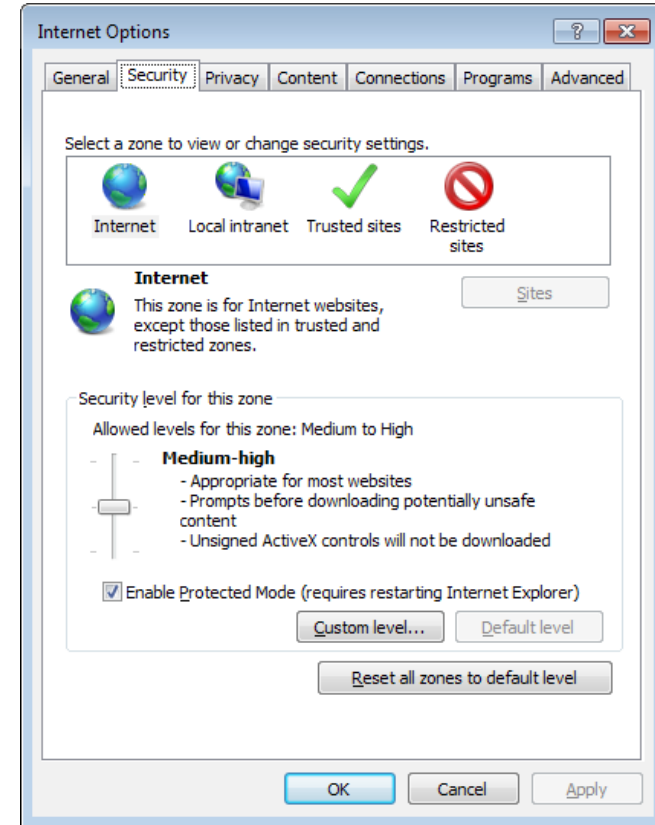
# Browser Configuration (Slide 3 of 7)

- 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.



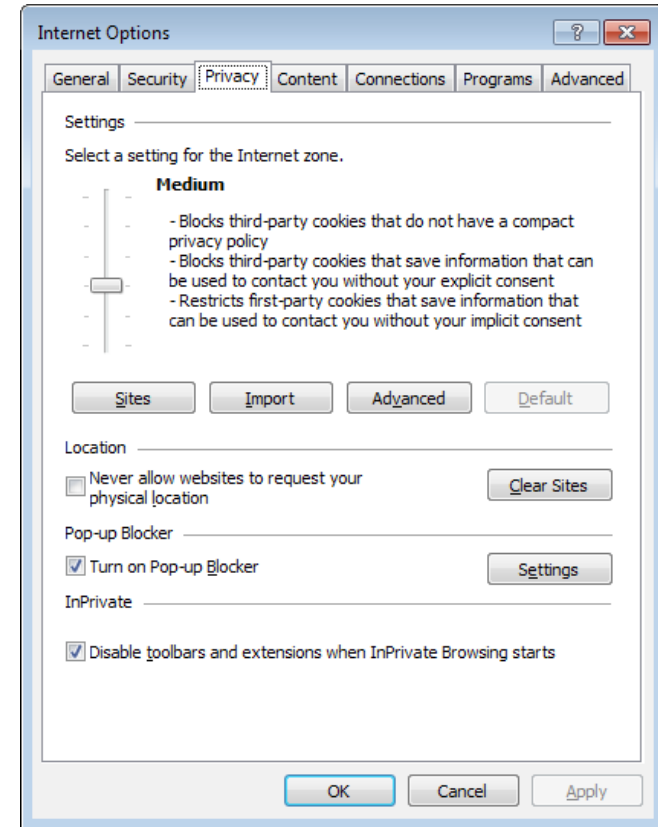
# Browser Configuration (Slide 4 of 7)

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



# Browser Configuration (Slide 5 of 7)

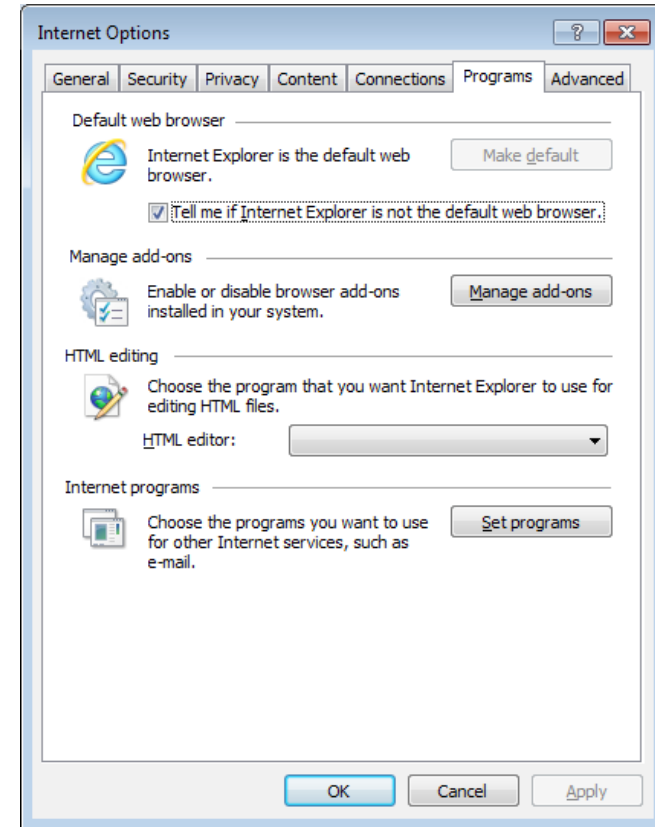
- Privacy settings control use of cookies
  - Text files containing session data
- Configure pop-up blocker





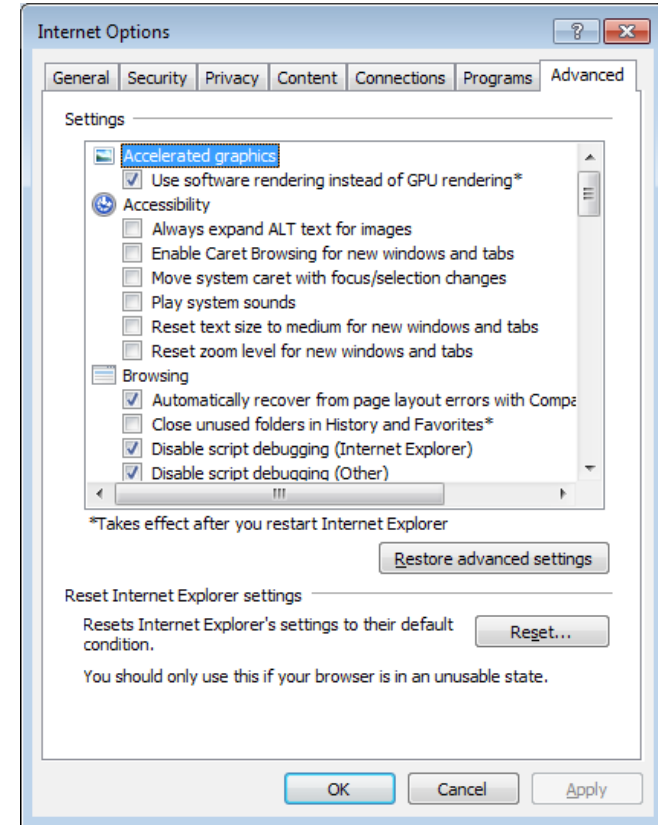
# Browser Configuration (Slide 6 of 7)

- Check or set default browser
- Manage add-ons



# Browser Configuration (Slide 7 of 7)

- Various advanced settings and options
- Resetting the browser



# Activity

