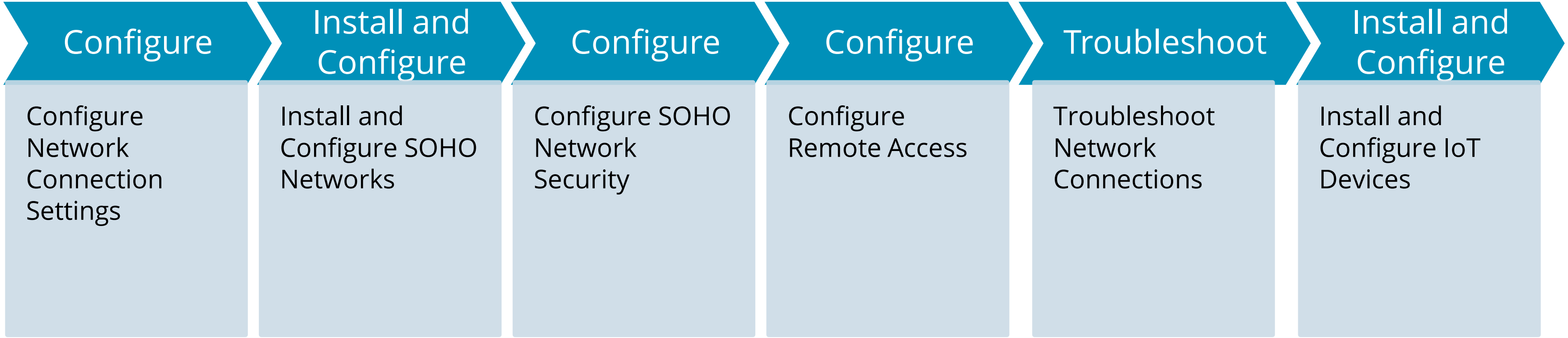
CH6: Network Operations and Diagnostics

© www.SoftwareTestingHelp.com
NETWORK TROUBLESHOOTING
Steps and Tips for Detection and Closure

Topic A: Configuring and Troubleshooting Networks



Configure

Configure Network Connection Settings

Install and Configure

Install and Configure SOHO Networks

Configure

Configure SOHO Network Security

Configure

Configure Remote Access

Troubleshoot

Troubleshoot Network Connections

Install and Configure

Install and Configure IoT Devices

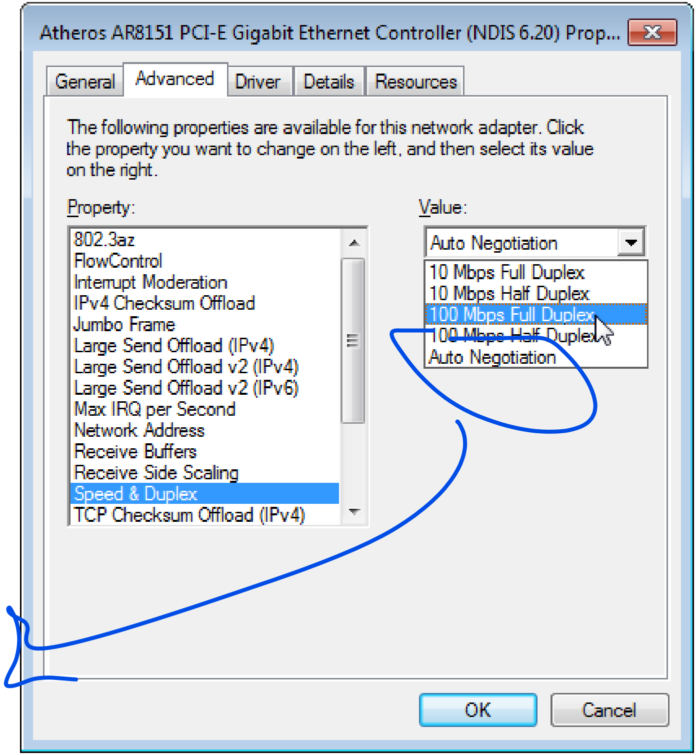
NIC Properties

- 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

Test


Atheros AR8151 PCI-E Gigabit Ethernet Controller (NDIS 6.20) Prop...

The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property:

- 802.3az
- FlowControl
- Interrupt Moderation
- IPv4 Checksum Offload
- Jumbo Frame
- Large Send Offload (IPv4)
- Large Send Offload v2 (IPv4)
- Large Send Offload v2 (IPv6)
- Max IRQ per Second
- Network Address
- Receive Buffers
- Receive Side Scaling
- Speed & Duplex
- TCP Checksum Offload (IPv4)

Value: Auto Negotiation

- 10 Mbps Full Duplex
- 10 Mbps Half Duplex
- 100 Mbps Full Duplex
- 100 Mbps Half Duplex
- Auto Negotiation

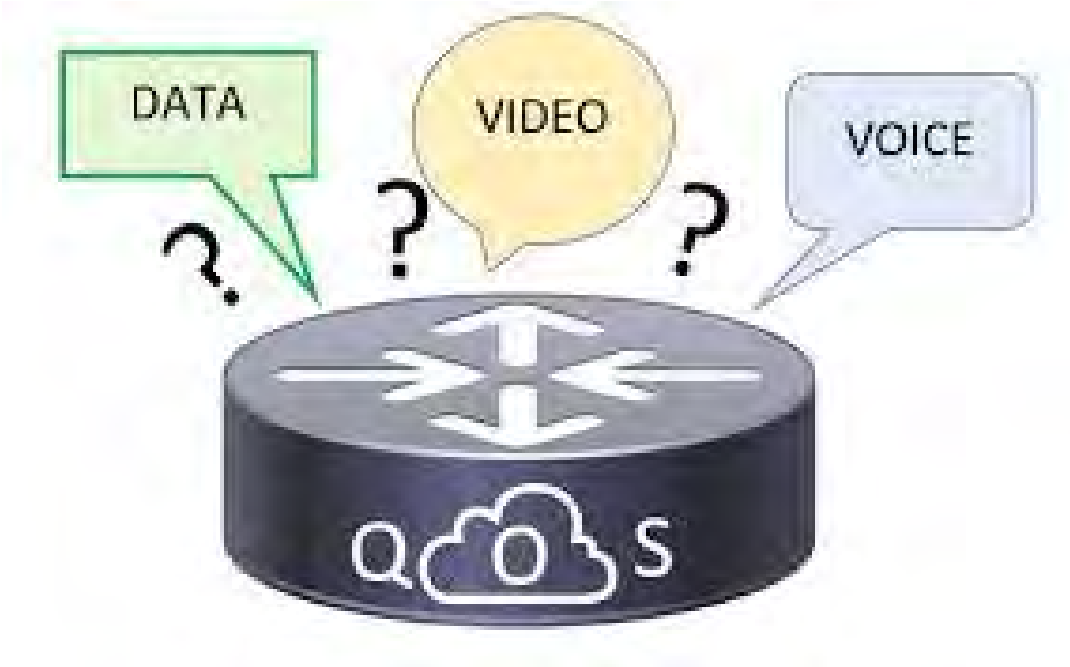
QoS

Network protocol that prioritizes some types of traffic.

Can help ensure real-time applications such as VoIP or video conference have priority.

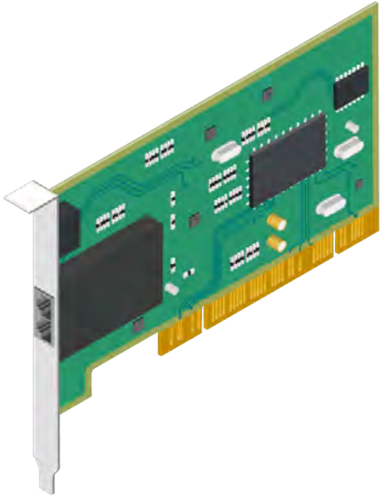
QoS usually configured on managed switches.

May need to enable QoS protocol on adapter.

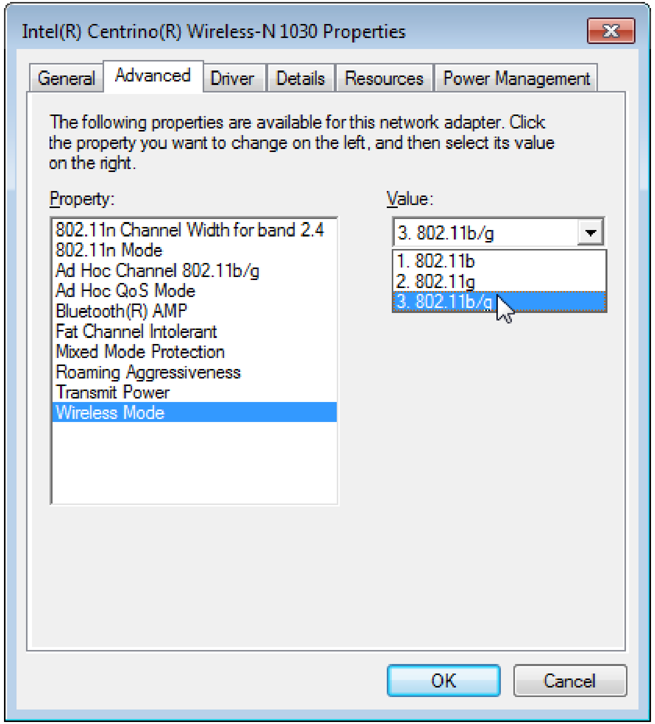


Onboard Network Cards

- 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



Intel(R) Centrino(R) Wireless-N 1030 Properties

The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property:

- 802.11n Channel Width for band 2.4
- 802.11n Mode
- Ad Hoc Channel 802.11b/g
- Ad Hoc QoS Mode
- Bluetooth(R) AMP
- Fat Channel Intolerant
- Mixed Mode Protection
- Roaming Aggressiveness
- Transmit Power
- Wireless Mode

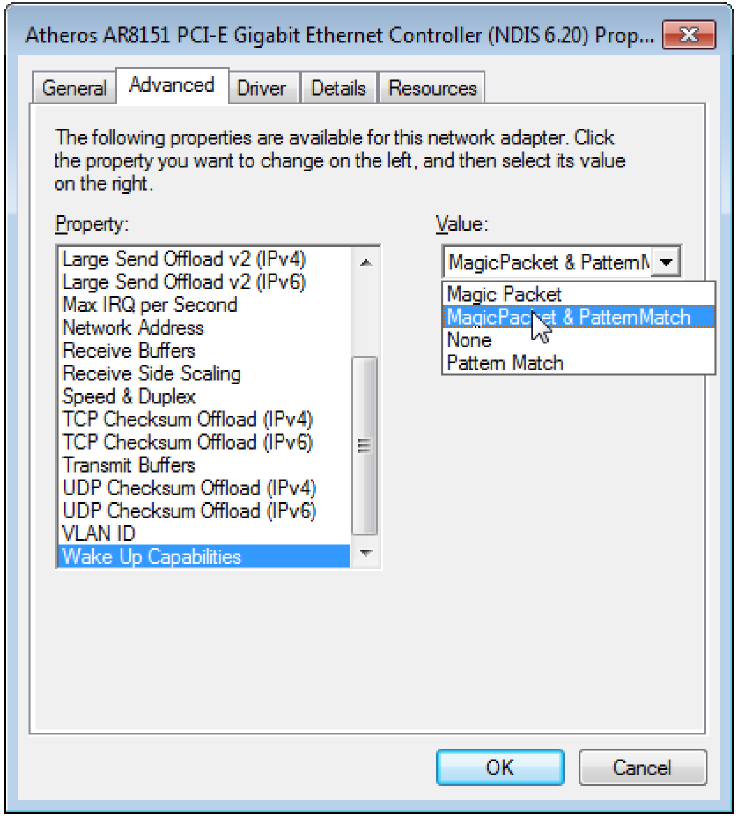
Value: 3. 802.11b/g

- 1. 802.11b
- 2. 802.11g
- 3. 802.11b/g

- 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



Atheros AR8151 PCI-E Gigabit Ethernet Controller (NDIS 6.20) Prop...

The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property:

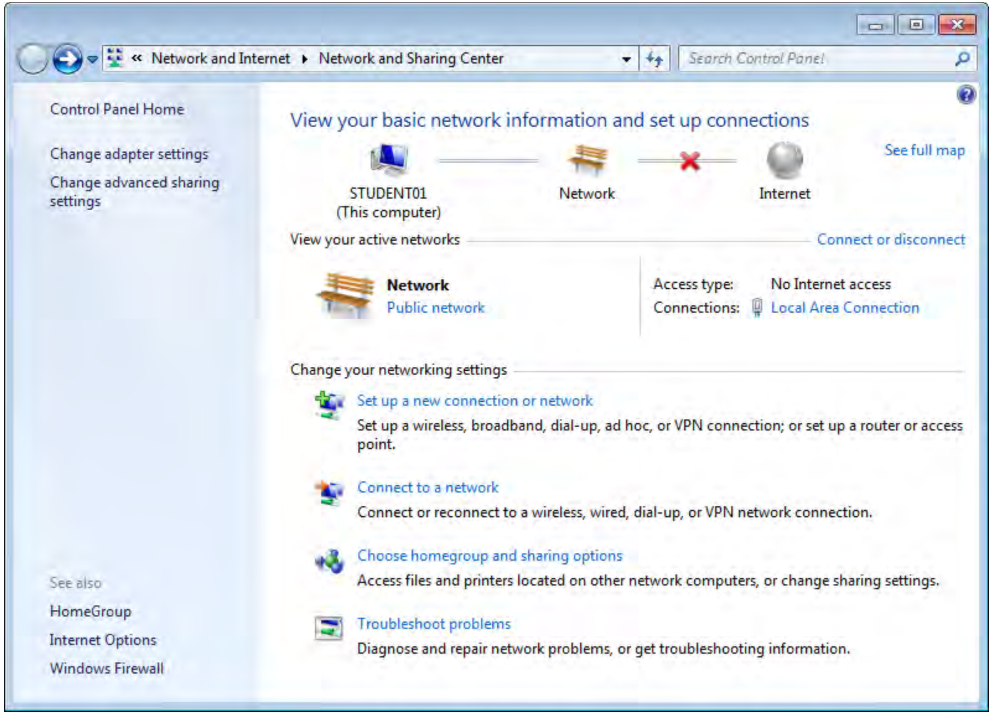
- Large Send Offload v2 (IPv4)
- Large Send Offload v2 (IPv6)
- Max IRQ per Second
- Network Address
- Receive Buffers
- Receive Side Scaling
- Speed & Duplex
- TCP Checksum Offload (IPv4)
- TCP Checksum Offload (IPv6)
- Transmit Buffers
- UDP Checksum Offload (IPv4)
- UDP Checksum Offload (IPv6)
- VLAN ID
- Wake Up Capabilities

Value: MagicPacket & PatternM

- Magic Packet
- MagicPacket & PatternMatch
- None
- Pattern Match

Network Connections in Windows

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



View your basic network information and set up connections

View your active networks

Network
Public network

Access type: No Internet access
Connections: Local Area Connection

Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

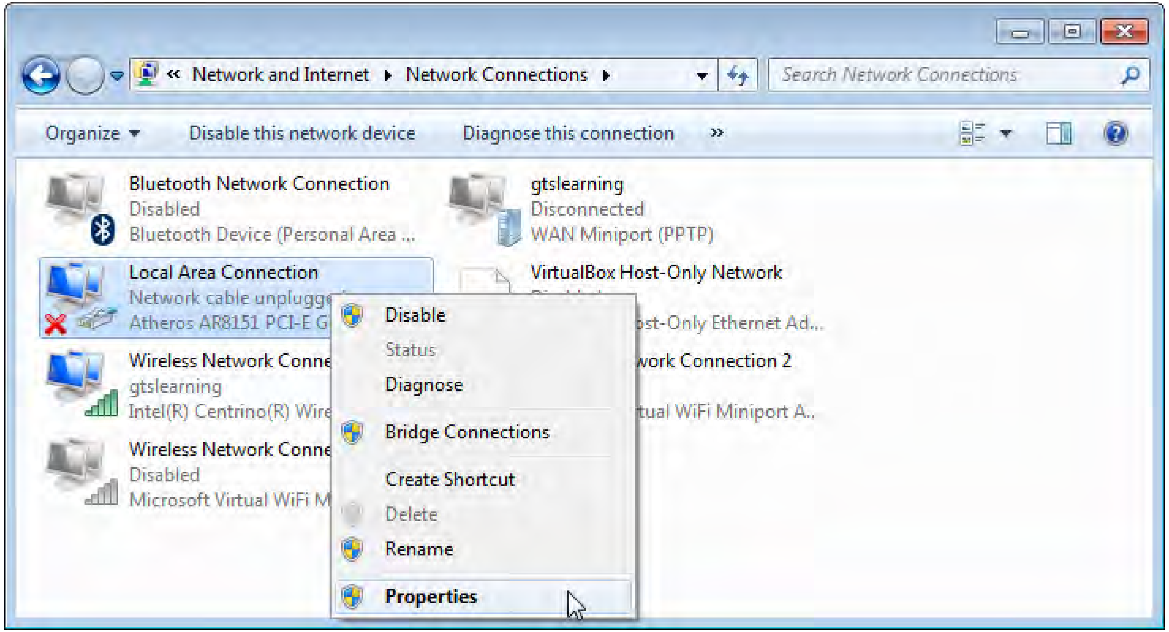
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

Network Connections in Windows

- Access adapter properties
- Wired/wireless adapter names vary



Network and Internet ▸ Network Connections ▸

Search Network Connections

Organize ▾ | Disable this network device | Diagnose this connection | »

Bluetooth Network Connection
Disabled
Bluetooth Device (Personal Area ...

gtslearning
Disconnected
WAN Miniport (PPTP)

Local Area Connection
Network cable unplugg
Atheros AR8151 PCI-E G

VirtualBox Host-Only Network
ost-Only Ethernet Ad...

Wireless Network Conne
gtslearning
Intel(R) Centrino(R) Wire

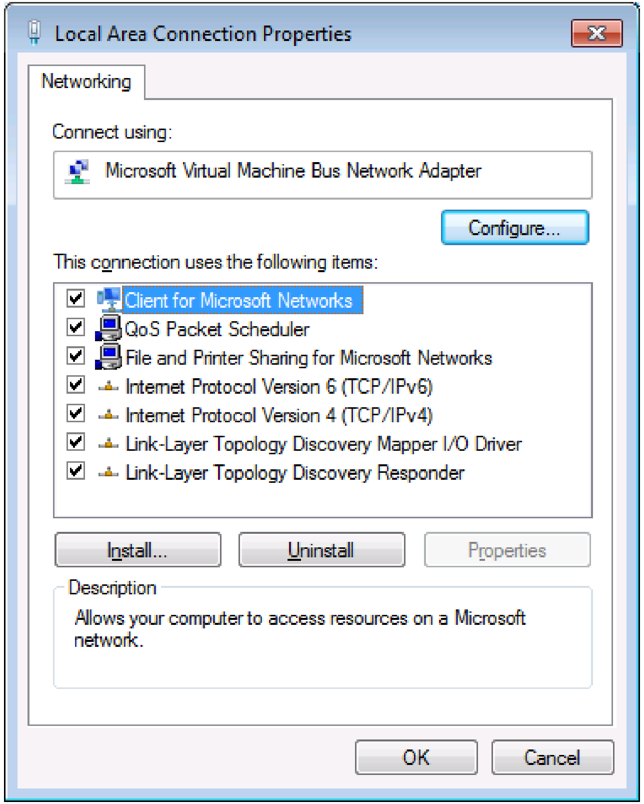
work Connection 2
tual WiFi Miniport A..

Wireless Network Conne
Disabled
Microsoft Virtual WiFi M

Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties

Network Connections in Windows

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



Local Area Connection Properties

Networking

Connect using:

Microsoft Virtual Machine Bus Network Adapter

Configure...

This connection uses the following items:

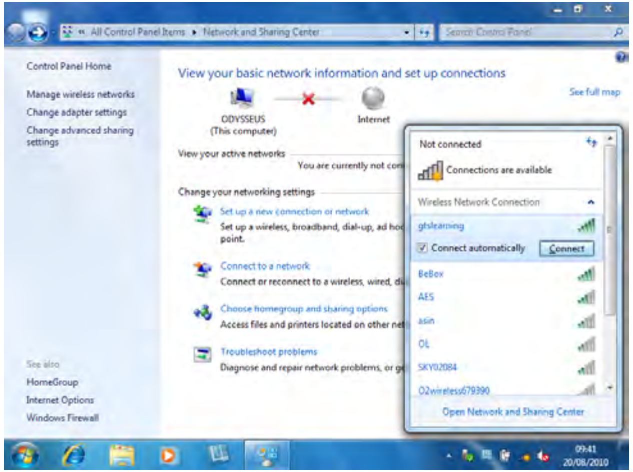
☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description

Allows your computer to access resources on a Microsoft network.

Network Connections in Windows

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



All Control Panel Items ▸ Network and Sharing Center

Search Control Panel

Control Panel Home

Manage wireless networks

Change adapter settings

Change advanced sharing settings

See also

HomeGroup

Internet Options

Windows Firewall

View your basic network information and set up connections

See full map

ODYSSEUS (This computer)

Internet

View your active networks

You are currently not con

Change your networking settings

Set up a new connection or network

Set up a wireless, broadband, dial-up, ad hoc point.

Connect to a network

Connect or reconnect to a wireless, wired, di

Choose homegroup and sharing options

Access files and printers located on other net

Troubleshoot problems

Diagnose and repair network problems, or g

Not connected

Connections are available

Wireless Network Connection

gtslearning

☑ Connect automatically Connect

BeBox

AES

asin

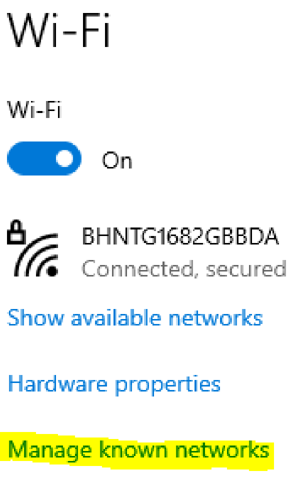
OL

SKY02084

O2wireless679390

Open Network and Sharing Center

09:41
20/08/2010



Wi-Fi

Wi-Fi

On

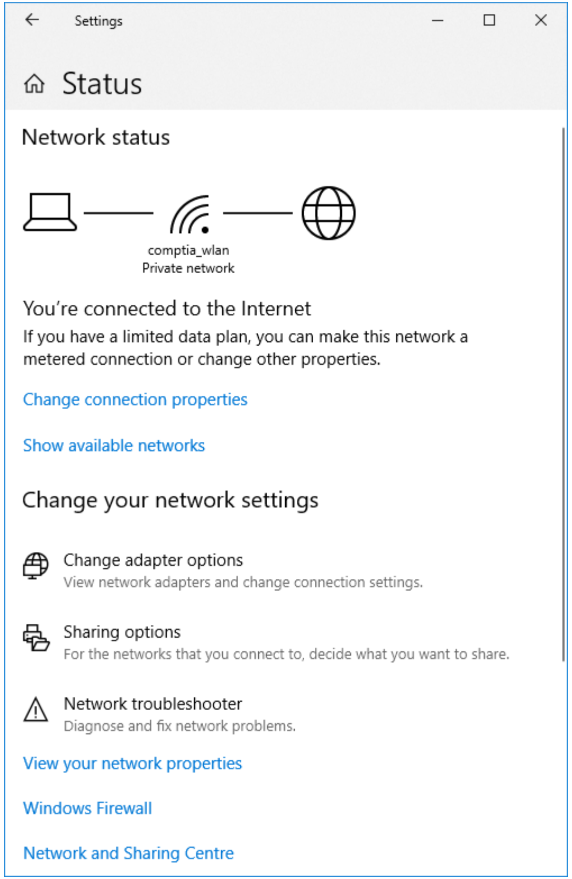
BHNTG1682GBBDA
Connected, secured

Show available networks

Hardware properties

Manage known networks

Network Connections in Windows 10



Network status

You're connected to the Internet

If you have a limited data plan, you can make this network a metered connection or change other properties.

Change connection properties

Show available networks

Change your network settings

Change adapter options
View network adapters and change connection settings.

Sharing options
For the networks that you connect to, decide what you want to share.

Network troubleshooter
Diagnose and fix network problems.

View your network properties

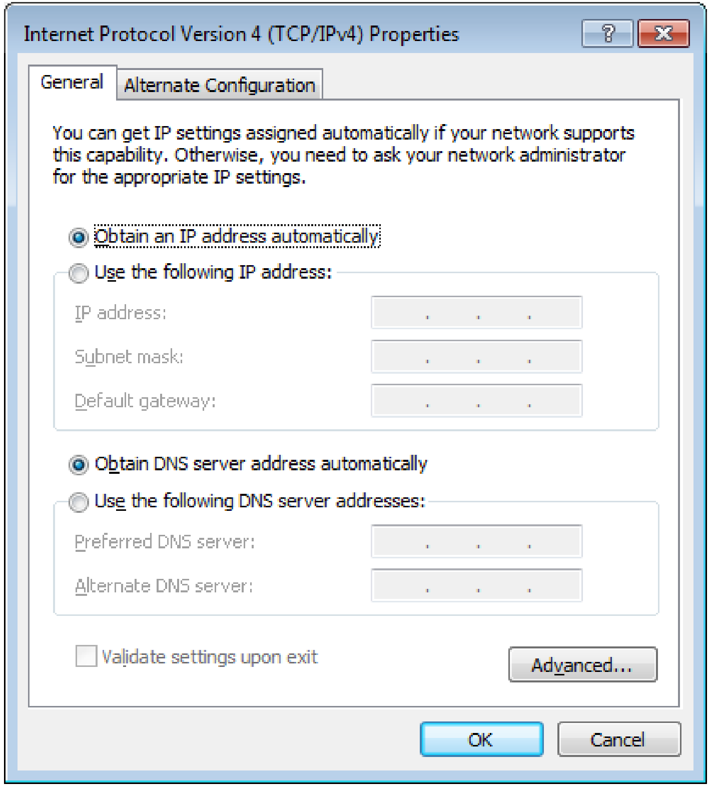
Windows Firewall

Network and Sharing Centre

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

IP Address Configuration

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



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

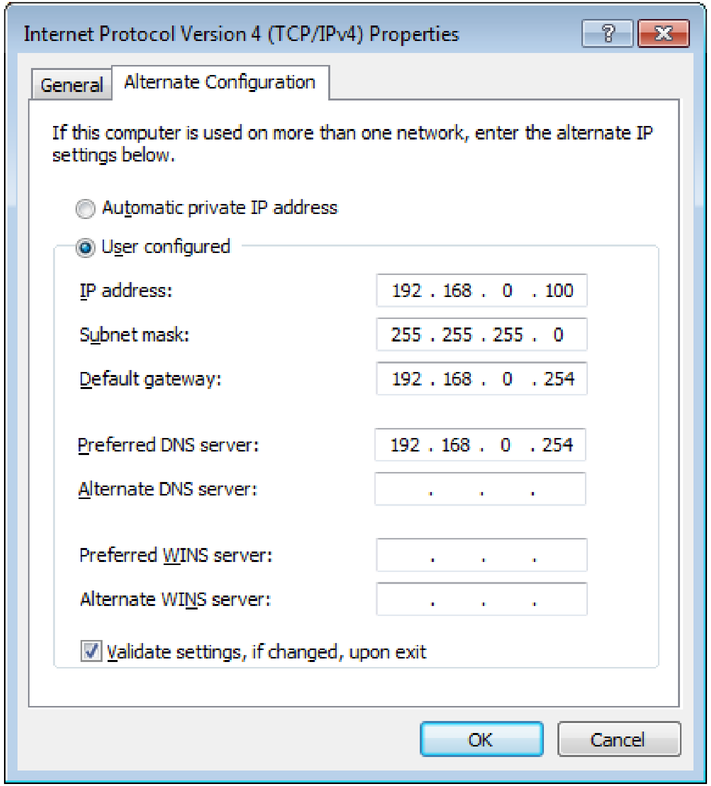
Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

IP Address Configuration

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



Internet Protocol Version 4 (TCP/IPv4) Properties

If this computer is used on more than one network, enter the alternate IP settings below.

○ Automatic private IP address

● User configured

IP address: 192 . 168 . 0 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 254

Preferred DNS server: 192 . 168 . 0 . 254

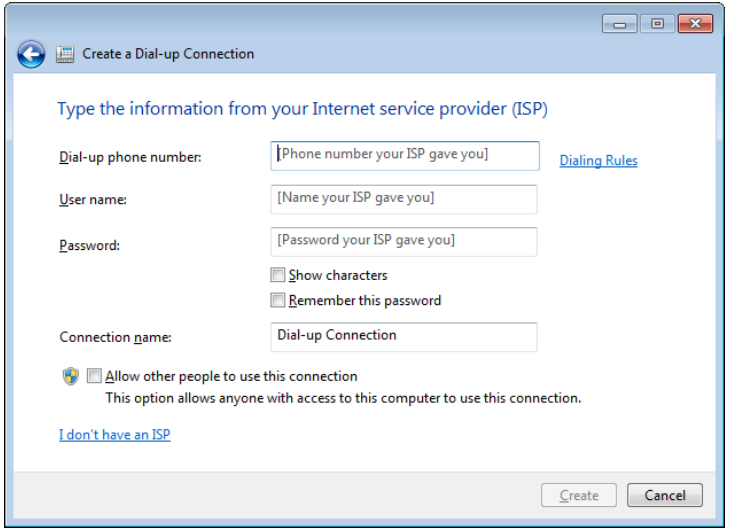
Alternate DNS server: . . .

Preferred WINS server: . . .

Alternate WINS server: . . .

☑ Validate settings, if changed, upon exit

Other Network Connections



Type the information from your Internet service provider (ISP)

Dial-up phone number: [Phone number your ISP gave you]

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.

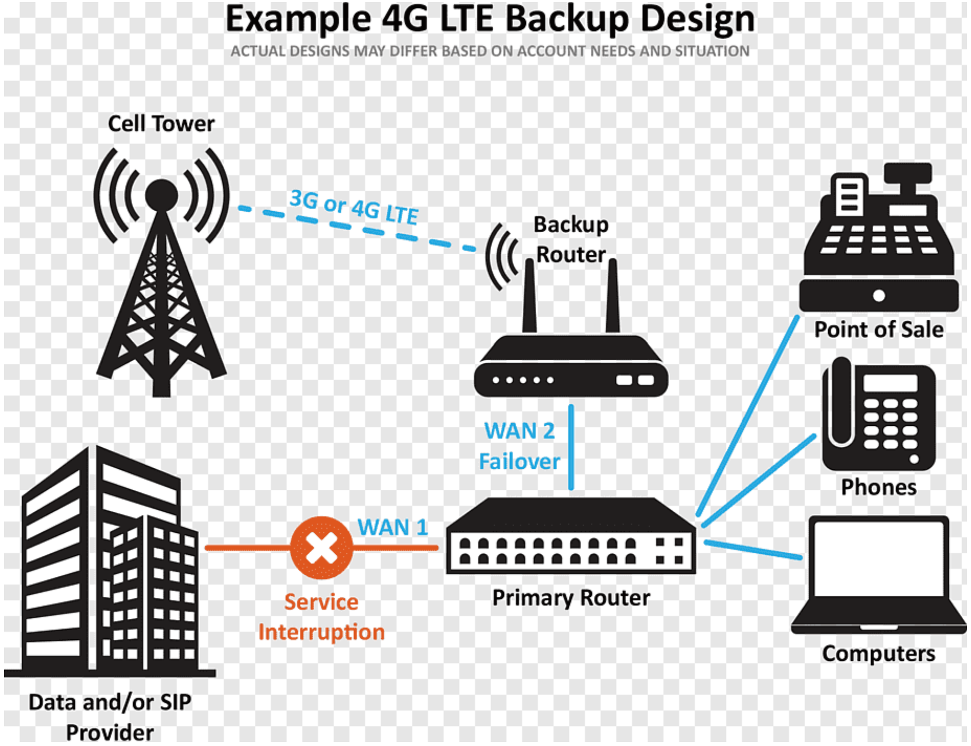
- SOHO router is typical; usually combines several functions
- Other connection options include dial-up
- Analog modem connects to ISP
- Use Set Up a Connection or Network to configure

Other Network Connections

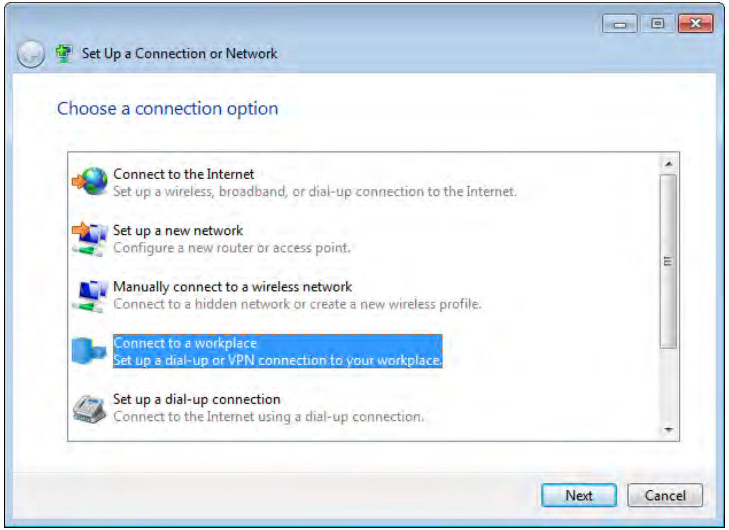
WAN cellular connects to a cell provider's network

Can be USB or internal

Install vendor software, plug in adapter, use software to view and configure



Other Network Connections



Set Up a Connection or Network

Choose a connection option

Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.

Set up a new network
Configure a new router or access point.

Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

Set up a dial-up connection
Connect to the Internet using a dial-up connection.

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

Discussing Network Connection

- **A Windows computer is configured to use DHCP, but no DHCP server is available. The computer is not using an APIPA address either. Why is this?**

- **ANSWER:**
  - It has been configured with an Alternate Configuration static IP address.

CompTIA

Discussing Network Connection

- **You need to configure duplex settings on a network adapter manually. What steps do you need to follow?**

- **ANSWER:**
  - Open **Device Manager** and the adapter's **Property** sheet. Select the **Advanced** tab and select the **Duplex** property (or **Speed and Duplex**). Change the value as required, and select **OK**.

Discussing Network Connection

- **True or false? If you want a computer to be available through Wake-on-LAN, you can disconnect it from the power supply but must leave it connected to the network data port.**

- **ANSWER:**
  - False. The network adapter must be connected to standby power, and the computer could not start anyway if it were disconnected from the power supply.

Discussing Network Connection

- **Why are IP addresses entered under DNS, and why should there be two of them?**

- **ANSWER:**
  - These are the IP addresses of DNS servers that will process client requests to resolve host and domain names to IP addresses.

  - DNS is a critical service on Windows networks and on the Internet, so a second server should always be specified for redundancy.

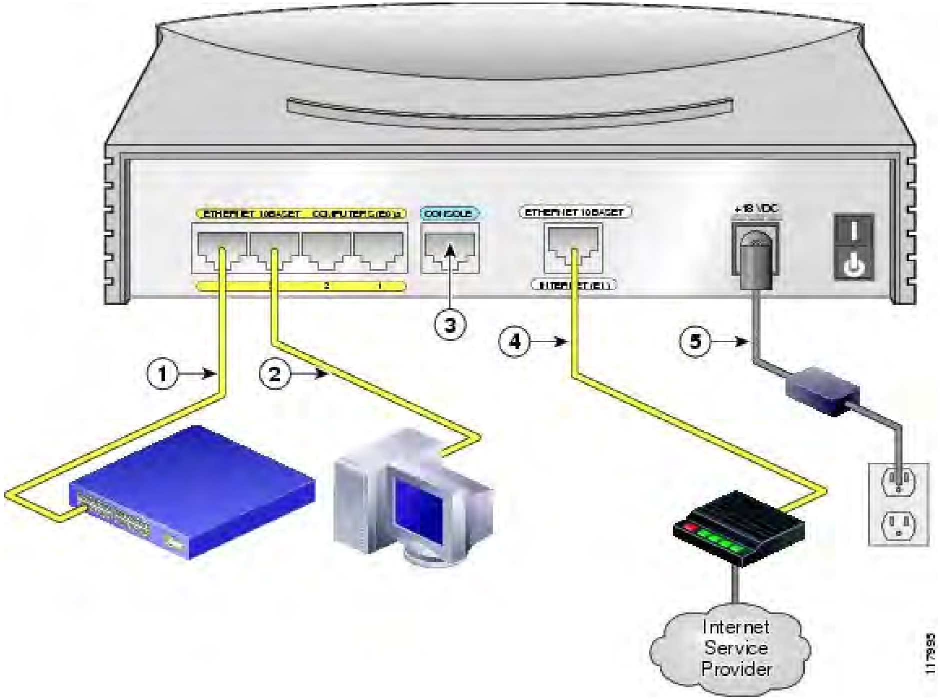
CompTIA

Discussing Network Connection

- **What parameters do you need to specify to connect to a VPN?**

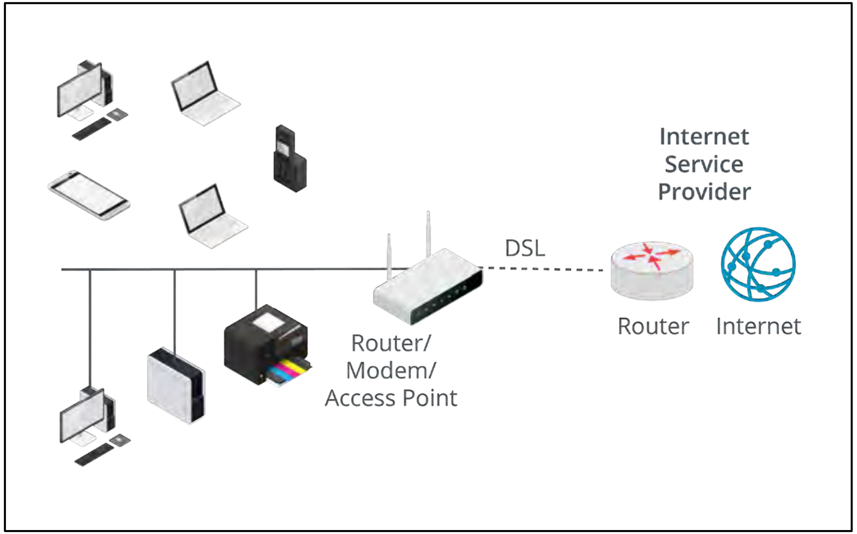
- **ANSWER:**
  - Assuming you have a remote host topology, you need to establish a connection to a server over a public network such as the Internet.
  - The VPN server then facilitates a connection to a local network. You need to specify the location of the VPN server as an IP address or Fully Qualified Domain Name (FQDN). If the VPN type is not detected automatically, you might need to configure extra settings or use third-party VPN client software. To connect to the VPN, the user must submit credentials, such as a user name and password.

Topic B: Install and Configure SOHO Networks



SOHO Networks

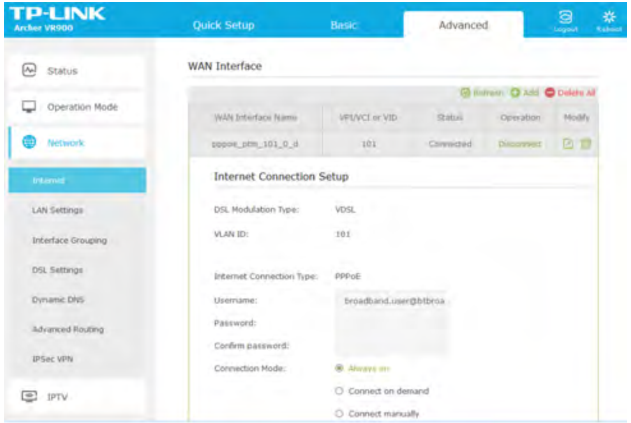
- Business network; may use centralized server as well as clients.
- Often uses single Internet device for connectivity.
- May be home/residential network as well.



SOHO Network Configuration (Slide 1 of 2)

SOHO installed on customer premises.

- Bundles several device types: Router, Switch, AP, DHCP, DNS, Firewall ex..
- Connect device to SOHO appliance to configure.
- Access management interface through browser.
- Change default password!
- Follow wizard interface to configure Internet access.



WAN Interface

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: broadband.user@btbroa

Password:

Confirm password:

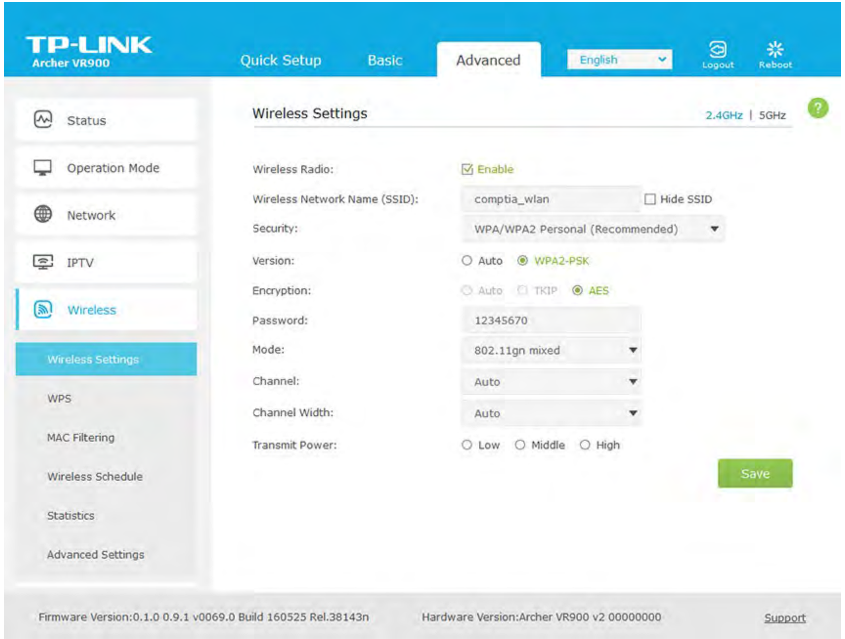
Connection Mode: ● Always on

○ Connect on demand

○ Connect manually

Wireless Settings

- Configure wireless settings; most hosts connect wirelessly.
- 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



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

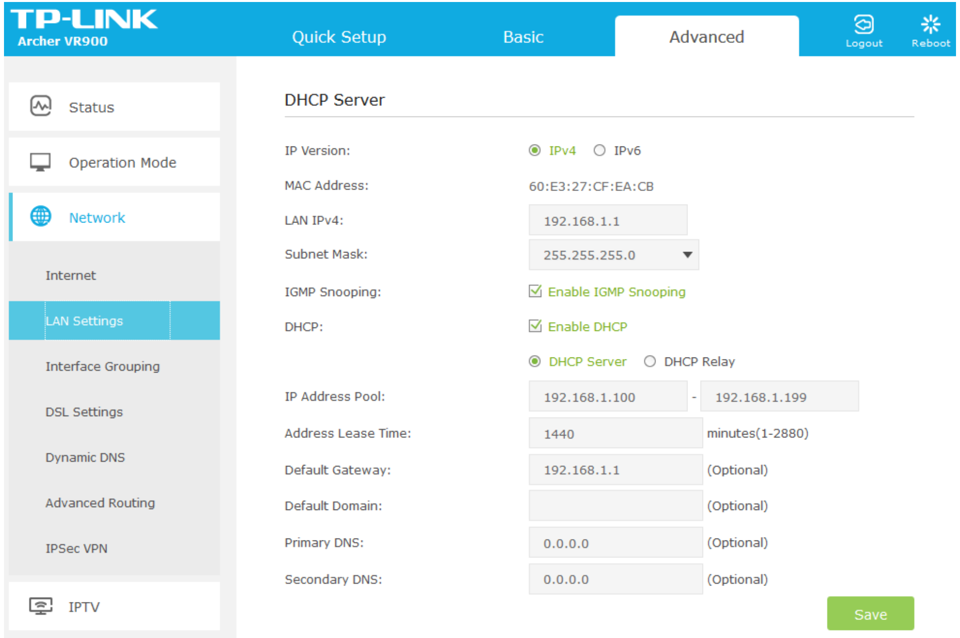
Channel: Auto

Channel Width: Auto

Transmit Power: ○ Low ○ Middle ○ High

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

DHCP and IP Address Configuration



DHCP Server

IP Version: ● IPv4 ○ IPv6

MAC Address: 60:E3:27:CF:EA:CB

LAN IPv4: 192.168.1.1

Subnet Mask: 255.255.255.0

IGMP Snooping: ☑ Enable IGMP Snooping

DHCP: ☑ Enable DHCP

● DHCP Server ○ DHCP Relay

IP Address Pool: 192.168.1.100 - 192.168.1.199

Address Lease Time: 1440 minutes(1-2880)

Default Gateway: 192.168.1.1 (Optional)

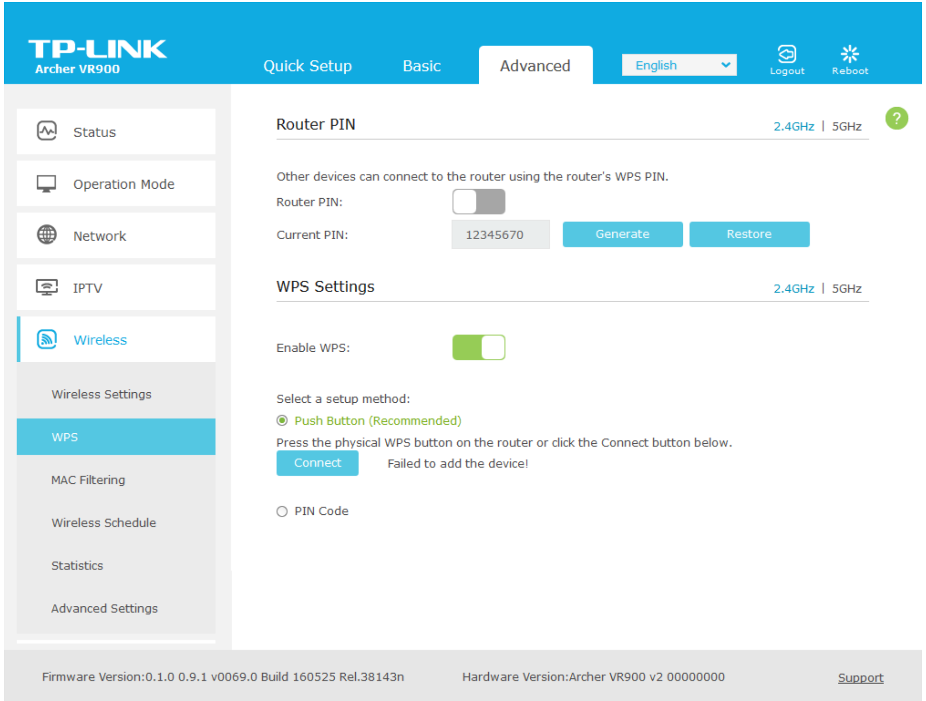
Default Domain: (Optional)

Primary DNS: 0.0.0.0 (Optional)

Secondary DNS: 0.0.0.0 (Optional)

- 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

WPA2



Router PIN 2.4GHz | 5GHz

Other devices can connect to the router using the router's WPS PIN.

Router PIN:

Current PIN: 12345670

WPS Settings 2.4GHz | 5GHz

Enable WPS:

Select a setup method:

● Push Button (Recommended)

Press the physical WPS button on the router or click the Connect button below.

Failed to add the device!

○ PIN Code

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

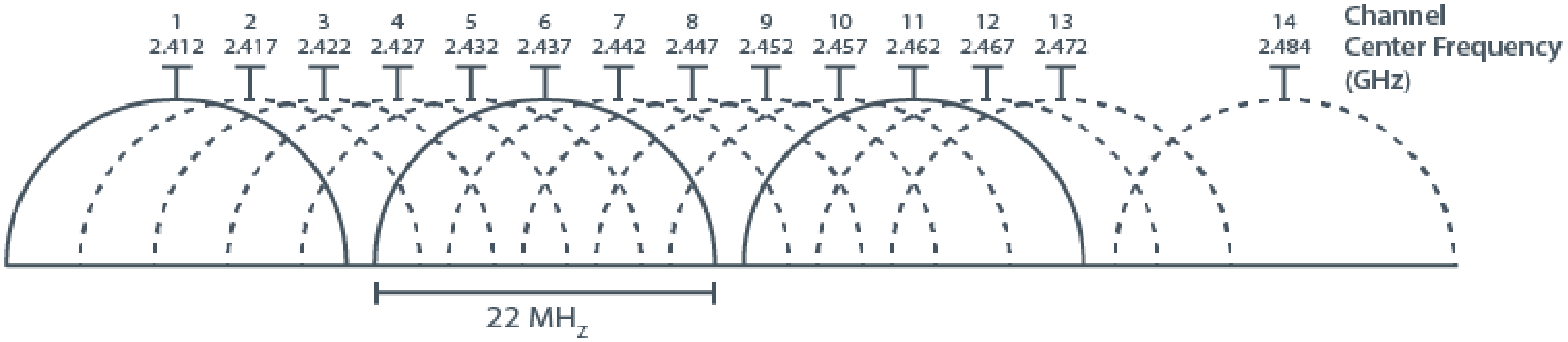
- Simplifies secure access point setup.
- AP and all adapters must be WPA-capable.
- Pushbutton on device typically causes device and AP to associate automatically over WPA2.
- Generates random SSID and passphrase.

Access Point Placement

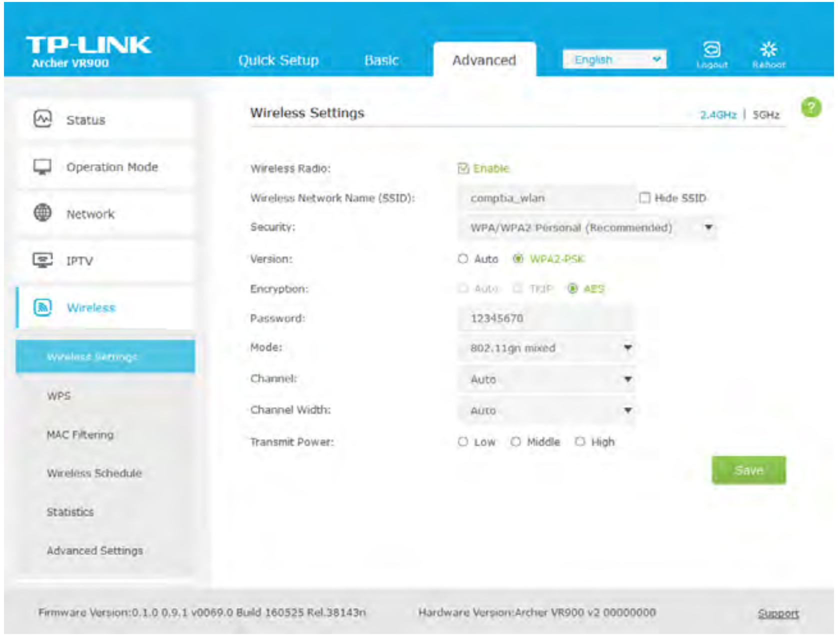
- Correct antenna and access point placement helps ensure robust network.
- AP placement made by provider’s cabling location.
- Can use extenders.
- Site survey can help identify dead zones.

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(1,6,11)
- Newer APs detect least-congested channel at boot.
- Use spectrum analyzer to find least busy channels.



Radio Power Levels



Wireless Settings

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

Firmware Version:0.1.0 0.9.1 v0069.0 Build 160525 Rel.38143n

Hardware Version:Archer VR900 v2 00000000

- Can turn down AP power to prevent War Driving.
- May expose to “evil twin” attack if a rogue AP is detected first.
- Increasing power may also cause signal bouncing.
- 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

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 & 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.

Discussing SOHO Network Installation and Configuration

- **What type of cable and connectors are used to connect a modem to a phone port?**

- **ANSWER:**
  - Twisted pair with RJ-11 connectors. In the UK, the phone port might use a BT-style connector though.

Discussing SOHO Network Installation and Configuration

- **To configure a router/modem, what type of IP interface configuration should you apply to the computer you are using to access the device administration web app?**

- **ANSWER:**
  - Set the adapter to obtain an IP address automatically.
  - The router/modem will be running a (DHCP) server that will allocate an appropriate IP address and DNS server.

Discussing SOHO Network Installation and Configuration

- **What is the function of a microfilter?**

- **ANSWER:**
  - It screens noise from data signals on jacks for voice or fax devices if DSL equipment is connected.

CompTIA

Discussing SOHO Network Installation and Configuration

- **What is the effect of reducing transmit power when you are configuring an access point?**

- **ANSWER:**
  - It reduces the supported range of the access point.
  - You might do this to prevent interference between two access points in proximity.
  - You might also reduce power to prevent the network being accessible outside.

CompTIA

Discussing SOHO Network Installation and Configuration

- **How can QoS improve performance for SOHO Internet access?**

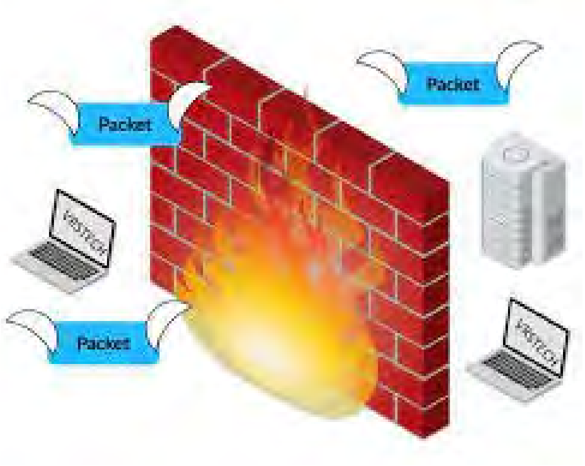
- **ANSWER:**
  - A Quality of Service (QoS) mechanism allows you to elevate certain types of traffic to a higher priority to be processed by the router/modem.

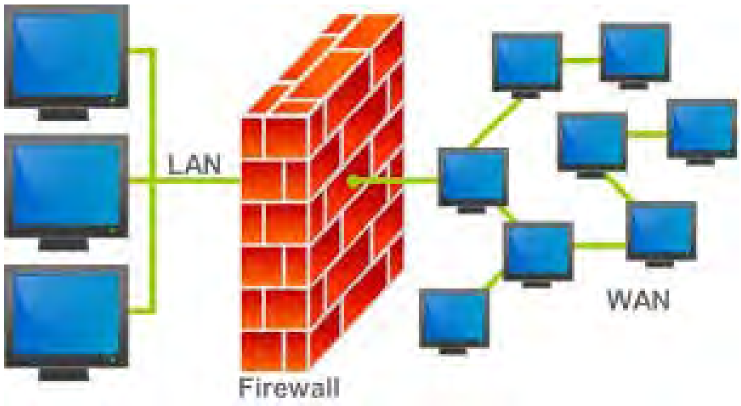
Discussing SOHO Network Installation and Configuration

- **Which standard represents the best available wireless network security?**

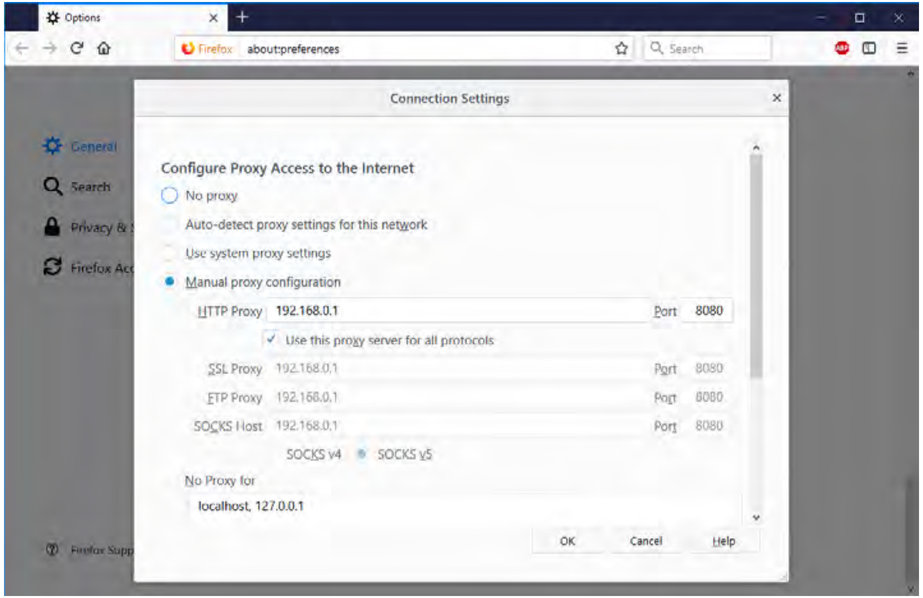
- **ANSWER:**
  - Wi-Fi Protected Access version 2 (WPA2).
  - Enterprise mode is more secure. Each user connects with his or her network credential, which is validated by an authentication server (typically RADIUS).

Topic C: Configure SOHO Network Security





Proxy Servers



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 192.168.0.1 Port 8080

☑ Use this proxy server for all protocols

SSL Proxy 192.168.0.1 Port 8080

FTP Proxy 192.168.0.1 Port 8080

SOCKS Host 192.168.0.1 Port 8080

○ SOCKS v4 ● SOCKS v5

No Proxy for

localhost, 127.0.0.1

OK Cancel Help

- User access from local network to Internet/websites:
  - Transparent proxy automatically intercepts requests
  - Non-transparent proxy requires client configuration with server IP address and proxy service port
- Can apply content filtering and time restrictions
- Caching function to improve performance

Spam Gateways and Unified Threat Management

- Network security functions
  - Firewalls
  - Intrusion detection systems (IDS)
  - Anti-virus/anti-malware solutions
  - Spam gateways
  - Content filters
  - Data leak/loss prevention (DLP) systems

- Unified Threat Management (UTM)
  - Single appliance/gateway that performs multiple security functions

Unified Threat Management (UTM)

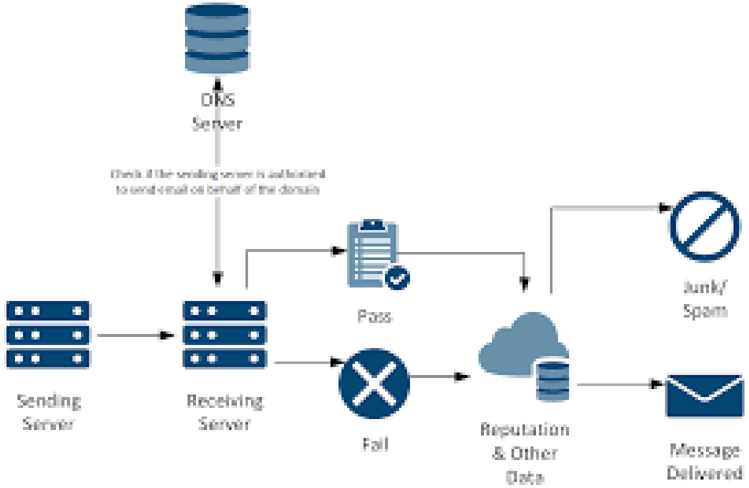
Security functions could be deployed as separate appliances or server applications, each with its own configuration and logging/reporting system.

- Unified Threat Management (UTM)
  - Single appliance/gateway that performs multiple security functions.
  - UTM centralizes the threat management service, providing simpler configuration and reporting compared to isolated applications spread across several servers or devices.

Spam Gateways

- Spam gateways: Use SPF, DKIM, and DMARC to verify the authenticity of mail servers and are configured with filters that can identify spoofed, misleading, malicious, or otherwise unwanted messages.

- Unified Threat Management (UTM)
  - Single appliance/gateway that performs multiple security functions

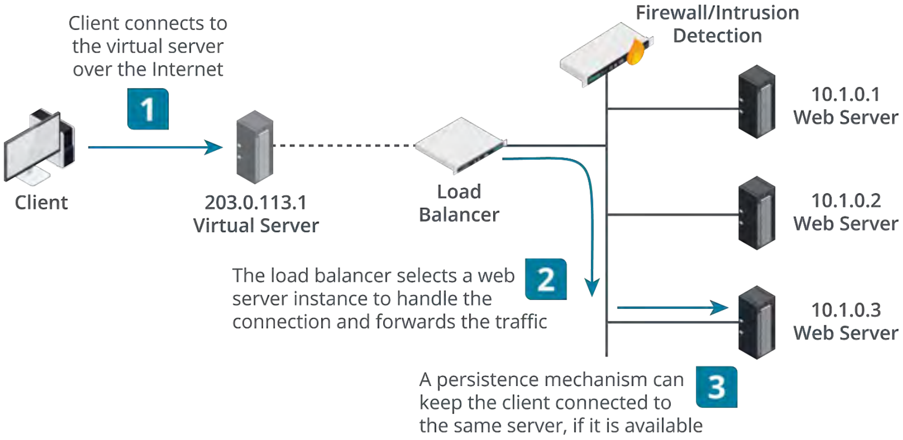


Load Balancers

- Distribute client requests between servers.

- Inbound client requests
  - Web, DNS, and mail servers and filtering.

  - Virtual server address


Client connects to the virtual server over the Internet
1
Client
203.0.113.1
Virtual Server
Load
Balancer
Firewall/Intrusion
Detection
10.1.0.1
Web Server
10.1.0.2
Web Server
10.1.0.3
Web Server
The load balancer selects a web server instance to handle the connection and forwards the traffic
2
A persistence mechanism can keep the client connected to the same server, if it is available
3

Images © 123RF.com

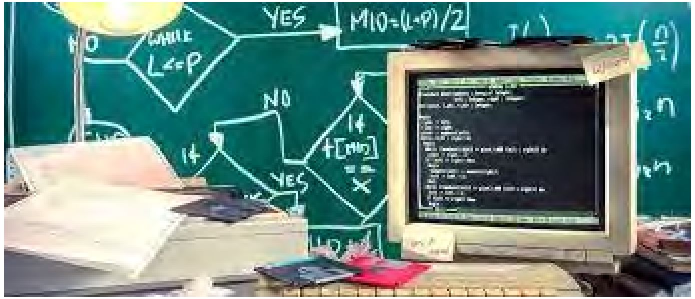
Legacy Systems

- Legacy systems
  - Vendor is no longer active
  - Product is deprecated by vendor as End of Life (EOL)

- Lack of support
- Risks from unpatchable vulnerabilities

Used for backwards compatibility with:

- Programs
- Equipment



Embedded Systems and SCADA

SCADA / ICS

- Supervisory Control and Data Acquisition System (SCADA)
  - SCADA PCs used to monitor multiple-site ICSs
  - Industrial Control Systems (ICS) Large-scale, multi-site

- Embedded systems designed to perform a specific, dedicated function.
  - Water pressure-rate meter
  - Large and complex as an industrial electric plant.
  - Operate within a closed network

Embedded Systems and SCADA

important

Workflow and process automation systems:

- Industrial control system (ICS) –Does the process automation

  Programmable logic controller (PLC):

  - PLCs are linked by a cabled network to actuators that operate valves, motors, Temp gages, and sensors

  Operational technology (OT) network:

  - Is a reference to An embedded system network to distinguish it from an IT network

  Human-machine interfaces (HMI) :

  - Output and configuration of a PLC is done by HMI

Embedded Systems and SCADA

Workflow and process automation systems:

PLCs are connected within a control loop, and the whole process automation system can be governed by a control server.

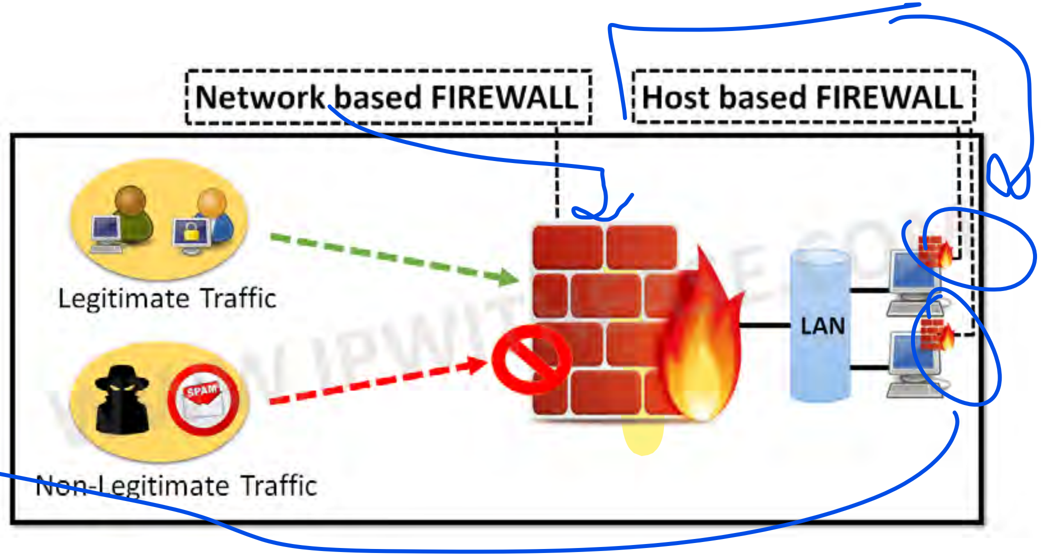
- Another important concept is the data historian, which is a database of all the information generated by the control loop.

Firewalls

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



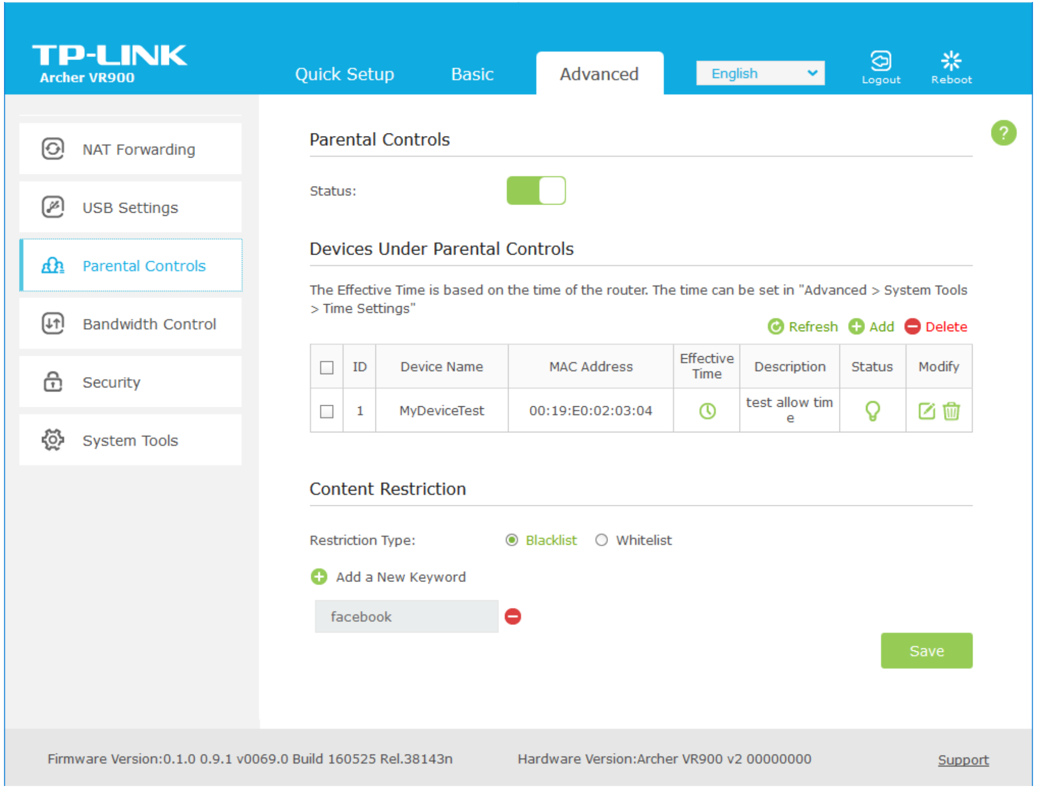
Firewalls

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

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



Parental Controls

Status: on

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"

□	ID	Device Name	MAC Address	Effective Time	Description	Status	Modify
□	1	MyDeviceTest	00:19:E0:02:03:04	🕓	test allow tim e	💡	✎ 🗑

Content Restriction

Restriction Type: ● Blacklist ○ Whitelist

Add a New Keyword

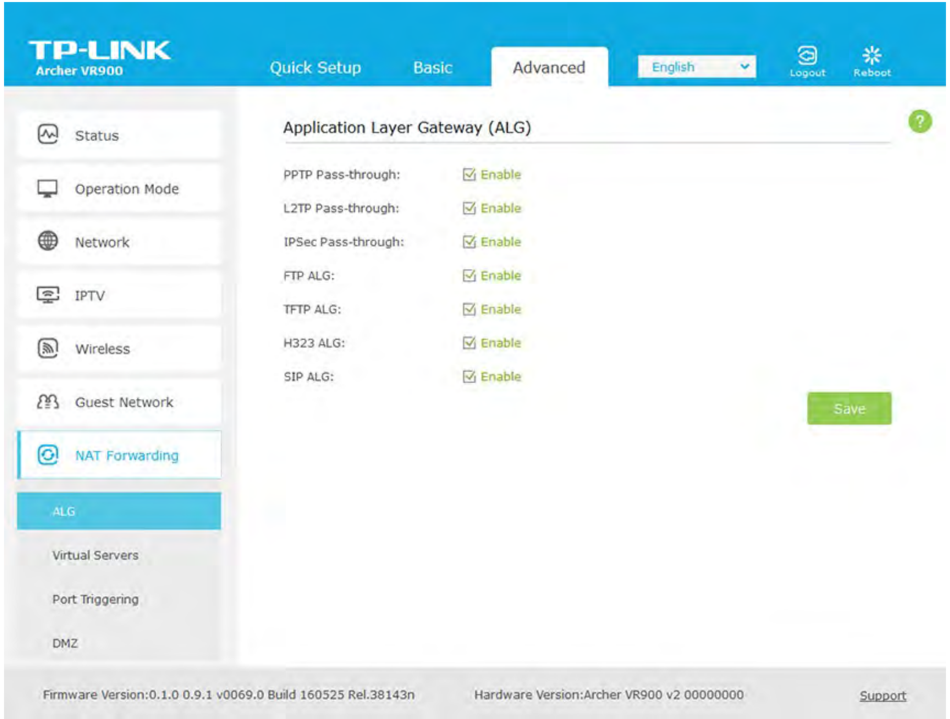
facebook

Firmware Version:0.1.0 0.9.1 v0069.0 Build 160525 Rel.38143n

Hardware Version:Archer VR900 v2 00000000

NAT

- All routers/modems use NAT
- 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



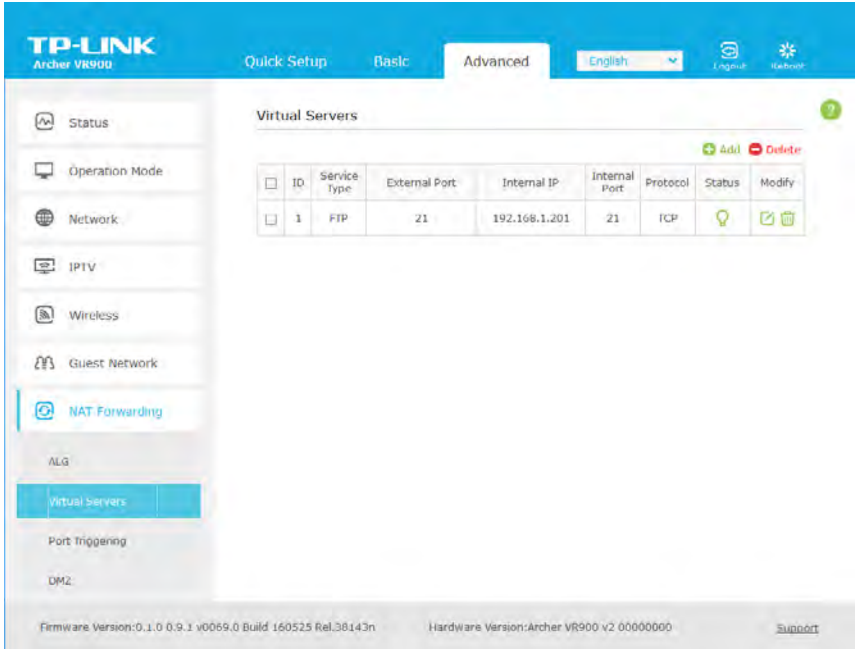
Application Layer Gateway (ALG)

PPTP Pass-through: ☑ Enable
L2TP Pass-through: ☑ Enable
IPSec Pass-through: ☑ Enable
FTP ALG: ☑ Enable
TFTP ALG: ☑ Enable
H323 ALG: ☑ Enable
SIP ALG: ☑ Enable

Firmware Version:0.1.0 0.9.1 v0069.0 Build 160525 Rel.38143n

Hardware Version:Archer VR900 v2 00000000

Port Forwarding and Port Triggering



Virtual Servers

□	ID	Service Type	External Port	Internal IP	Internal Port	Protocol	Status	Modify
□	1	FTP	21	192.168.1.201	21	TCP		

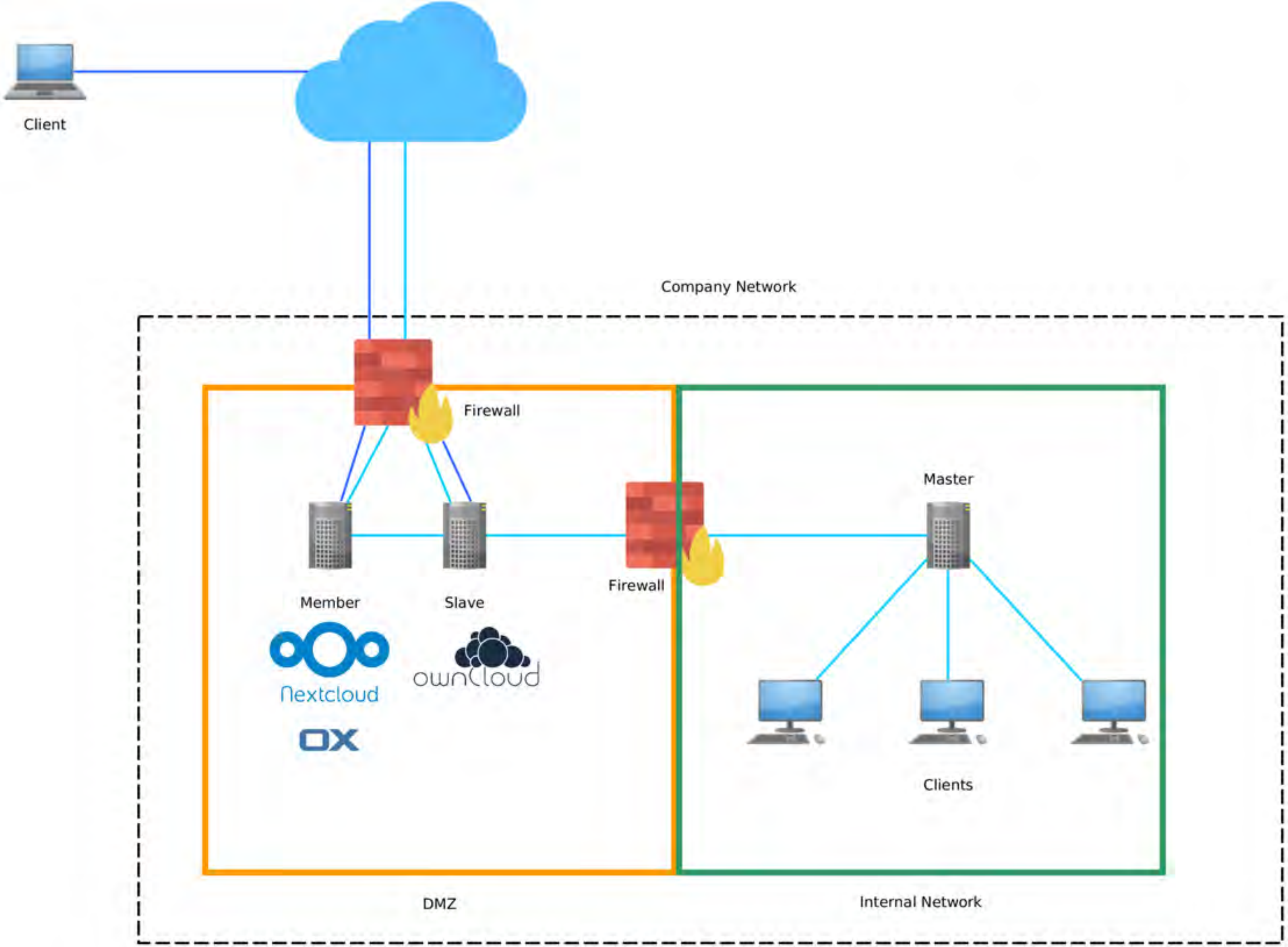
Firmware Version:0.1.0 0.9.1 v0069.0 Build 160525 Rel.38143n Hardware Version:Archer VR900 v2 00000000 Support

- 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.

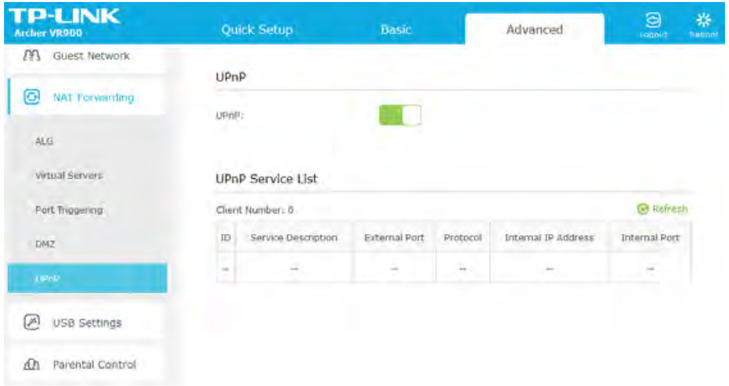
DMZ

- 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.

DMZ


Client
Company Network
Firewall
Master
Member
Slave
Firewall
Nextcloud
ownCloud
OX
Clients
DMZ
Internal Network

Universal Plug-and-Play



UPnP

UPnP: ●

UPnP Service List

Client Number: 0

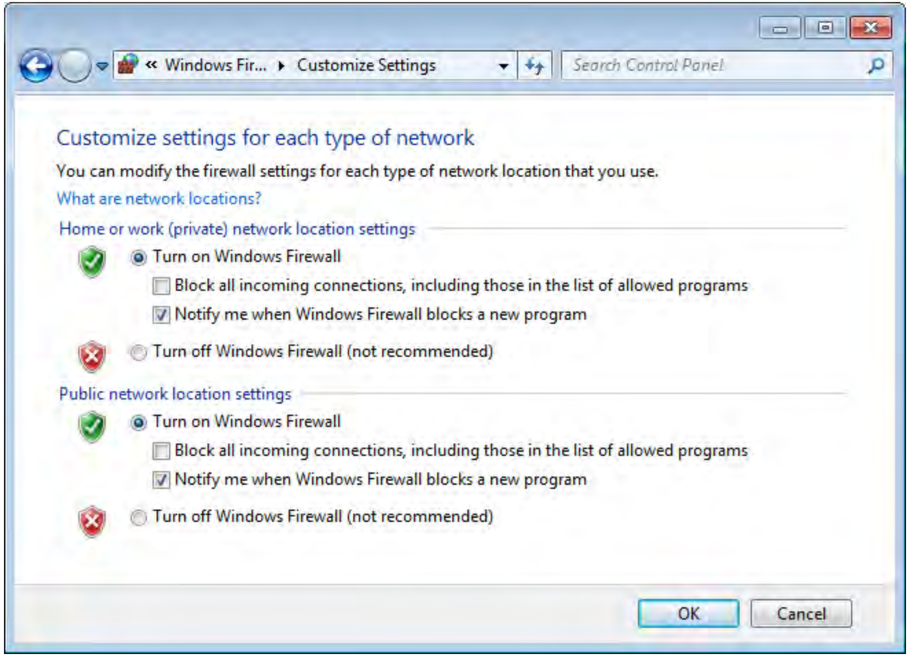
ID	Service Description	External Port	Protocol	Internal IP Address	Internal Port
--	--	--	--	--	--

- 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

Each version has become more advanced

Configure in Control Panel



Customize settings for each type of network

You can modify the firewall settings for each type of network location that you use.

What are network locations?

Home or work (private) network location settings

● Turn on Windows Firewall

□ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

○ Turn off Windows Firewall (not recommended)

Public network location settings

● Turn on Windows Firewall

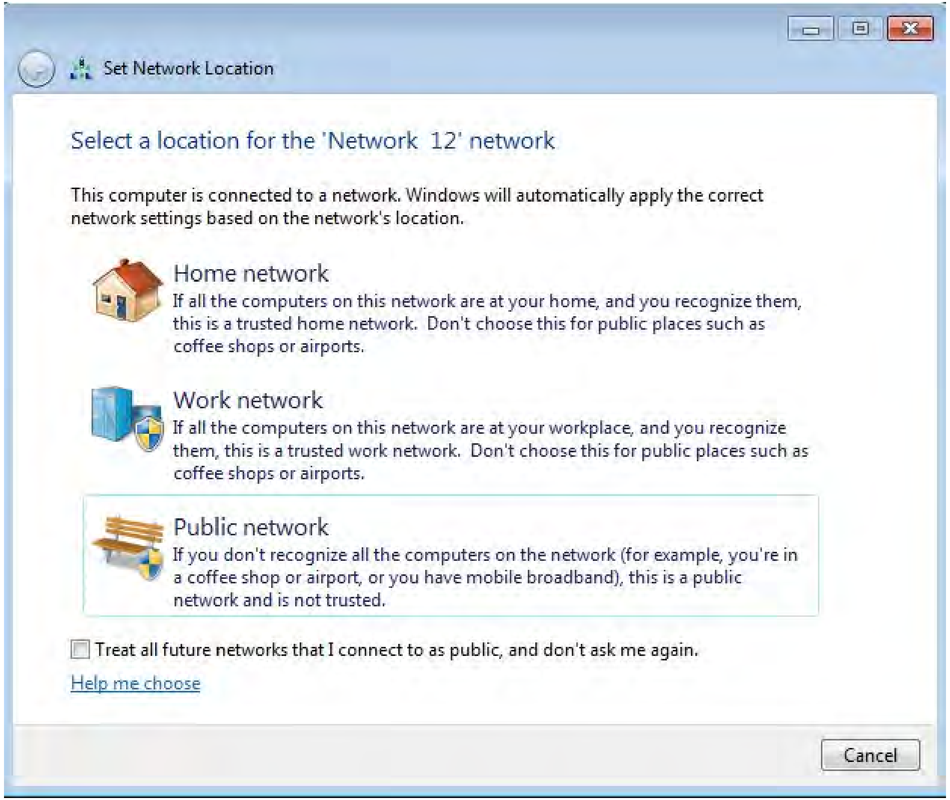
□ Block all incoming connections, including those in the list of allowed programs

☑ Notify me when Windows Firewall blocks a new program

○ Turn off Windows Firewall (not recommended)

Location Awareness

- 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.



Select a location for the 'Network 12' network

This computer is connected to a network. Windows will automatically apply the correct network settings based on the network's location.

Home network
If all the computers on this network are at your home, and you recognize them, this is a trusted home network. Don't choose this for public places such as coffee shops or airports.

Work network
If all the computers on this network are at your workplace, and you recognize them, this is a trusted work network. Don't choose this for public places such as coffee shops or airports.

Public network
If you don't recognize all the computers on the network (for example, you're in a coffee shop or airport, or you have mobile broadband), this is a public network and is not trusted.

□ Treat all future networks that I connect to as public, and don't ask me again.

Help me choose

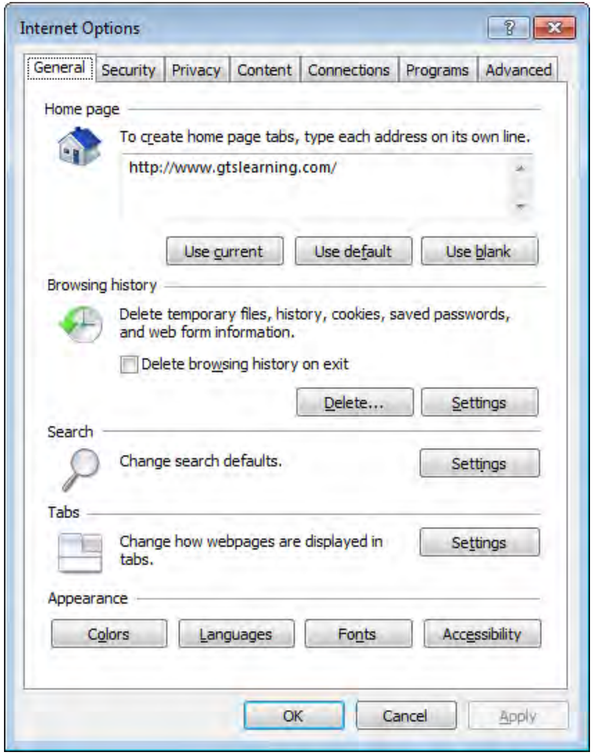
Browser Configuration

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.



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

Home page

To create home page tabs, type each address on its own line.

http://www.gtslearning.com/

Use current | Use default | Use blank

Browsing history

Delete temporary files, history, cookies, saved passwords, and web form information.

☐ Delete browsing history on exit

Delete... | Settings

Search

Change search defaults. | Settings

Tabs

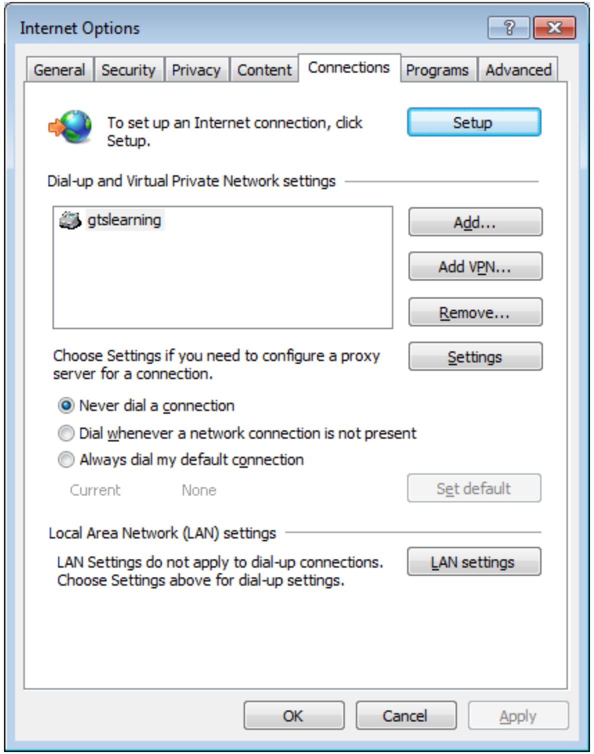
Change how webpages are displayed in tabs. | Settings

Appearance

Colors | Languages | Fonts | Accessibility

OK | Cancel | Apply

Browser Configuration



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

gtslearning

Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection

○ Dial whenever a network connection is not present

○ Always dial my default connection

Current None

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

Network Security & Embedded Appliances

- **You are recommending that a small business owner replace separate firewall and antimalware appliances with a UTM. What is the principal advantage of doing this??**

- **ANSWER:**
- A unified threat management (UTM) appliance consolidates the configuration, monitoring, and reporting of multiple security functions to a single console or dashboard.

Network Security & Embedded Appliances

- **You are setting up a games console on a home network. What feature on the router will simplify configuration of online multiplayer gaming?**

- **ANSWER:**
  - Universal Plug and Play (UPnP).

Network Security & Embedded Appliances

- **You are advising a customer about replacing the basic network address translation (NAT) function performed by a SOHO router with a device that can work as a proxy. The customer understands the security advantages of this configuration. What other benefit can it have?**

- **ANSWER:**
- The proxy can be configured to cache data that is commonly requested by multiple clients, reducing bandwidth consumption and speeding up requests.

Network Security & Embedded Appliances

- **A network owner has configured three web servers to host a website. What device can be deployed to allow them to work together to service client requests more quickly?**

- **ANSWER:**
- A load balancer..

Network Security & Embedded Appliances

- **You are writing an advisory to identify training requirements for support staff and have included OT networks as one area not currently covered.**
- **Another technician thinks you should have written IT. Are they correct??**

- **ANSWER:**
- No. Operational technology (OT) refers to networks that connect embedded systems in industrial and process automation systems.

Network Security & Embedded Appliances

- **You are auditing your network for the presence of legacy systems. Should you focus exclusively on identifying devices and software whose vendor has gone out of business?**

- **ANSWER:**
- No. While this can be one reason for products becoming unsupported, vendors can also deprecate use of products that they will no longer support by classifying them as end of life (EOL).

Network Security & Embedded Appliances

- **What security method could you use to allow only specific hosts to connect to a SOHO router/modem?**

- **ANSWER:**
  - You could configure a whitelist of permitted Media Access Control (MAC) addresses.

Network Security & Embedded Appliances

- **A user wants to be able to access an FTP server installed on a computer on their home network from the Internet. The home network is connected to the Internet by a DSL router. How would you enable access?**

- **ANSWER:**
    - Configure port forwarding on the router to send incoming connections on port 21 to the LAN computer.

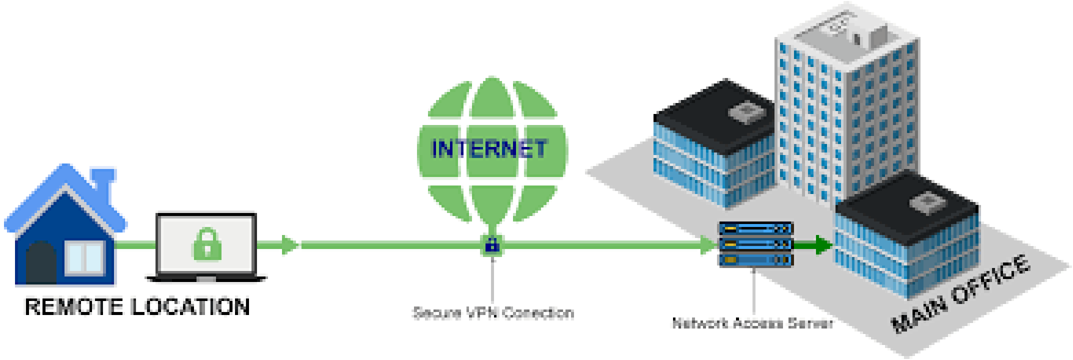
CompTIA

Network Security & Embedded Appliances

- **What option on the General tab of the Internet Options dialog box is most relevant to user privacy?**

- **ANSWER:**
  - Delete browsing history.

Topic D: Configure Remote Access



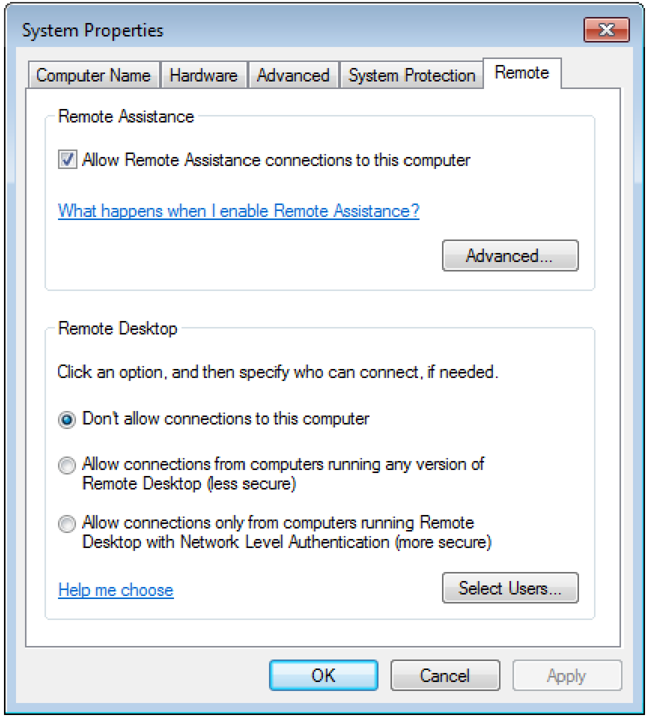
Windows Remote Access Tools

Microsoft's protocol for operating remote GUI connections to a Windows machine.

[illegible]

Tool	Description
Remote Desktop	• 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	• 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



System Properties

Remote Assistance

☑ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Remote Desktop

Click an option, and then specify who can connect, if needed.

● Don't allow connections to this computer

○ Allow connections from computers running any version of Remote Desktop (less secure)

○ Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)

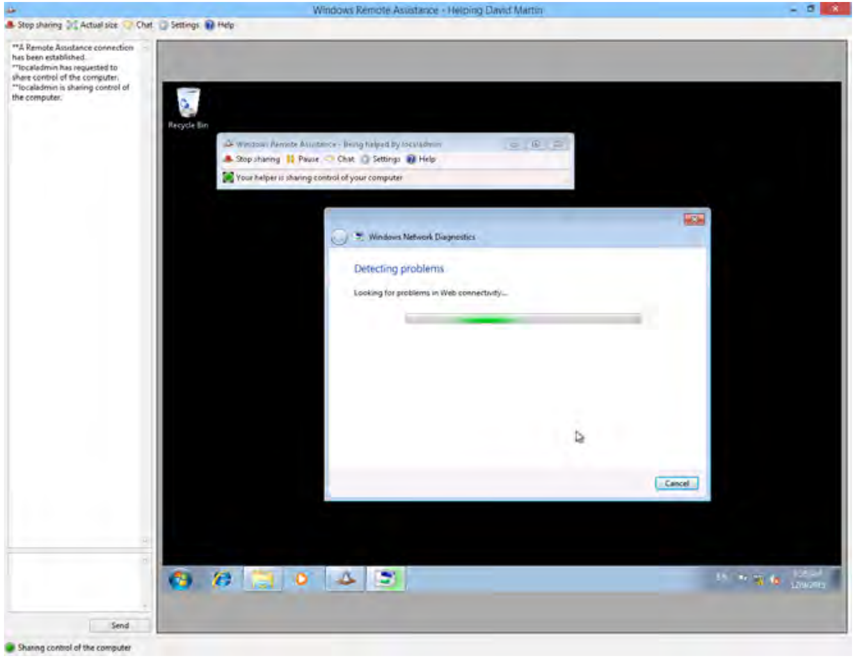
Help me choose

- Remote Assistance allowed by default; **Remote Desktop is not**
- Configure in System Properties/Remote Settings
- 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 (RDP restricted admin mode)
- Remote Credential Guard mitigate this risk.

The Remote Assistance Process



Windows Remote Assistance - Helping David Martin
Stop sharing
Actual size
Chat
Settings
Help
Recycle Bin
Windows Remote Assistance - Being helped by localadmin
Stop sharing
Pause
Chat
Settings
Help
Windows Network Diagnostics
Cancel
Send

**A Remote Assistance connection has been established.
**localadmin has requested to share control of the computer.
**localadmin is sharing control of the computer.

Your helper is sharing control of your computer

Detecting problems

Looking for problems in Web connectivity...

Sharing control of the computer

- 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

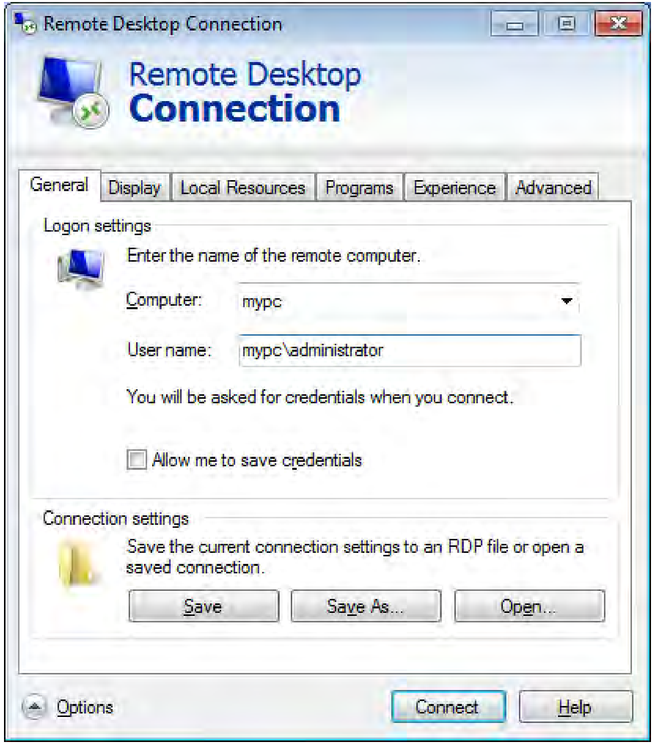
Open via the Communications menu in Accessories or by typing mstsc at a command prompt.

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.



Enter the name of the remote computer.

Computer: mypc

User name: mypc\administrator

You will be asked for credentials when you connect.

☐ Allow me to save credentials

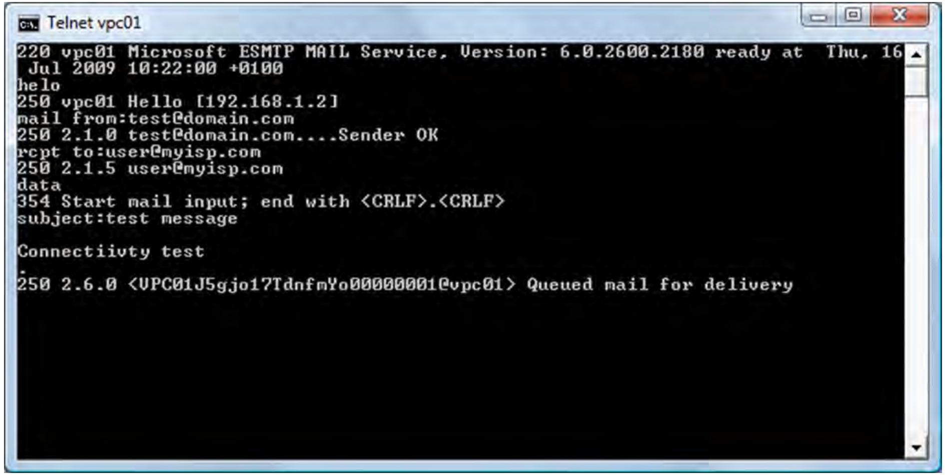
Save the current connection settings to an RDP file or open a saved connection.

Remote Access Technologies

- RDP Microsoft's protocol for operating remote GUI
- connections to a Windows machine.
- 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



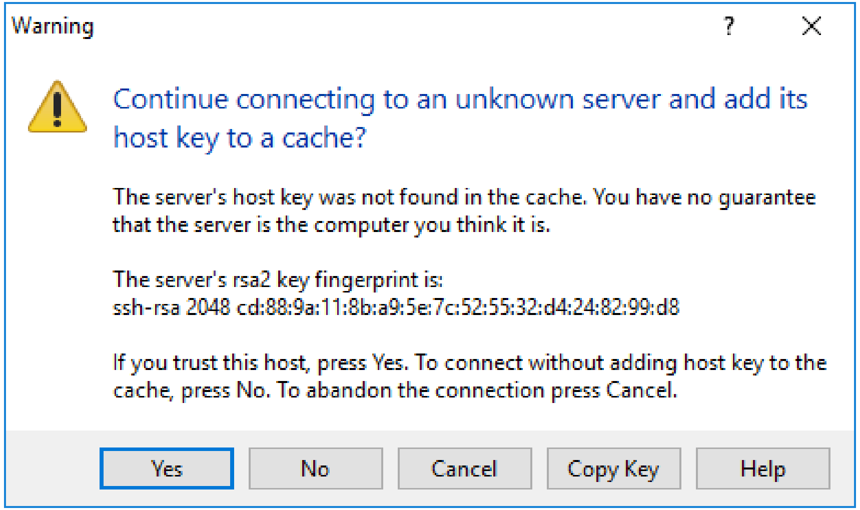
```
220 vpc01 Microsoft ESMTP MAIL Service, Version: 6.0.2600.2180 ready at  Thu, 16
 Jul 2009 10:22:00 +0100
helo
250 vpc01 Hello [192.168.1.2]
mail from:test@domain.com
250 2.1.0 test@domain.com....Sender OK
rcpt to:user@myisp.com
250 2.1.5 user@myisp.com
data
354 Start mail input; end with <CRLF>.<CRLF>
subject:test message

Connectiivty test
.
250 2.6.0 <VPC01J5gjo17TdnfmYo00000001@vpc01> Queued mail for delivery
```

- Telnet is both a protocol and a terminal emulation software tool that transmits shell commands in and output between a client and the remote host.

- A Telnet server
- listens on port TCP/23 by default.

SSH

- SSH: The principal means of obtaining secure remote access to
- UNIX and Linux servers and to most types of network appliances (switches, routers, and firewalls).
- Replaces unsecure administration and file copy programs (Telnet, FTP)
- SSH can be used for SFTP and to achieve many other network configurations.
- Uses TCP port 22, Encrypts each session
- SSH servers identified by public/private key pairs



Continue connecting to an unknown server and add its host key to a cache?

The server's host key was not found in the cache. You have no guarantee that the server is the computer you think it is.

The server's rsa2 key fingerprint is:
ssh-rsa 2048 cd:88:9a:11:8b:a9:5e:7c:52:55:32:d4:24:82:99:d8

If you trust this host, press Yes. To connect without adding host key to the cache, press No. To abandon the connection press Cancel.

SSH

- 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

- **Which edition(s) of Windows support connecting to the local machine over Remote Desktop?**

- **ANSWER:**
  - The Remote Desktop server functionality is available in Professional, Enterprise, and Ultimate editions.

Discussing Remote Access Configuration

- **What is the goal of RDP Restricted Admin (RDPRA) Mode and Remote Credential Guard?**

- **ANSWER:**
  - If the local machine is compromised, malware may be able to obtain the credentials of a user account connecting to the machine over Remote Desktop. RDPRA Mode and Remote Credential Guard are designed to mitigate this risk.

Discussing Remote Access Configuration

- **True or false? SSH is not available for use with Windows.**

- **ANSWER:**
  - False. Support for an SSH client and server is being included in feature updates to Windows 10, and there are numerous commercial and open source products.

Discussing Remote Access Configuration

- **How can you confirm that you are connecting to a legitimate SSH server?**

- **ANSWER:**
  - The server displays its host key on connection. You need to keep a record of valid host keys and compare the key presented by the server to the record you have.

Topic E: Troubleshoot Network Connections

Common Wired Network Connectivity Issues

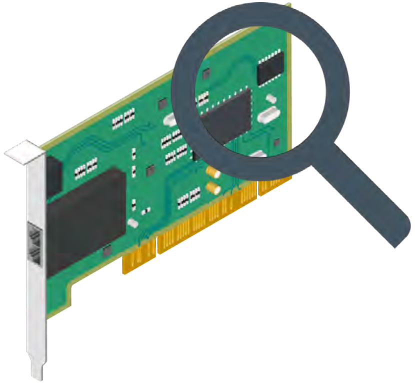
Identify the problem

- NIC port > Patch Cord > Wall Port > Structured Cable > Patch Panel > Switch Port
- Complete loss of connectivity or intermittent loss of connectivity

- Verify patch cords using known good examples or cable tester
- Verify network ports using a loopback adapter
- Verify permanent link using a cable tester
- Verify switch interface configuration or consider updating NIC driver

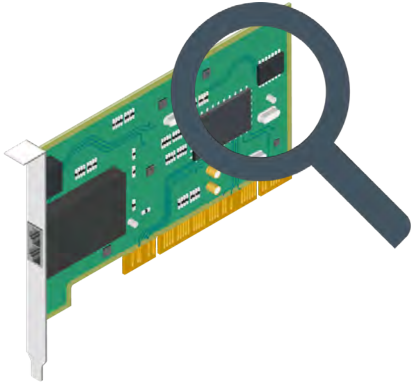
Common Wired Network Connectivity Issues

- 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 Wired Network Connectivity Issues

- 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 Wireless Network Connectivity Issues

- 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

- Signal issues:
  - Channel interference
  - Signal blocking

Common Wireless Network Connectivity Issues

Poor ~~VoIP quality~~ voice Over ip

- High speed and low latency

– Real-time applications are demanding

- Check the Internet connection

– A speed test can identify slow links

- Verify the local networking equipment

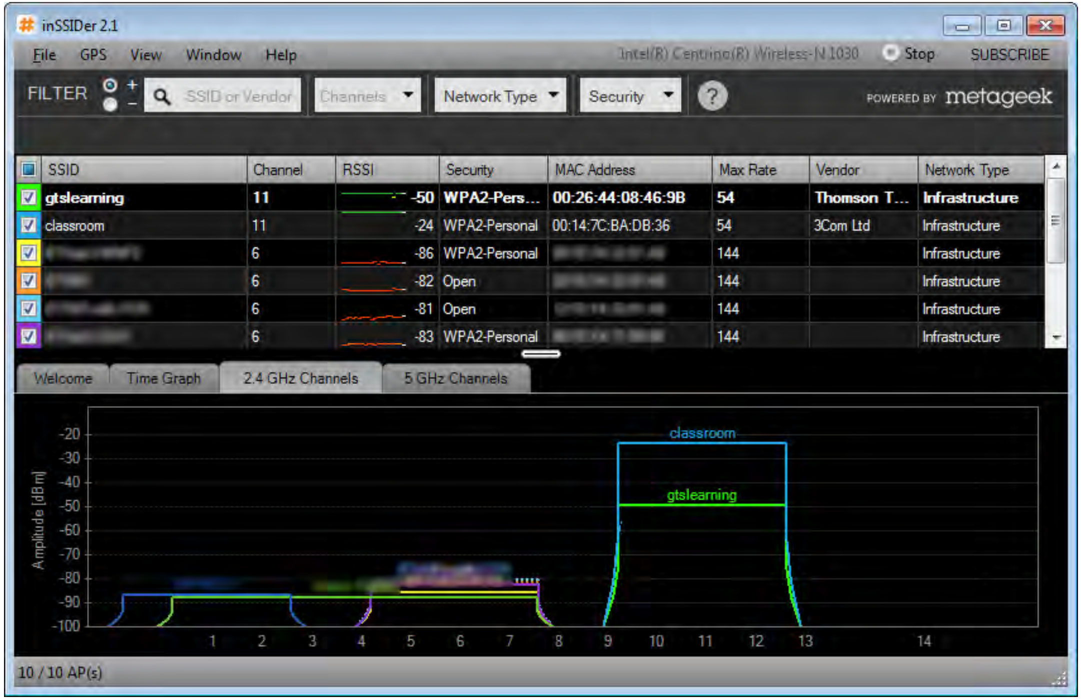
– An old router can cause significant problems

- View the network performance

– A packet capture would be useful

Common Wireless Network Connectivity Issues

- Use Wi-Fi analyzer
- Site survey can:
  - Identify sources of interference problems
  - Measure signal strength
  - Identify congested channels



☑ SSID	Channel	RSSI	Security	MAC Address	Max Rate	Vendor	Network Type
☑ **gtslearning**	**11**	**-50**	**WPA2-Pers...**	**00:26:44:08:46:9B**	**54**	**Thomson T...**	**Infrastructure**
☑ classroom	11	-24	WPA2-Personal	00:14:7C:BA:DB:36	54	3Com Ltd	Infrastructure
☑ [redacted]	6	-86	WPA2-Personal	[redacted]	144		Infrastructure
☑ [redacted]	6	-82	Open	[redacted]	144		Infrastructure
☑ [redacted]	6	-81	Open	[redacted]	144		Infrastructure
☑ [redacted]	6	-83	WPA2-Personal	[redacted]	144		Infrastructure

10 / 10 AP(s)

Troubleshooting Troubleshoot Port Flapping Issues

- Port flapping: Is intermittent connectivity

  Causes:

  - Bad cabling
  - External interference
  - A faulty NIC at the host

- You can use the switch configuration interface to report how long a port remains in the up state.

Troubleshooting Network Connections

- Windows includes several utilities you can use to troubleshoot networking problems:
  - ping
  - ipconfig
  - nslookup
  - tracert
  - Two net commands
  - netstat

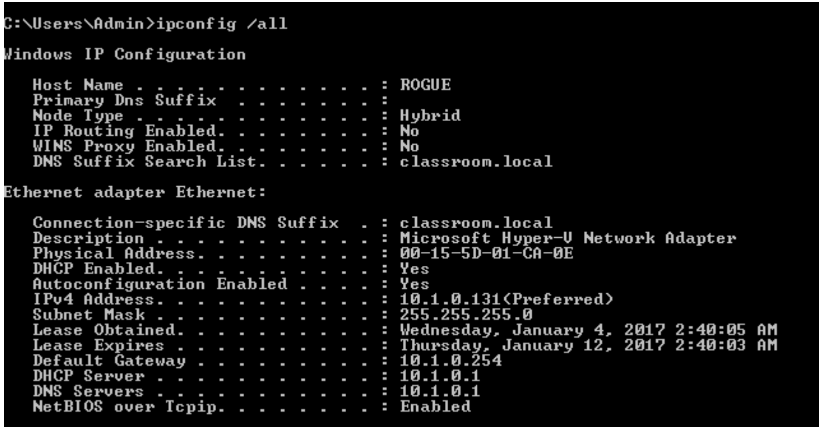
1

IP Configuration Issues

- If host IP configuration is incorrect it will not be able to communicate
- Use ipconfig at command line
- Typical switches:
  - /all
  - /release
  - /renew
  - /displaydns
  - /flushdns

IP Configuration Issues

important



```
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-V 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
```

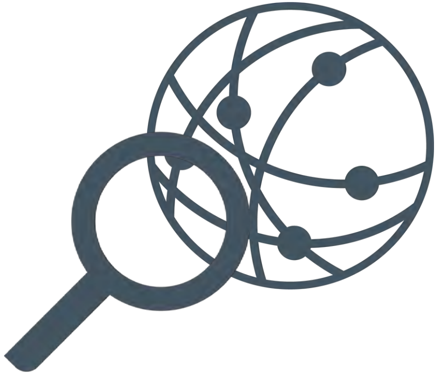
- Use ipconfig to test adapter configuration:
  - Static or DHCP? If DHCP, correct parameters?
- If configuration is correct, check for:
  - Communication with DHCP server
  - Configuration with DHCP server
  - Multiple conflicting DHCP servers
- On Linux, use ifconfig; some different functionality

CompTIA

IP Connectivity Issues

link ip check

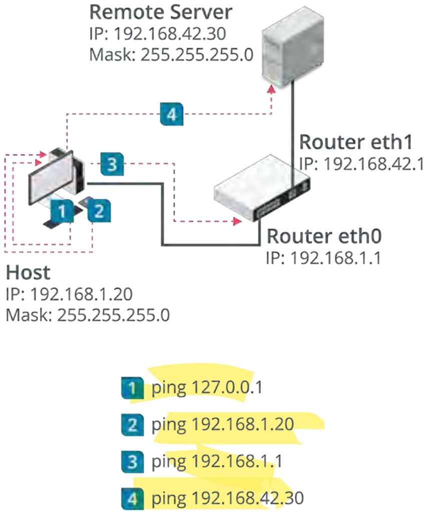
- If link and IP are correct, problem may be in network topology.
- Test connections by trying to use resources (but doesn't eliminate application fault).
- Use other connectivity tests:
  - Ping
  - DNS testing
  - IP conflict



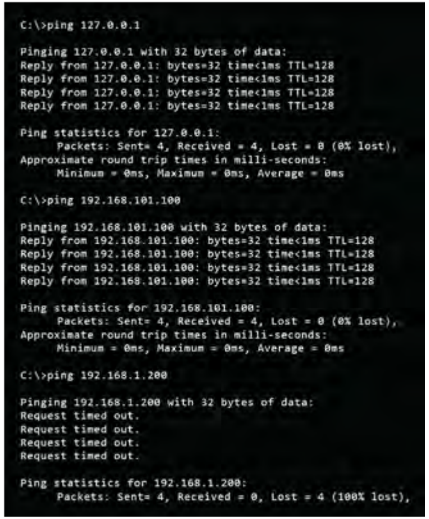
CompTIA

IP Connectivity Issues

Important



1 ping 127.0.0.1
2 ping 192.168.1.20
3 ping 192.168.1.1
4 ping 192.168.42.30



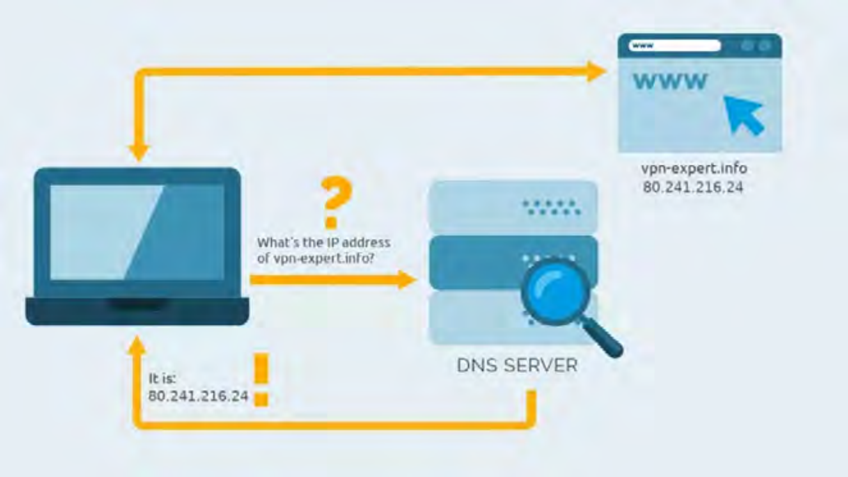
```
C:\>ping 127.0.0.1

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(**127.0.0.1**), workstation, default gateway, remote host.
- If successful, reply with time in milliseconds.
- If unsuccessful:
  - Destination unreachable
  - No reply (request timed out)

CompTIA

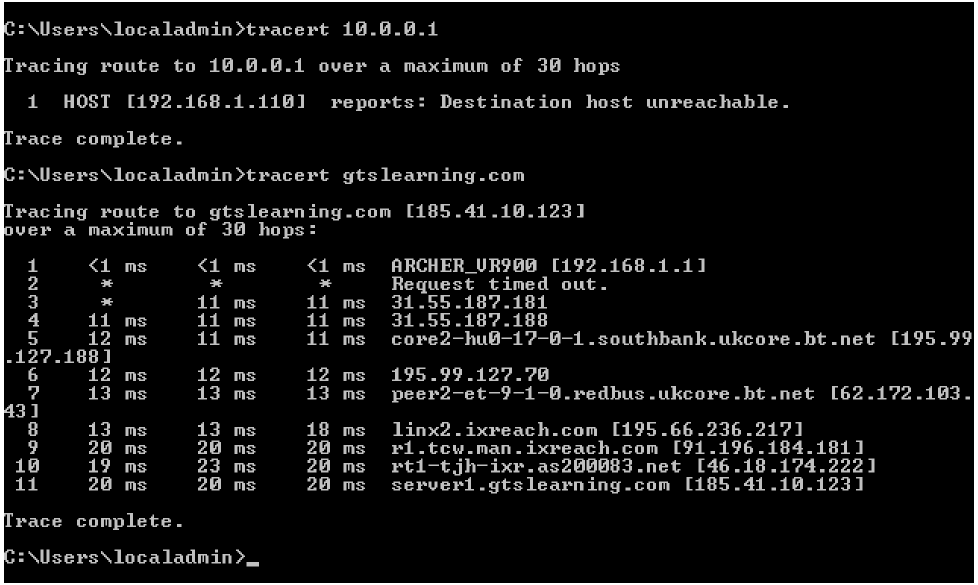
IP Connectivity Issues

- 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 would time out if host not located
- It will list:
  - Router hops
  - Ingress interface
  - Response time
  - Asterisk if no response



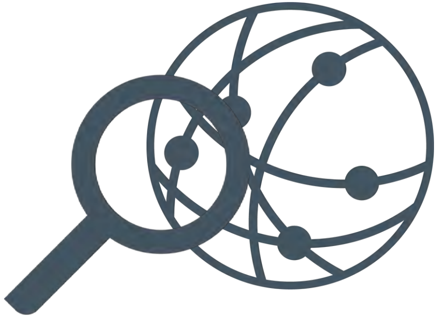
```
C:\Users\localadmin>tracert 10.0.0.1

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_VR900 [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

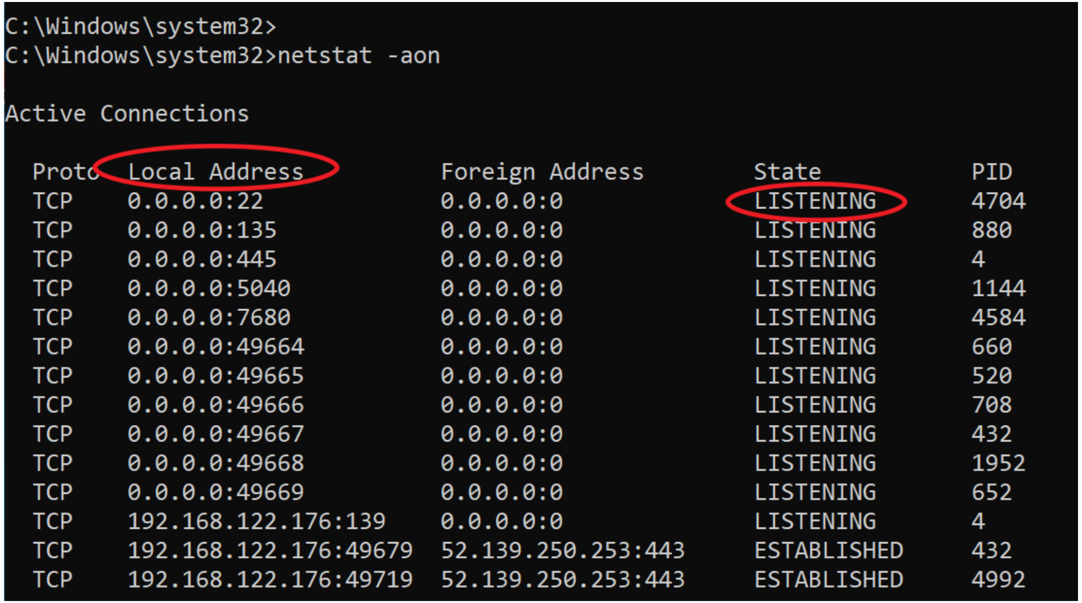


Unavailable Resources

Use netstat to investigate open ports and connections

Use –a, -b, -n switches

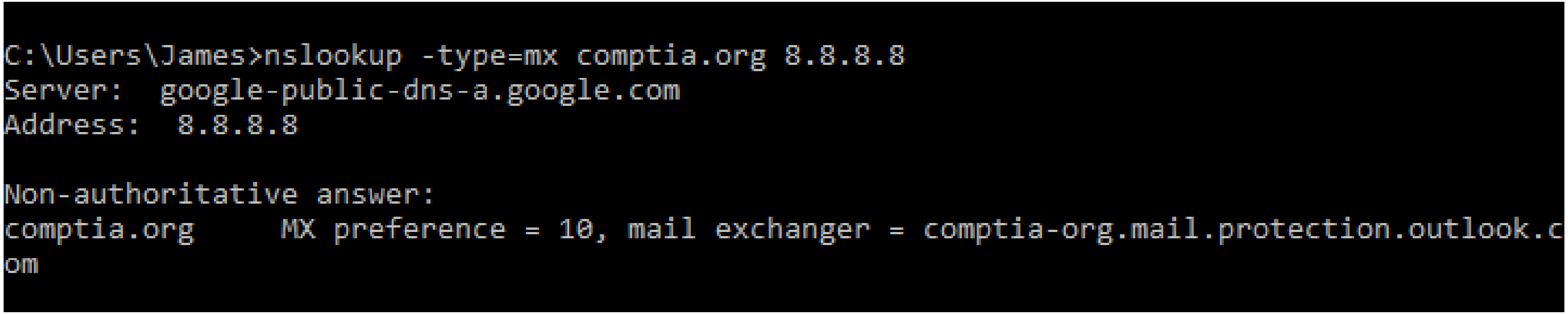
Linux has slightly different utility



```
C:\Windows\system32>
C:\Windows\system32>netstat -aon

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:22             0.0.0.0:0              LISTENING       4704
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       880
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       1144
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       4584
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       660
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       520
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       708
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       432
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       1952
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       652
  TCP    192.168.122.176:139    0.0.0.0:0              LISTENING       4
  TCP    192.168.122.176:49679  52.139.250.253:443     ESTABLISHED     432
  TCP    192.168.122.176:49719  52.139.250.253:443     ESTABLISHED     4992
```

Unavailable Resources

- 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
```

Discussing Network Connection Troubleshooting

- **What readings would you expect to gather with a Wi-Fi analyzer?**

- **ANSWER:**
  - The signal strength
  - Channels within range of the analyzer.

CompTIA

Discussing Network Connection Troubleshooting

- **You have restarted the DHCP server following a network problem. What command would you use to refresh the IP configuration on Windows 10 client workstations?**

- **ANSWER:**
  - `ipconfig /renew`

Discussing Network Connection Troubleshooting

- **What command can you use on a Linux computer to report the IP configuration?**

- **ANSWER:**
  - `ifconfig` tool.
  - The `ip` command is now preferred.

Discussing Network Connection Troubleshooting

- **You are trying to add a computer to a wireless network but cannot detect the access point. What would you suspect the problem to be?**

- **ANSWER:**
    - The computer's wireless adapter is not supported by the AP, the computer is not in range, or there is some sort of interference.

CompTIA

Discussing Network Connection Troubleshooting

- **A single PC on a network cannot connect to the Internet. Where would you start troubleshooting?**

- **ANSWER:**
  - You could test the PC's IP configuration, specifically the default gateway or name resolution, or you could check that the cable is good.

Discussing Network Connection Troubleshooting

- **What Windows tool is used to test the end-to-end path between two IP hosts on different IP networks?**

- **ANSWER:**
  - `tracert`

Discussing Network Connection Troubleshooting

- **A computer cannot connect to the network. The machine is configured to obtain a TCP/IP configuration automatically. You use ipconfig to determine the IP address and it returns 0.0.0.0. What does this tell you?**

- **ANSWER:**
  - If a DHCP server cannot be contacted, the machine should default to using an APIPA address (169.254.x.y).
  - As it has not done this, something is wrong with the networking software installed on the machine (probably the DHCP client service, TCP/IP stack, or registry configuration, to be specific).

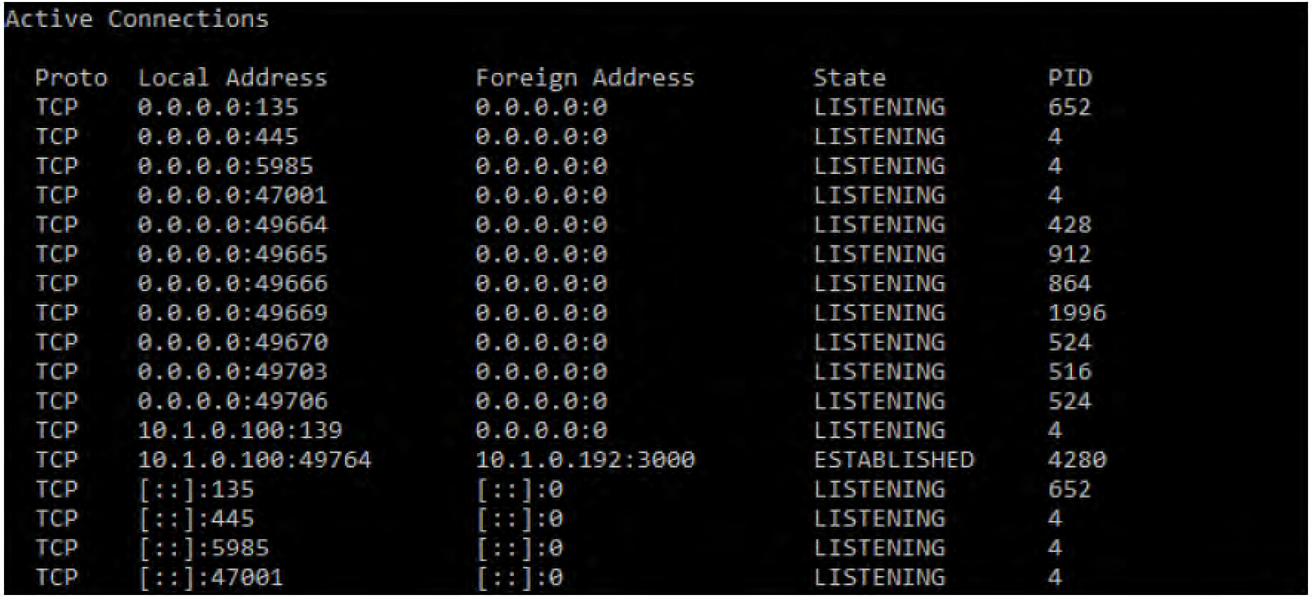
Discussing Network Connection Troubleshooting

- **If a host has a firewall configured to block outgoing ICMP traffic, what result would you expect from pinging the host (assuming that the path to the host is otherwise OK)?**

- **ANSWER:**
  - Destination unreachable.

Discussing Network Connection Troubleshooting

- **Which command produces the output shown in this graphic?** ***(slide 1 of 2)***

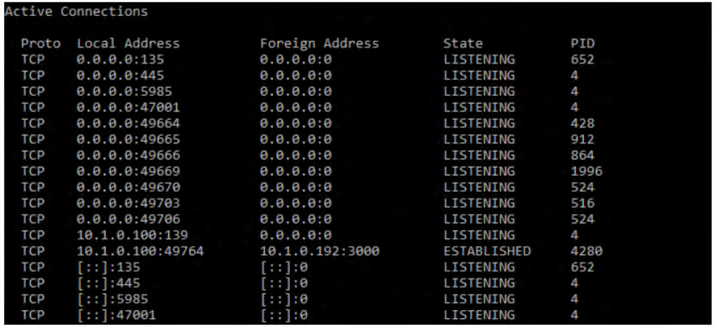


```
Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       652
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       428
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       912
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       864
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       1996
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       524
  TCP    0.0.0.0:49703          0.0.0.0:0              LISTENING       516
  TCP    0.0.0.0:49706          0.0.0.0:0              LISTENING       524
  TCP    10.1.0.100:139         0.0.0.0:0              LISTENING       4
  TCP    10.1.0.100:49764       10.1.0.192:3000        ESTABLISHED     4280
  TCP    [::]:135               [::]:0                 LISTENING       652
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:5985              [::]:0                 LISTENING       4
  TCP    [::]:47001             [::]:0                 LISTENING       4
```

Discussing Network Connection Troubleshooting

- **Which command produces the output shown in this graphic?** *(slide 2 of 2)*

- **ANSWER:**
  - This is output from `netstat`. Specifically, it is `netstat -ano`. The switches show all connections, with ports in numeric format, and the PID of the process that opened the port.



```
Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       652
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5985           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       428
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       912
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       864
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       1996
  TCP    0.0.0.0:49670          0.0.0.0:0              LISTENING       524
  TCP    0.0.0.0:49703          0.0.0.0:0              LISTENING       516
  TCP    0.0.0.0:49706          0.0.0.0:0              LISTENING       524
  TCP    10.1.0.100:139         0.0.0.0:0              LISTENING       4
  TCP    10.1.0.100:49764       10.1.0.192:3000        ESTABLISHED     4280
  TCP    [::]:135               [::]:0                 LISTENING       652
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:5985              [::]:0                 LISTENING       4
  TCP    [::]:47001             [::]:0                 LISTENING       4
```

Topic F: Install and Configure IoT Devices

Internet of Things

Is used to describe the global network of Smart Devices:

- Wearable technology
- Home appliances
- Home control systems

- Devices can communicate and pass data between devices.

- “Things” identified with unique numbers/codes.

IoT Wireless Networking Technologies

Technology	Description
Bluetooth Low Energy	• 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	• 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	• 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	• 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 (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 can combine (Z-Wave, Zigbee, Wi-Fi, Bluetooth, NFC)

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

- **What type of network topology is used by protocols such as Zigbee and ZWave?**

- **ANSWER:**
  - A wireless mesh network topology.

Discussing IoT Devices

- **What are the two main options for operating smart devices?**

- **ANSWER:**
  - Using a smartphone/tablet app, or using a voice-enabled smart speaker. Some devices might also support configuration via a web app.

Discussing IoT Devices

- **True or false? Voice processing by a smart speaker is performed internally so these devices can be used without an Internet connection.**

- **ANSWER:**
  - False. The speaker passes the voice data to a backend server for processing.