APPLIED NETWORKING

Chapter 8

8.1 Computer to Network Connection

Understand how to connect computer to network and tools.

8.1.1 Networking Cards

A wired or wireless network interface card (NIC) is required to connect to the network. Modern network adapter cards are connect via USB.

Objective

8.1 Computer to Network Connection

8.2 ISP Connection Technologies

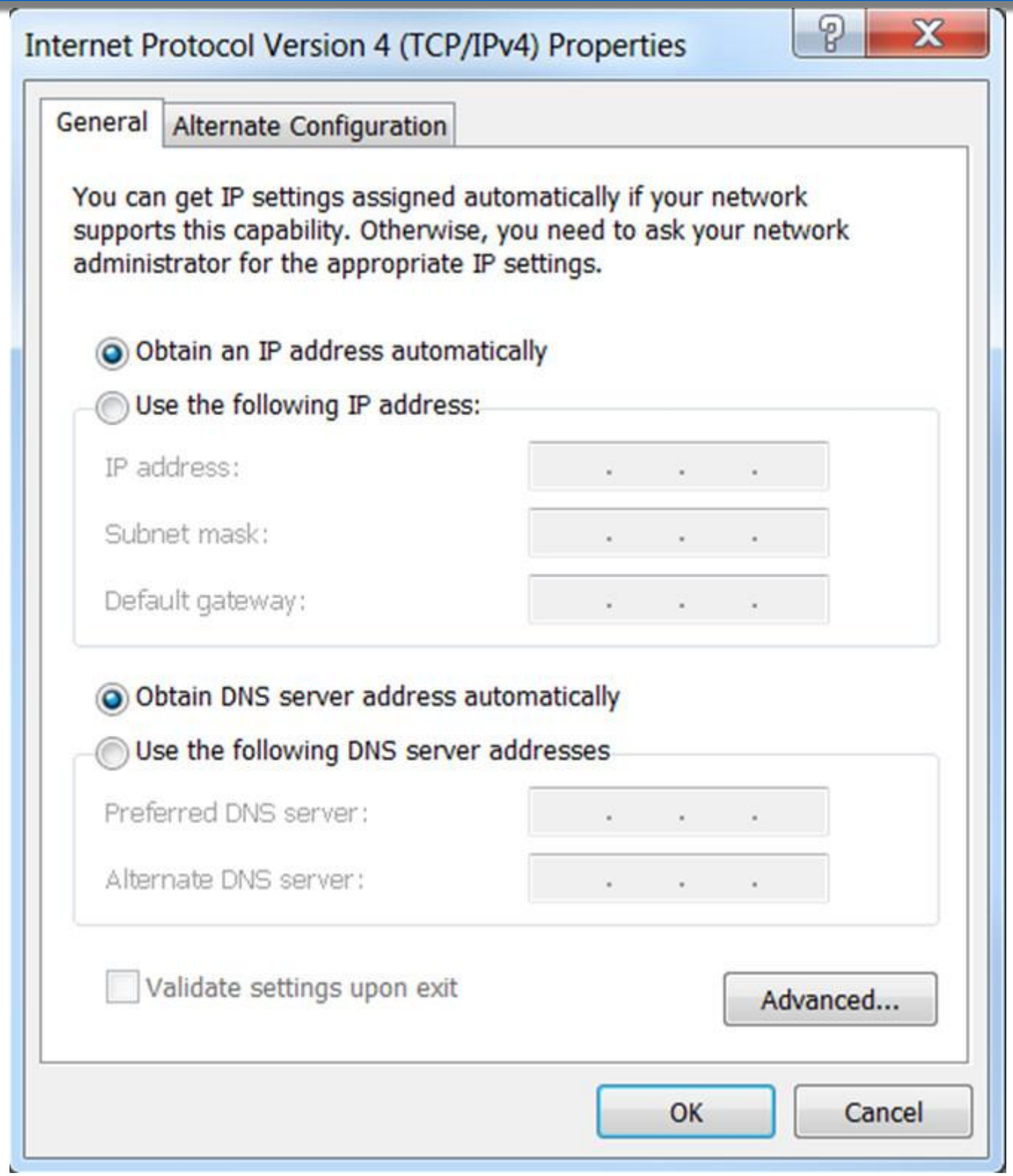
8.3 Internet Technologies

8.4 Common Preventive Maintenance

8.5 Basic Troubleshooting Process for Networks

After it is installed, IP settings must be configured either manually or dynamically.

You can also configure advanced settings, such as speed, duplex, Wake on LAN, and quality of service (QoS).



8.1.2 Wireless and Wired Router Configurations

To connect to a network, attach a straight-through Ethernet cable to the NIC port.

The other end connects to a router or to a telecommunications port that is wired so that data will reach the router.

For wireless connections, configure the router with the following:

- Network Mode (set the 802.11 standard)
- Network Name (SSID)
- Channel (important when there are multiple APs in the network)
- Wireless Security (should be WPA2)

8.1.3 Network Sharing

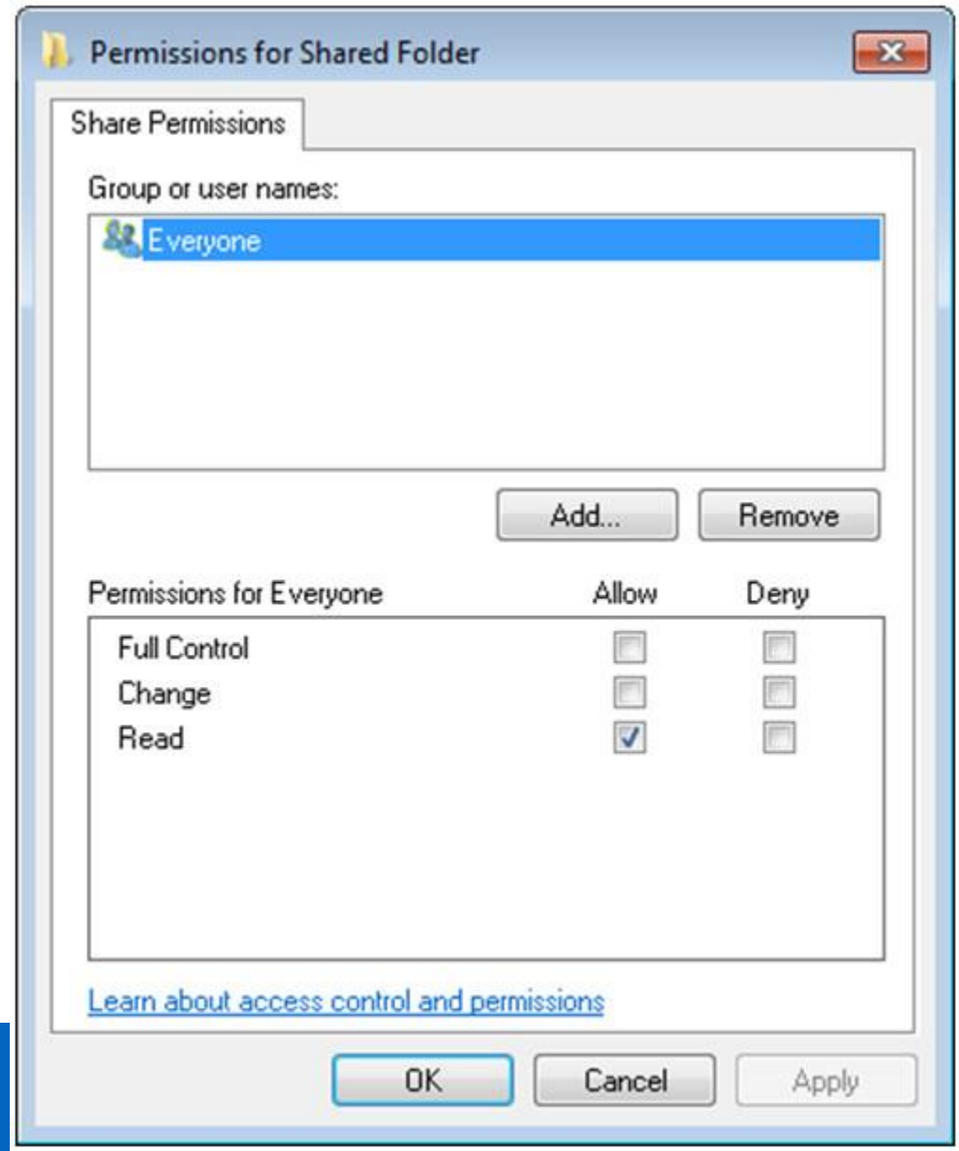
All Windows computers on a network must be part of either a domain or a workgroup.

Before computers can share resources, they must **share** the same domain name or workgroup name.

Mapping a local drive is a useful way to access a single file, specific folders, or an entire drive between different operating systems over a network.

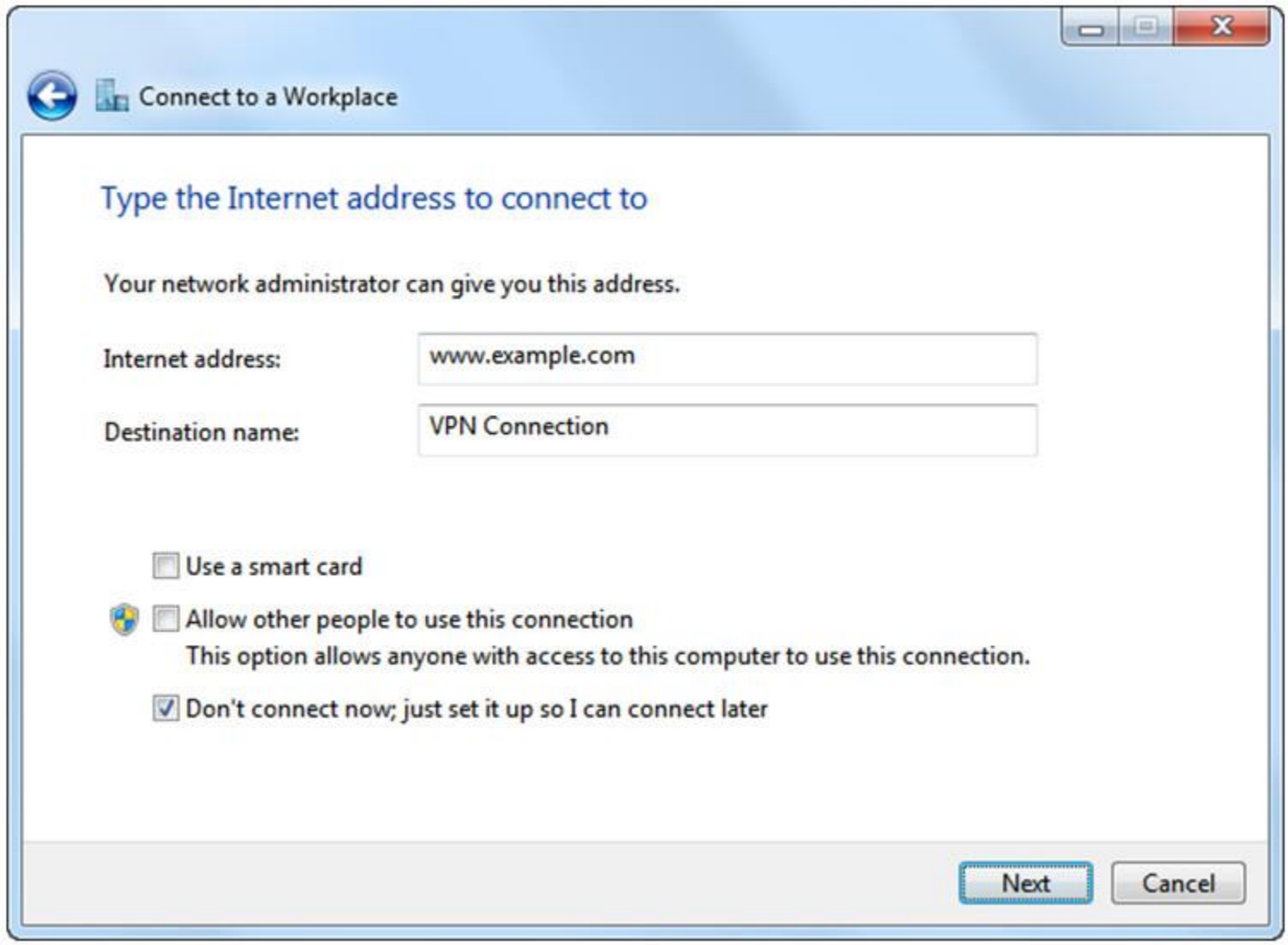
Determine which resources will be shared over the network and the type of permissions users will have to the resources.

- **Read** – user can view data in files and run programs
- **Change** – user can add files and subfolders, change the data in files, and delete subfolders and files
- **Full Control** – user can change permissions of files and folders



8.1.4 Remote Connections

A virtual private network (**VPN**) is a private network that connects remote sites or users together over a public network, like the Internet.

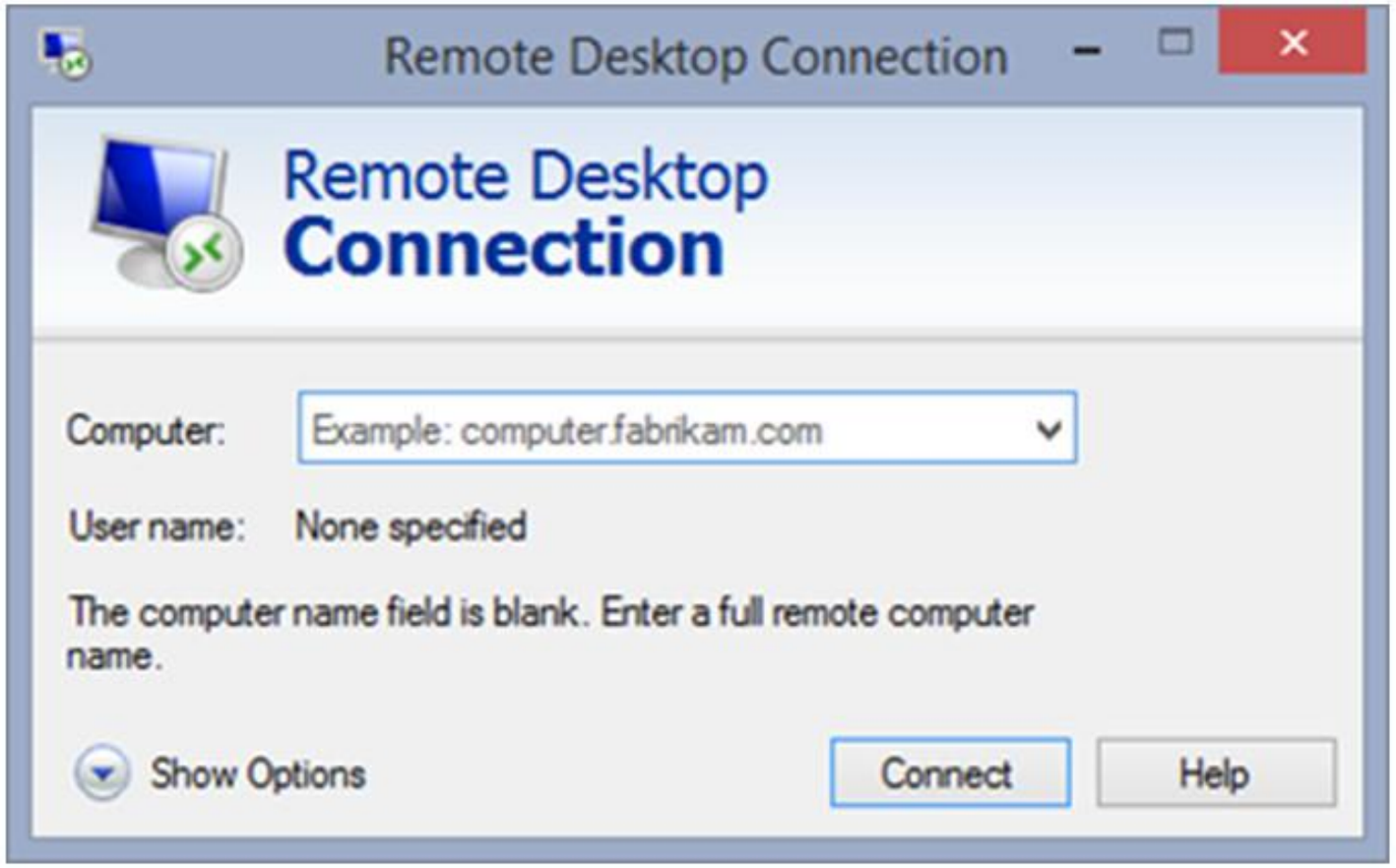


When connected to the corporate private network, users become part of that network and have access to all services and resources as if they were physically connected to the corporate LAN.

Remote-access users must install the VPN client on their computers to form a secure connection with the corporate private network.

Remote Desktop allows technicians to view and control a computer from a remote location.

Remote Assistance allows technicians to assist customers with problems from a remote location.

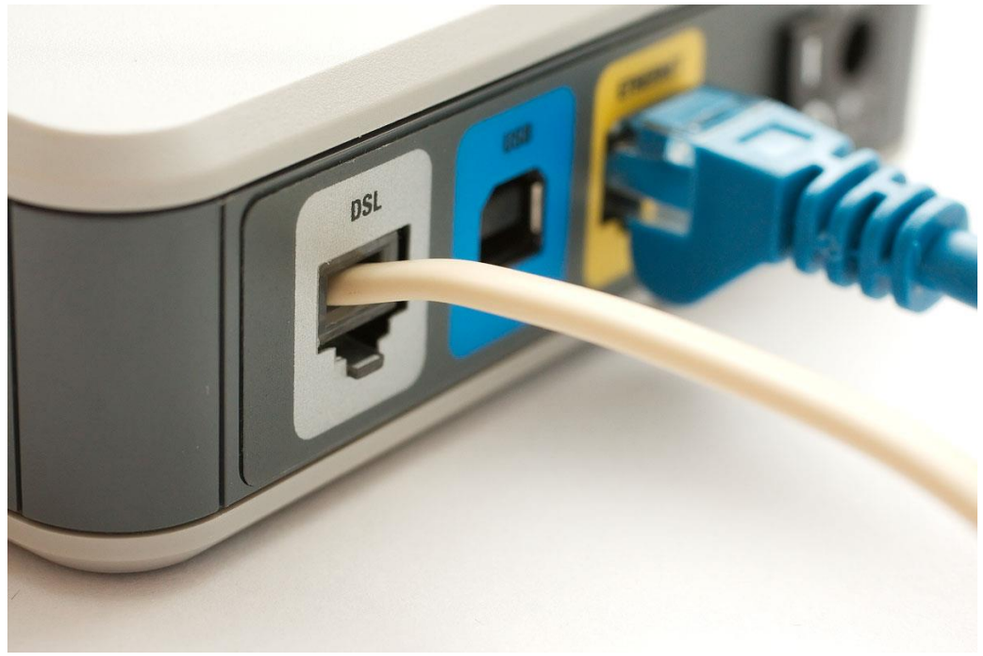


8.2 ISP Connection Technologies

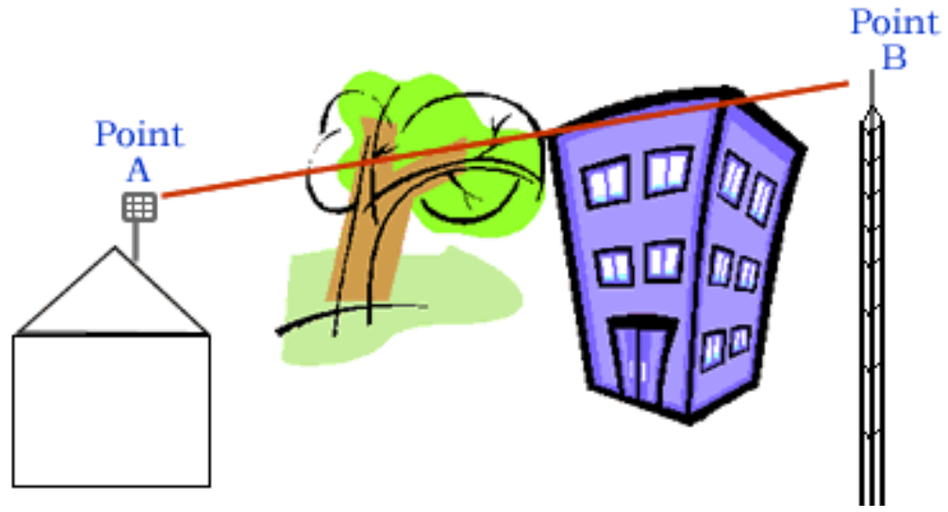
ISP = Internet Service Provider

8.2.1 Broadband Technologies

- **DSL** (Digital Subscriber Line) uses the existing copper telephone lines to provide high-speed digital data communication between end users and telephone companies.



- **Line of sight wireless** Internet is an always-on service that uses radio signals for transmitting Internet access

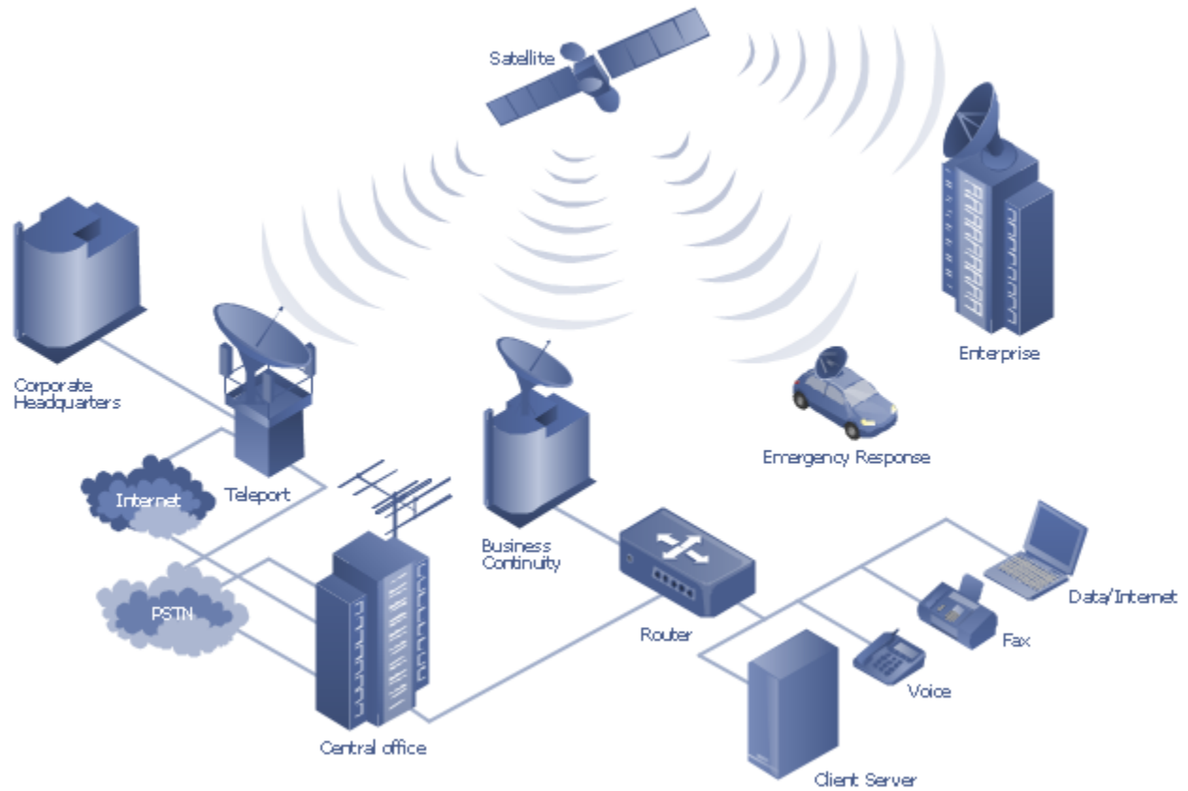


- **Cellular** technology enables the transfer of voice, video, and data.

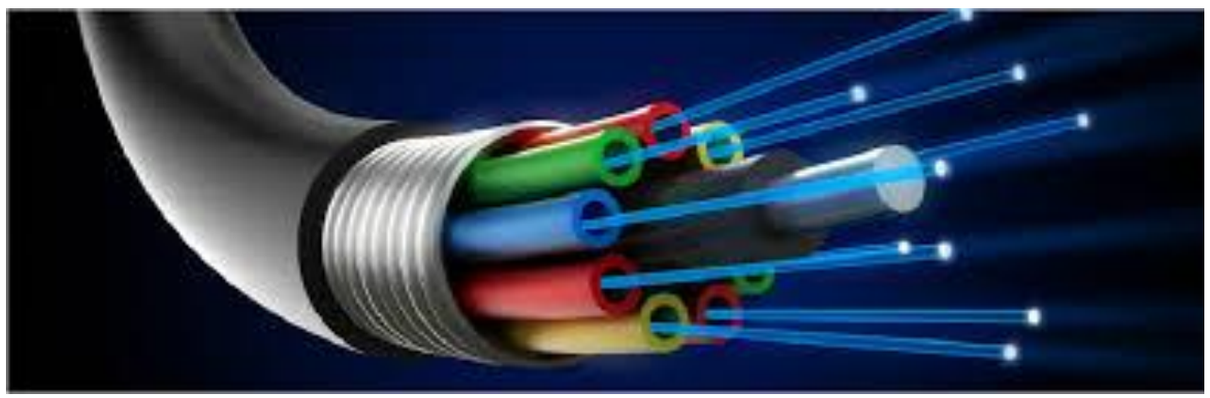
1G	2G	3G	4G	5G
1981	1992	2001	2010	2020(?)
2 Kbps	64 Kbps	2 Mbps	100 Mbps	10 Gbps
asic voice service sing analog rotocols	Designed primarily for voice using the digital standards (GSM/CDMA)	First mobile broadband utilizing IP protocols (WCDMA / CDMA2000)	True mobile broadband on a unified standard (LTE)	'Tactile Internet' with service-awar devices and fiber- like speeds

- **Cable** uses coaxial cable lines originally designed to carry cable television.

- **Satellite** is an alternative for customers who cannot get cable or DSL connections.



- **Fiber** broadband provides faster connection speeds and bandwidth than cable and DSL.



8.3 Internet Technologies

8.3.1 Data Centers and Cloud Computing

Data center is a data storage and processing facility run by an in-house IT department or leased offsite.

Cloud computing is an off-premise service that offers on-demand access to a shared pool of configurable computing resources.

The three main **Cloud services** models are:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

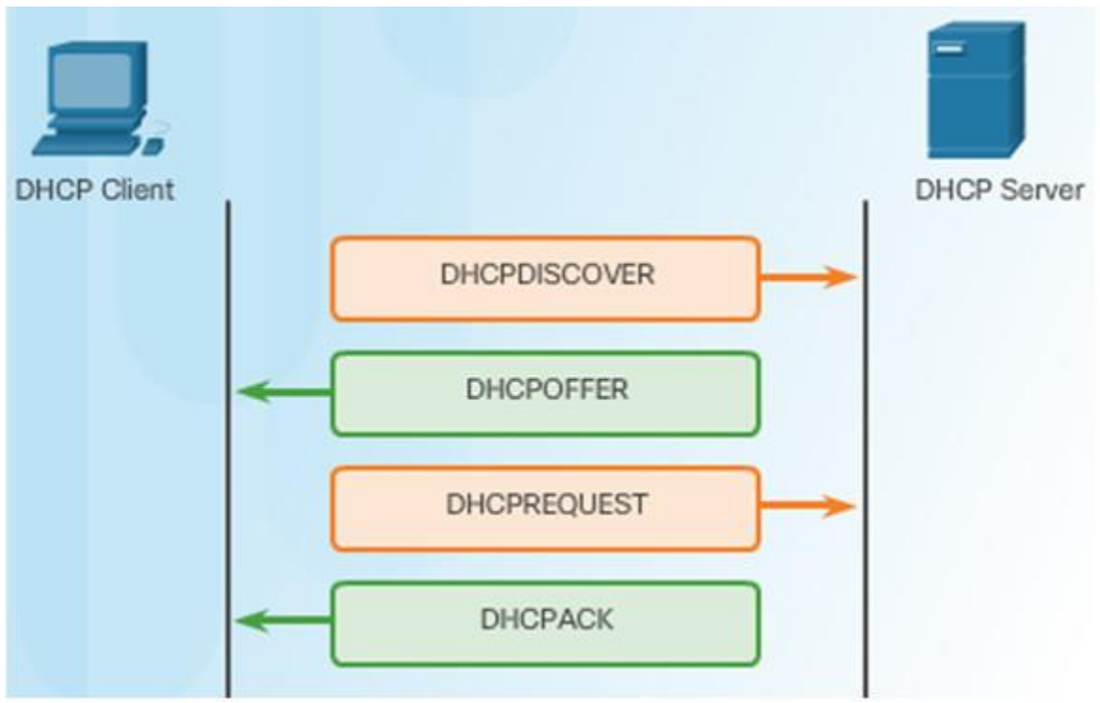
The four Cloud deployment models are:

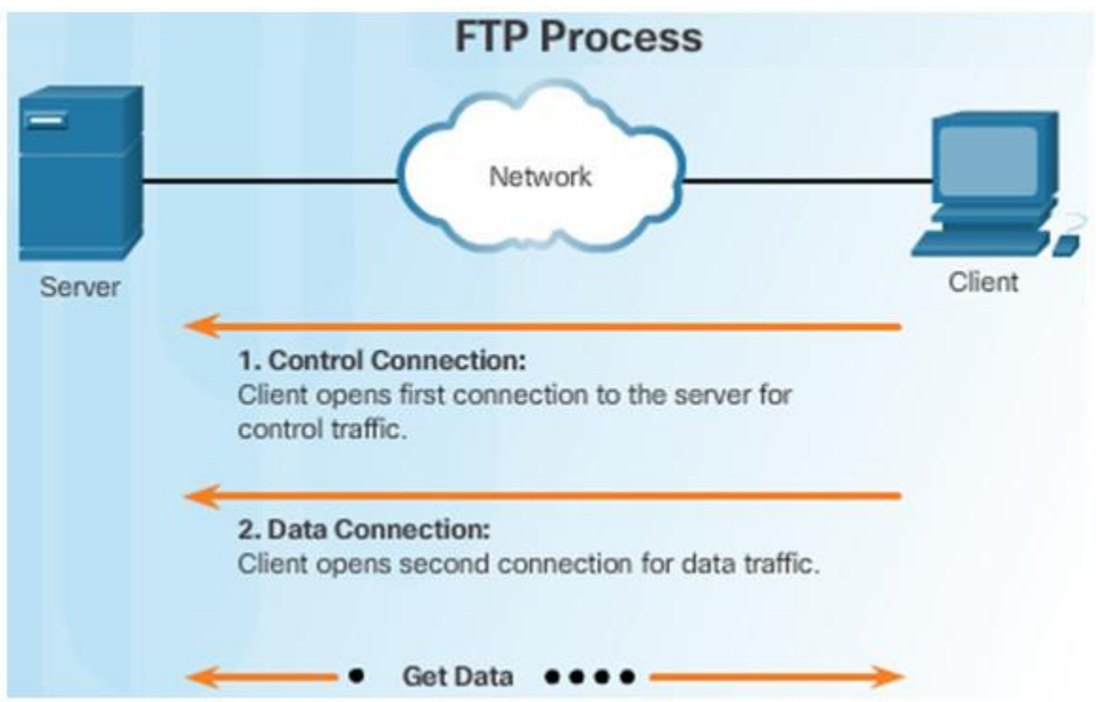
- Private
- Public
- Community
- Hybrid

8.3.2 Networked Host Services

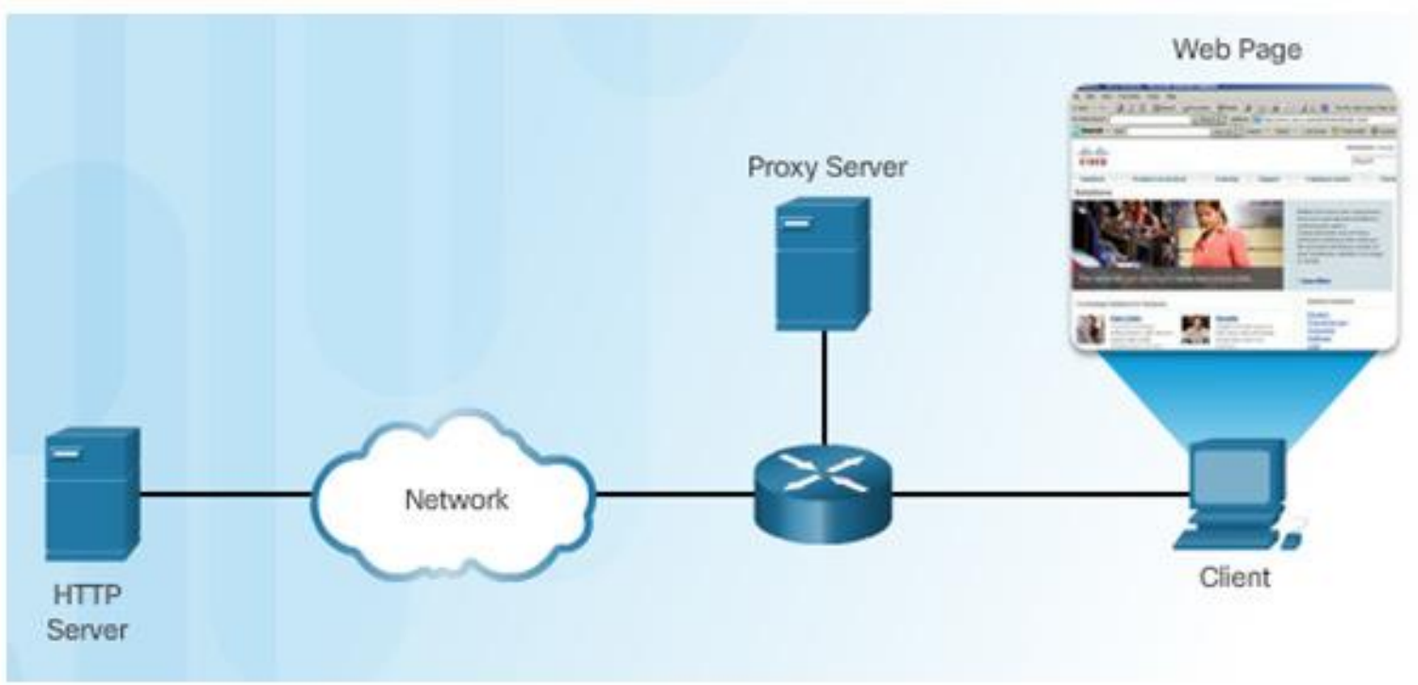
Hosts need a variety of services to securely access resources on the network and the Internet.

- Dynamic Host Configuration Protocol (**DHCP**) dynamically assigns IP addressing information to hosts.
- Domain Name Service (**DNS**) is the method computers use to translate domain names into IP addresses.



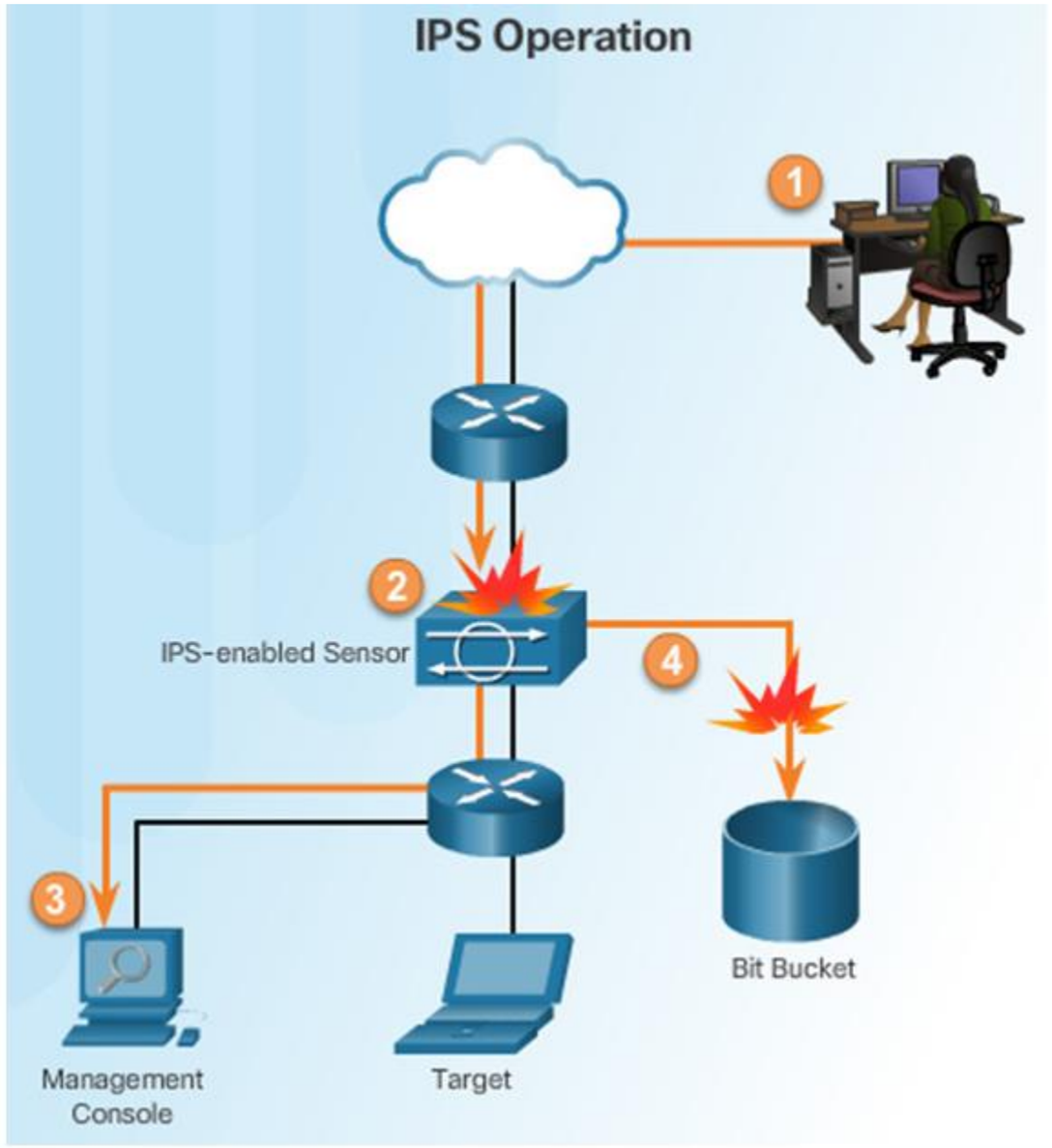


- Hypertext Transfer Protocol (**HTTP**) or the secure HTTP (**HTTPS**) are used by hosts to access web resources
- File Transfer Protocol (**FTP**) allows hosts to transfer data between a client and a server. Secure file transfer options include File Transfer Protocol Secure (FTPS), SSH File Transfer Protocol (SFTP), and Secure Copy (SCP)
- Simple Mail Transfer Protocol (**SMTP**), Post Office Protocol (**POP**), and Internet Message Access Protocol (**IMAP**) are the protocols hosts used to send and receive email.



Hosts need a variety of services to securely access resources on the network and the Internet.

- **Print servers** enable multiple computer users to access a single printer
- **Proxy servers** are popularly used to act as storage or cache for web pages that are frequently accessed by hosts on the internal network.
- **Intrusion Detection Systems** (IDSs) passively monitor traffic on the network while Intrusion Prevention Systems (**IPSs**) can detect and immediately address a network problem.
- **Universal Threat Management** (UTM) include all the functionality of an IDS/IPS as well as stateful firewall services.



8.4 Common Preventive Maintenance Techniques Used for Networks

8.4.1 Network Maintenance

Preventive maintenance for networks includes the condition of cables, network devices, servers, and computers to make sure that they are kept clean and are in good working order.

You should develop a plan to perform scheduled maintenance and cleaning at regular intervals.

Inform the network administrator if you notice any of these issues to prevent unnecessary network downtime.

8.5 Basic Troubleshooting Process for Networks

8.5.1 Applying the Troubleshooting Process to Networks

Identify the Problem

- The first step in the troubleshooting process.
- A list of open and closed-ended questions is useful.

Establish a Theory of Probable Cause

- Based on the answers received, establish a theory probable cause.
- A list of common problems can be useful.

Test the Theory to Determine Cause

- Test your theories to determine the cause of the problem.
- A list of quick procedures to common problems can help.

Establish a Plan of Action to Resolve the Problem and Implement the Solution

- A plan of action is needed to solve the problem and implement a permanent solution.

Verify Full Network Functionality and Implement Preventive Measures

It is important to perform a full network check.

If applicable, implement preventive measures to avoid future problem recurrences.

Document Findings, Actions and Outcomes

Findings, repairs and notes should be documented.

This log can be helpful for future reference.

8.5.2 Common Problems and Solutions for Networks

Network problems can be attributed to hardware, software, or configuration issues

Common networking problems include:

- Network cables are damaged or unplugged.
- Legitimate users are denied remote access.
- Device lacks sufficient addressing information.
- Users cannot access the Internet.
- User cannot map a drive or share a folder on the network