Module 6

Windows Networking

Objectives

1. 1.6 Setup and configure Windows networking

NETWORKING

WorkGroup vs. Domain

1. Computers on home networks are usually part of a workgroup and computers on workplace networks are usually part of a domain.
2. **Workgroup**:
   1. Peer-to-Peer network
   2. All computers are peers; no computer has control over another computer
   3. Must have an account on every computer to login
   4. There are typically no more than twenty computers
   5. A workgroup is not protected by a password
   6. All computers must be on the same local network or subnet
3. **Domain**:
   1. Client/Server network
   2. One or more computers are servers, used to control the security and permissions for all computers on the domain
   3. Domain users must provide a password or other credentials each time they access the domain
   4. If you have a user account on the domain, you can log on to any computer on the domain without needing an account on that computer
   5. There can be thousands of computers in a domain
   6. The computers can be on different local networks

Network Shares

1. Once a drive or folder you share and assign permissions for access, it can be accessed by:
   A. Shared Drives
      - Must be opened each time you access it using the Run command or Network window
   B. Map Drives
      - Appears as a local disk on your PC
      - `\\servername\usershare`

Network Connections

1. Network Connections provide connectivity between your computer and the Internet, a network, or another computer. With Network Connections, you can configure settings to reach local or remote network resources or functions.
2. Things to consider:
   - A. When using multiple network adapters, rename each local area connection
   - B. Verify required connection settings for your network adapter
   - C. Create dial-up, VPN, or direct connections by using the New Connection wizard
   - D. Specify the order in which network providers and protocols are accessed
   - E. Only install and enable the network protocols that you need

Network Connections

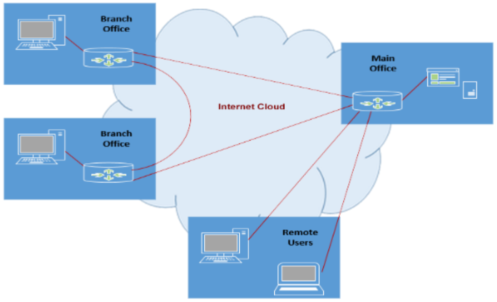
1. The network connections settings specify how your computer will connect to a network. To manage your network connections:
   A. Click Start, Control Panel, Network and Sharing Center, Change Adaptor Settings (on left) to display the Network Connections window.
2. In the Network Connections window, you can perform any of the following network management tasks:
   A. Disable a network connection
   B. Enable a previously disabled network connection
   C. Repair a network connection.
   D. Configure your Internet Protocol (IP) settings

Network Connections

1. To configure your IP settings
   A. Right-click the network connection, and then click Properties
   B. Click Internet Protocol version 4 (TCP/IPv4), and then click Properties
   C. In the TCP/IPv4 Properties dialog box, configure your network settings, and then click OK
2. There are three pieces of information your computer must know in order to send packets over the Internet:
   A. IP address – a unique address that identifies the computer
   B. Subnet Mask – used to find the network address
   C. Default Gateway – the router interface your computer uses to access the Internet
   D. DNS (optional) – allows the computer to lookup IP addresses from a given name

Network Connections

1. A **virtual private network** (**VPN**) is a secure way of connecting to a private Local Area Network from a remote location, using the Internet or any insecure public network to transport the network data packets privately, using encryption.
2. VPNs are frequently used by remote workers or companies with remote offices to share private data and network resources.
3. The VPN uses authentication to permit/deny access to users, and encryption to prevent unauthorized users from reading the private network packets.
4. Creates a secure connection between two points.



Typical Business Network

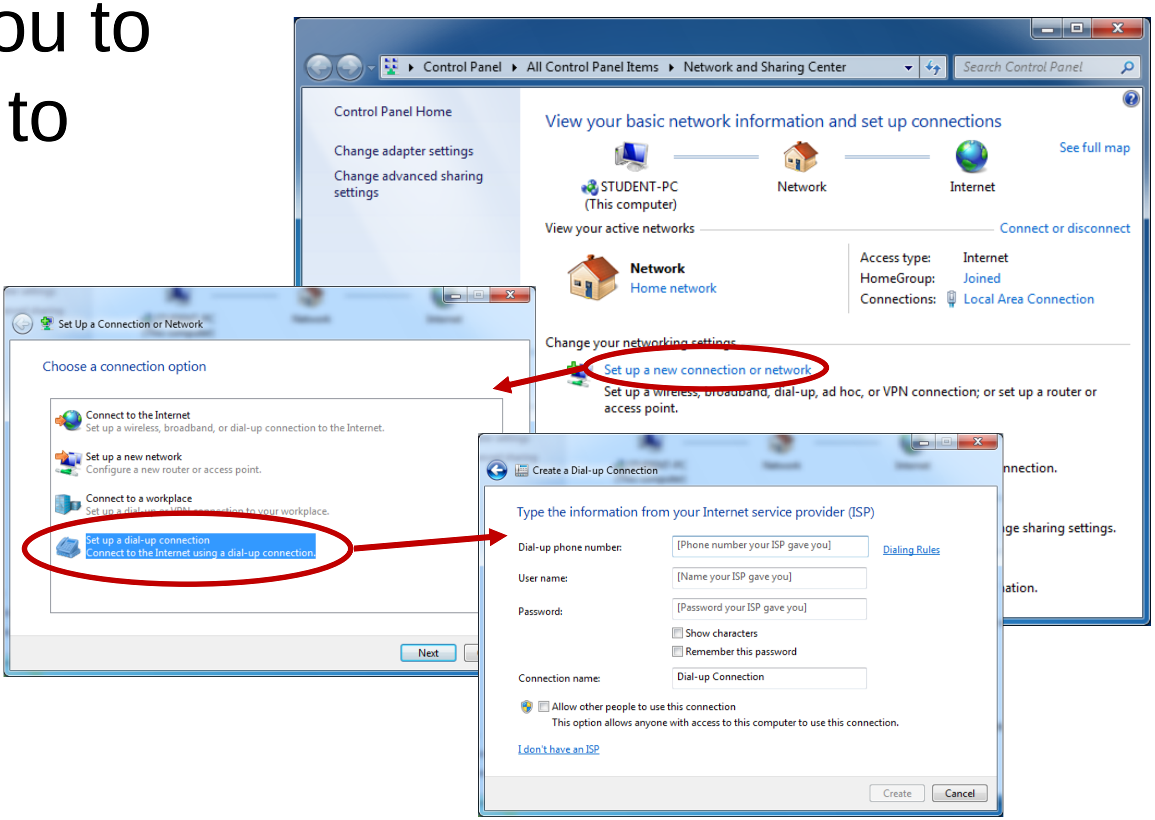
Remote access/Branch office

1. **DirectAccess** – provides intranet connectivity to client computers when they are connected to the Internet. Replaces VPNs with HTTPS.
2. **BranchCache** – copies content from a remote file or Web server and caches the content at branch office locations, allowing client computers at branch offices to access the content locally rather than over the WAN.

Remote Access

Network Connections

1. **Dialup** allows you to setup a modem to add network connectivity
2. Settings will be added to the network settings on the connections tab in Internet Options



Control Panel ▸ All Control Panel Items ▸ Network and Sharing Center

Search Control Panel

Control Panel Home

Change adapter settings

Change advanced sharing settings

View your basic network information and set up connections

See full map

STUDENT-PC (This computer) — Network — Internet

View your active networks

Connect or disconnect

Network
Home network

Access type: Internet
HomeGroup: Joined
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.

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.
- 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.

Create a Dial-up Connection

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

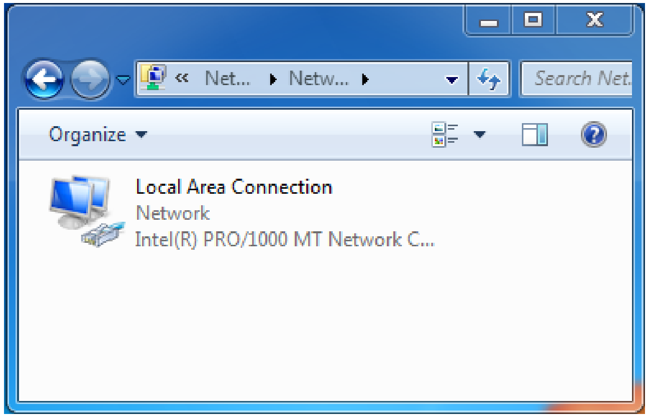
Connection name: Dial-up Connection

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

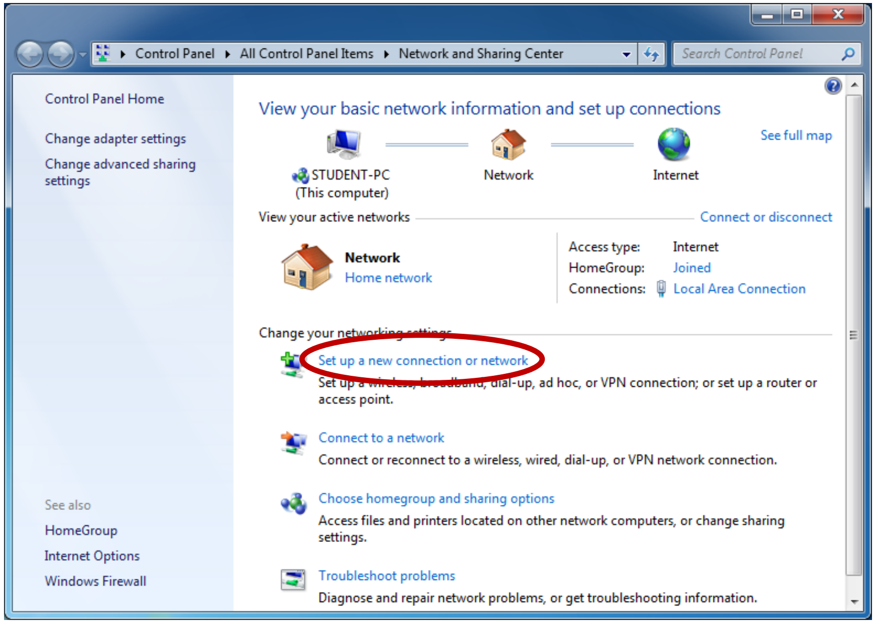
I don't have an ISP

Network Connections

1. **Wired** is the fastest and most secure network connection type
2. Requires a wired NIC



Local Area Connection
Network
Intel(R) PRO/1000 MT Network C...



View your basic network information and set up connections

View your active networks

Network
Home network

Access type: Internet
HomeGroup: Joined
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.

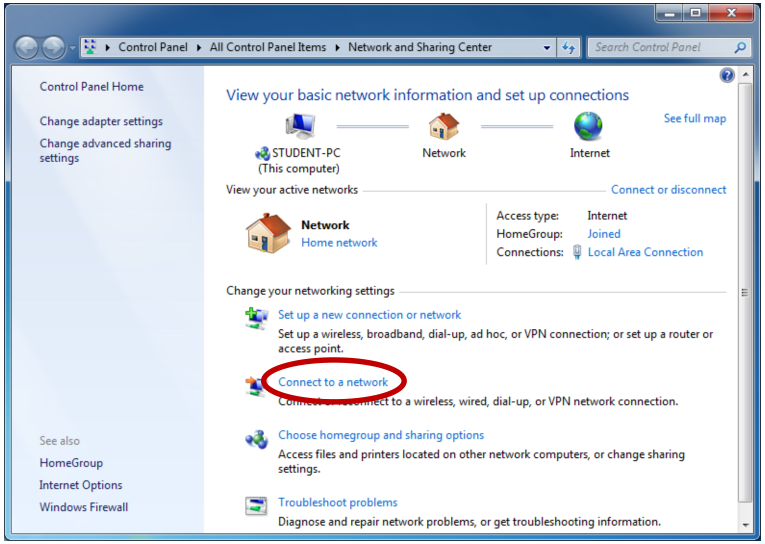
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

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

1. **Wireless** allows you to connect to any infrastructure network, WLAN, to access network resources and the Internet
2. You can use broadcasting SSIDs or hidden network if you know the right information



View your basic network information and set up connections

View your active networks — Connect or disconnect

Network
Home network

Access type: Internet
HomeGroup: Joined
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

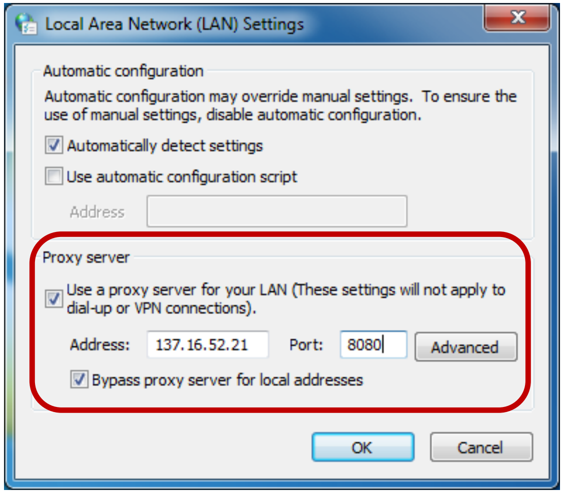
1. A **Wireless Wide Area Network** (**WWAN**) allows a user with a laptop and a WWAN card to surf the web, check email, or connect to a virtual private network (VPN) from anywhere within the regional boundaries of cellular service.
2. Uses mobile telecommunication cellular network technologies such as LTE, WiMAX, UMTS, CDMA, GSM, or cellular digital packet data (CDPD).
3. These technologies are provided by a wireless service provider.

Home vs. Work vs. Public Networks

1. The first time that you connect to a network, you must choose a network location. This automatically sets the appropriate firewall and security settings for the type of network that you connect to.
   A. **Home network** – for home networks or when you know and trust the people and devices on the network. Network discovery is turned on for home networks, which allows you to see other computers and devices on the network and allows other network users to see your computer.
   B. **Work network** – for small office or other workplace networks. Network discovery is turned on, which allows you to see other computers and devices on a network and allows other network users to see your computer.
   C. **Public network** – for networks in public places. This location is designed to keep your computer from being visible to other computers around you and to help protect your computer from any malicious software from the Internet. Choose this option if you're connected directly to the Internet without using a router, or if you have a mobile broadband connection.

Proxy Settings

1. A **proxy server** is a server that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity.
2. On the local computer, the proxy settings are located in Internet Options, Connections, LAN settings, Proxy settings. Enter the Proxy server's IP address and the port used.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings

□ Use automatic configuration script

Address:

Proxy server

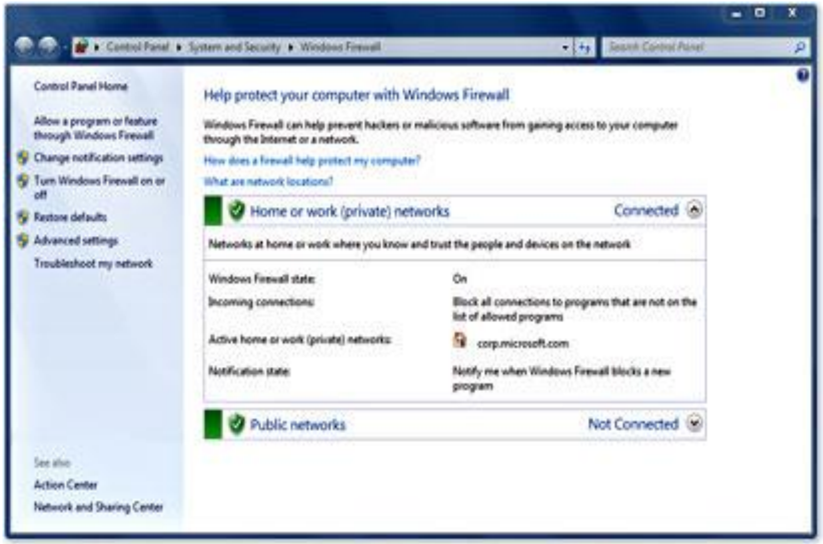
☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 137.16.52.21 Port: 8080

☑ Bypass proxy server for local addresses

Firewall Settings

1. A firewall can help prevent hackers or malicious software from gaining access to your computer through a network or the Internet
2. A firewall can also help stop your computer from sending malicious software to other computers



Control Panel ▸ System and Security ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state: On

Incoming connections: Block all connections to programs that are not on the list of allowed programs

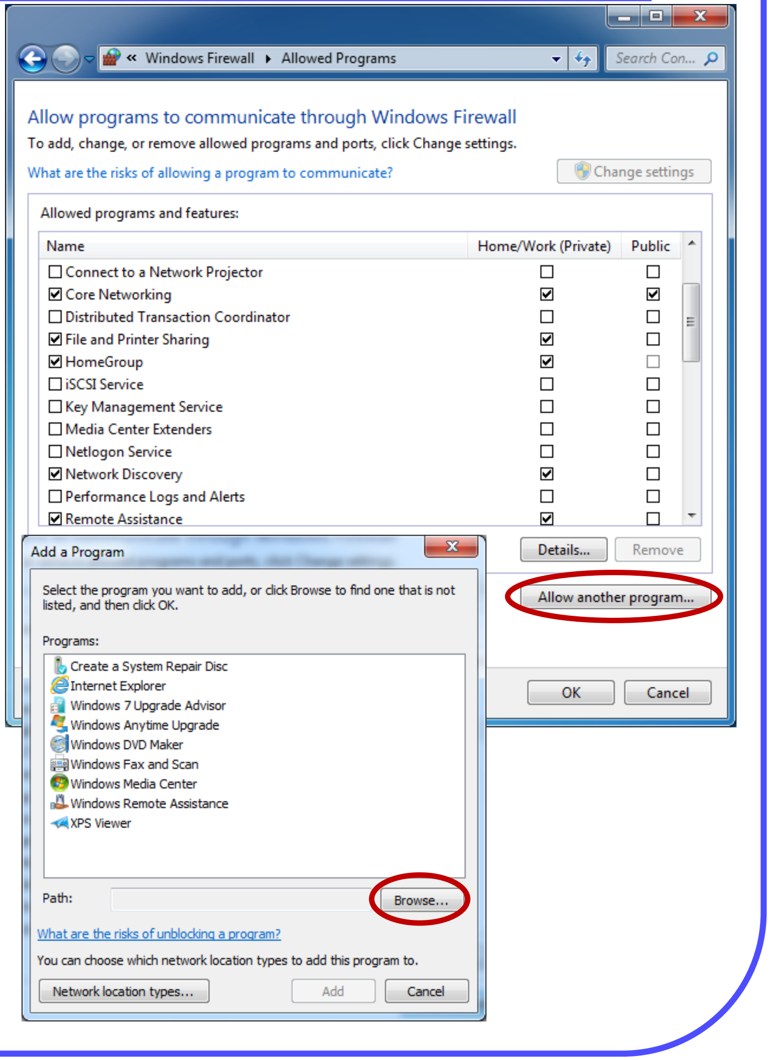
Active home or work (private) networks: corp.microsoft.com

Notification state: Notify me when Windows Firewall blocks a new program

Public networks — Not Connected

Firewall Settings

1. If Windows Firewall is blocking a program and you want to allow that program to communicate through the firewall, you can:
   A. Selecting the program in the list of allowed programs (also called the exceptions list)
   B. If the program isn't listed, you might need to open a port. For example, to play a multiplayer game with friends online, you might need to open a port for the game so that the firewall allows the game information to reach your computer. A port stays open all the time, so be sure to close ports that you don't need open anymore.



Allow programs to communicate through Windows Firewall

To add, change, or remove allowed programs and ports, click Change settings.

What are the risks of allowing a program to communicate?

Allowed programs and features:

Name	Home/Work (Private)	Public
☐ Connect to a Network Projector	☐	☐
☑ Core Networking	☑	☑
☐ Distributed Transaction Coordinator	☐	☐
☑ File and Printer Sharing	☑	☐
☑ HomeGroup	☑	☐
☐ iSCSI Service	☐	☐
☐ Key Management Service	☐	☐
☐ Media Center Extenders	☐	☐
☐ Netlogon Service	☐	☐
☑ Network Discovery	☑	☐
☐ Performance Logs and Alerts	☐	☐
☑ Remote Assistance	☑	☐

Add a Program

Select the program you want to add, or click Browse to find one that is not listed, and then click OK.

Programs:

- Create a System Repair Disc
- Internet Explorer
- Windows 7 Upgrade Advisor
- Windows Anytime Upgrade
- Windows DVD Maker
- Windows Fax and Scan
- Windows Media Center
- Windows Remote Assistance
- XPS Viewer

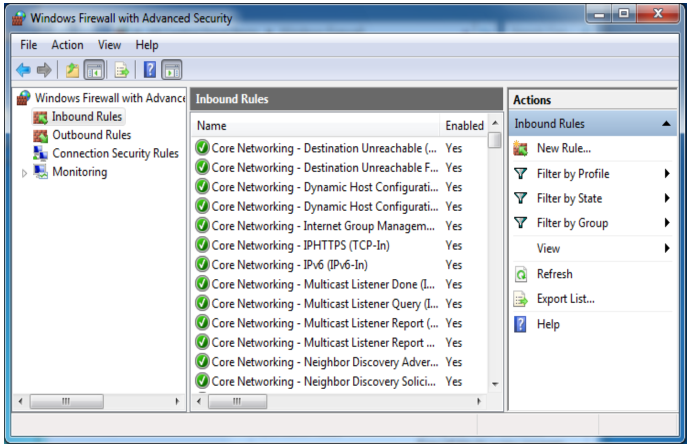
Path:

What are the risks of unblocking a program?

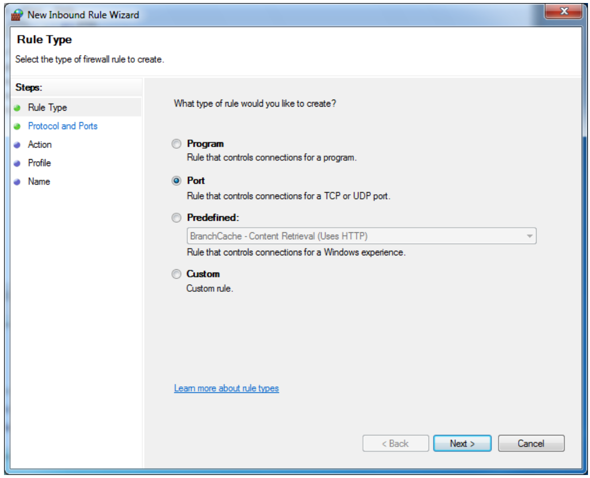
You can choose which network location types to add this program to.

Firewall Settings

1. To open a port:
   A. Open by clicking the Start button, Control Panel, Windows Firewall
   B. In the left pane, click Advanced settings
   C. In the left pane, click Inbound Rules
   D. In the right pane, click New Rule and follow the instructions



Name	Enabled
Core Networking - Destination Unreachable (...	Yes
Core Networking - Destination Unreachable F...	Yes
Core Networking - Dynamic Host Configurati...	Yes
Core Networking - Dynamic Host Configurati...	Yes
Core Networking - Internet Group Managem...	Yes
Core Networking - IPHTTPS (TCP-In)	Yes
Core Networking - IPv6 (IPv6-In)	Yes
Core Networking - Multicast Listener Done (I...	Yes
Core Networking - Multicast Listener Query (I...	Yes
Core Networking - Multicast Listener Report (...	Yes
Core Networking - Multicast Listener Report ...	Yes
Core Networking - Neighbor Discovery Adver...	Yes
Core Networking - Neighbor Discovery Solici...	Yes



Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

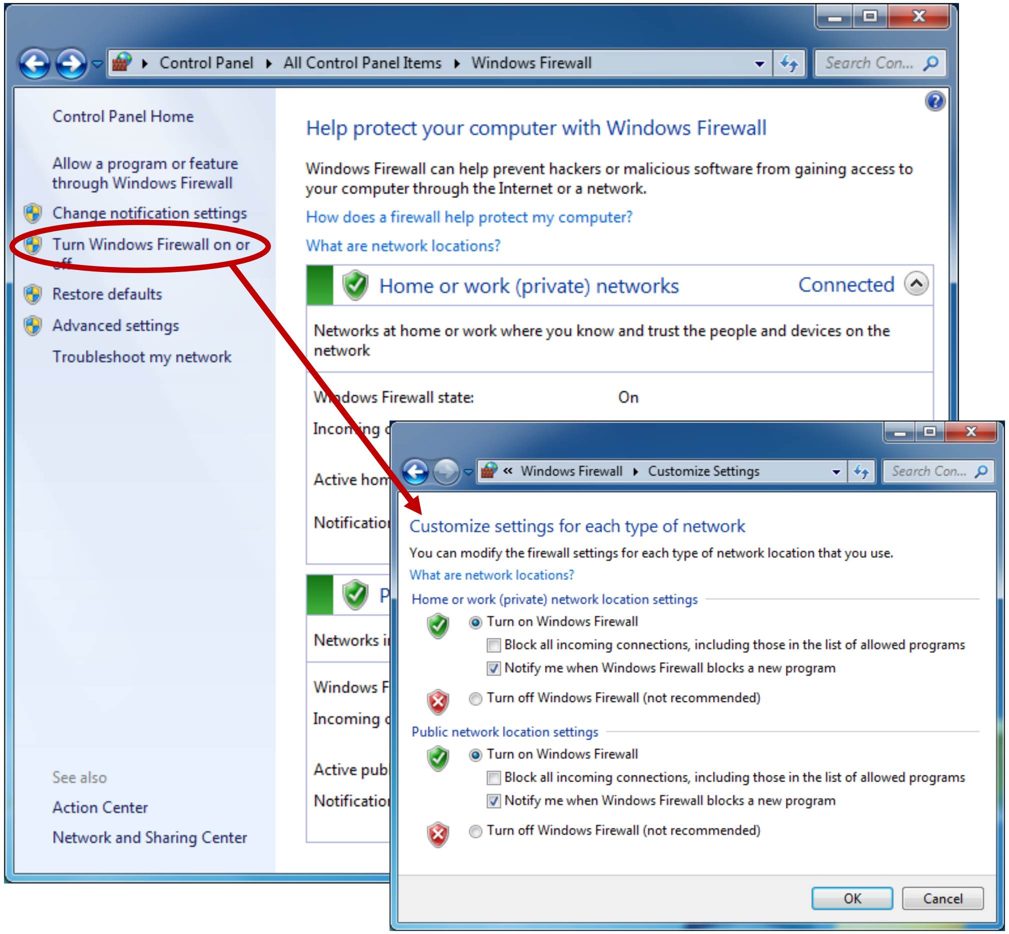
● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Firewall Settings

1. Enable/Disable
2. Private or Public



Control Panel ▸ All Control Panel Items ▸ Windows Firewall
Search Con...
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Network and Sharing Center

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Home or work (private) networks — Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state: On

Incoming c

Active hom

Notificatio

P

Networks i

Windows F

Incoming c

Active pub

Notificatio

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)

Network Card Settings

1. A network interface card (NIC) is used to connect a computer to a network or Internet. Common settings:
   A. Duplex – half or full
   B. Speed – 10, 100, 1000 Mbps
   C. Wake-on-LAN – is an Ethernet networking standard that allows a computer to be turned on or awakened remotely
   D. Quality of Service (QoS) – specifies a guaranteed level of delivery including: availability, bandwidth, delay, and error rate.

HomeGroup

1. Connect two or more PCs running Windows 7 on the same network to automatically start sharing printers, media and document libraries
2. You can join a **homegroup** in any edition of Windows 7, but you can only create one in Windows 7 Home Premium, Professional, Ultimate, or Enterprise editions

Summary

In this Module we discussed:

1. Workgroups
2. Domains
3. Network Shares
4. Network connections
5. IP addressing
6. VPNs
7. Types of networks
8. Proxy settings
9. Firewall settings
10. HomeGroups

Glossary and Terms

- **Network** – Two or more devices connected together to share data.
- **Workgroup** – Creates a peer-to-peer network.
- **Peer-to-peer** – No computer has control over another computer.
- **Domain** – Creates a Client/Server network.
- **Client/Server** – One or more computers are servers that are used to control the security and permissions for all computers on the domain.
- **VPN** – Virtual Private Network
- **Protocol** – A set of rules that networked device use to communicate.
- **UNC** – Universal Naming Convention

Glossary and Terms

- **IP address** – A unique Dotted Decimal address that identifies a computer on a network or Internet.
- **Subnet Mask** – Dotted Decimal number that is used to find the network address.
- **Default Gateway** – The router interface your computer uses to access the Internet.
- **DNS** – Domain Name Service allows a computer to lookup IP addresses from a given name.
- **WAN** – Wide Area Network
- **LAN** – Local Area Network
- **WLAN** – Wireless Local Area Network
- **WWAN** – Wireless Wide Area Network

Glossary and Terms

- **LTE** – Long Term Evolution
- **WiMAX** – Worldwide Interoperability for Microwave Access
- **UMTS** – Universal Mobile Telecommunications System
- **CDMA** – Code Division Multiple Access
- **GSM** – Global System for Mobile
- **CDPD** - Cellular Digital Packet Data
- **NIC** – Network Interface Card
- **QoS** - Quality of Service