11g High Power Wireless AP/Bridge

WAP-200A

User Manual

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

IMPORTANT NOTE:
FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

U-MEDIA declares that WAP -200A (FCC ID: SI5WAP200A) is limited in CH1~CH11 for 2.4 GHz by specified firmware controlled in U.S.A.

Copyright

This publication, including all photographs, illustrations and software, is protected under international copyright laws, with all rights reserved. Neither this manual, nor any of the material contained herein, may be reproduced without written consent of the author.

Copyright 2006

Trademark recognition

All product names used in this manual are the properties of their respective owners and are acknowledged.

Table of Contents

Getting Started with the WAP-200A

Congratulations on purchasing the WAP-200A! This manual provides information for setting up and configuring the WAP-200A. This manual is intended for both home users and professionals.

The following conventions are used in this manual:

THE NOTE SYMBOL INDICATES ADDITIONAL INFORMATION ON THE TOPIC AT HAND.

THE TIP SYMBOL INDICATES HELPFULL INFORMATION AND TIPS TO IMPROVE YOUR NETWORK EXPERIENCE.

THE CAUTION SYMBOL ALERTS YOU TO SITUATIONS THAT MAY DEGRADE YOUR NETWORKING EXPERIENCE OR COMPROMISE

LIKE NOTES AND TIPS, THE IMPORTANT SYMBOL INDICATES INFORMATION THAT CAN IMPROVE NETWORKING. THIS INFORMATION SHOULD NOT BE OVERLOOKED.

Package Contents

- WAP-200A Wireless AP/Bridge

- CAT-5 Ethernet Cable (the WAP-200A's Ethernet ports is Auto-MDIX)

- Power Adapter (5.0V, 2A)

- CD-ROM with Manual

- Quick Installation Guide

CAUTION

Using a power supply with a different voltage than the one included with your product will cause damage and void the warranty for this product.

Minimum System Requirements

- Computers with Windows, Macintosh, or Linux-based operating systems with an installed Ethernet adapter and CD-ROM.

- Internet Explorer Version 6.0 or Netscape Navigator Version 7.0 and Above

Wireless LAN Networking

This section provides background information on wireless LAN networking technology. Consult the "Glossary" for definitions of the terminology used in this section.

THE INFORMATION IN THIS SECTION IS FOR YOUR REFERENCE. CHANGING NETWORK SETTINGS AND PARTICULARLY SECURITY SETTTINGS SHOULD ONLY BE DONE BY AN AUTHORIZED ADMINISTRATOR.

Transmission Rate (Transfer Rate)

The WAP-200A provides various transmission (data) rate options for you to select. Options include Best (Auto), 1 Mbps, 2 Mbps, 5.5 Mbps, 11 Mbps, 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 22 Mbps, 24 Mbps, 36 Mbps, 48 Mbps and 54 Mbps. In most networking scenarios, the factory default Best (Auto) setting proves the most efficient. This setting allows your WAP-200A to operate at the maximum transmission (data) rate. When the communication quality drops below a certain level, the WAP-200A automatically switches to a lower transmission (data) rate. Transmission at lower data speeds is usually more reliable. However, when the communication quality improves again, the WAP-200A gradually increases the transmission (data) rate again until it reaches the highest available transmission rate.

## Types of Wireless Networks

Wireless LAN networking works in either of the two modes: ad-hoc and infrastructure. In infra-structure mode, wireless devices communicate to a wired LAN via access points. Each access point and its wireless devices are known as a Basic Service Set (BSS). An Extended Service Set (ESS) is two or more BSSs in the same subnet. In ad hoc mode (also known as peer-to-peer mode), wireless devices communicate with each other directly and do not use an access point. This is an Independent BSS (IBSS).

To connect to a wired network within a coverage area using access points, set the WAP-200A operation mode to Infrastructure (BSS). To set up an independent wireless workgroup without an access point, use Ad-hoc (IBSS) mode.

AD-HOC (IBSS) NETWORK

Ad-hoc mode does not require an access point or a wired network. Two or more wireless stations communicate directly to each other. An ad-hoc network may sometimes be referred to as an Independent Basic Service Set (IBSS).

To set up an ad-hoc network, configure all the stations in ad-hoc mode. Use the same SSID and channel for each station.
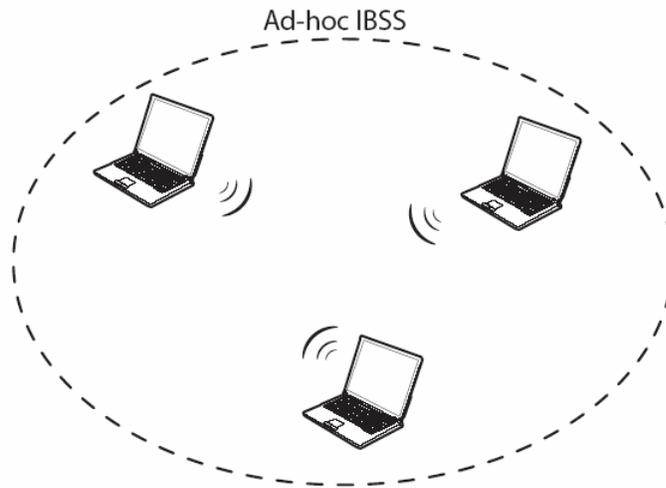
Ad-hoc (also known as peer-to-peer) network diagram

When a number of wireless stations are connected using a single access point, you have a Basic Service Set (BSS).

Infrastructure (IBSS) network diagram
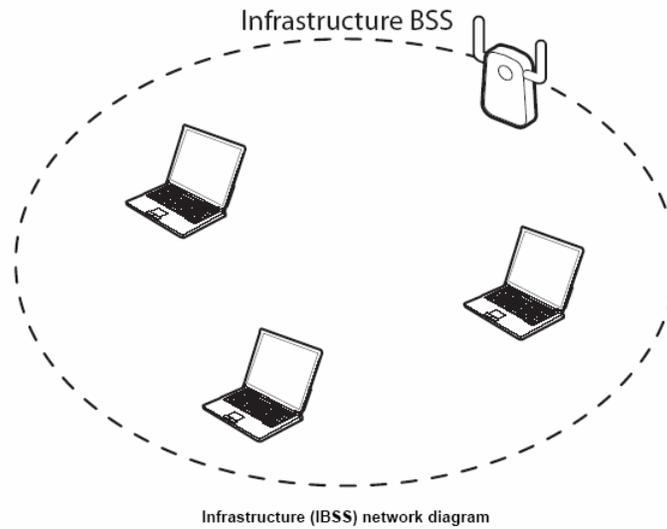
In the ESS diagram below, communication is done through the access points, which relay data packets to other wireless stations or devices connected to the wired network. Wireless stations can then access resources, such as a printer, on the wired network.

Infrastructure (ESS) network diagram
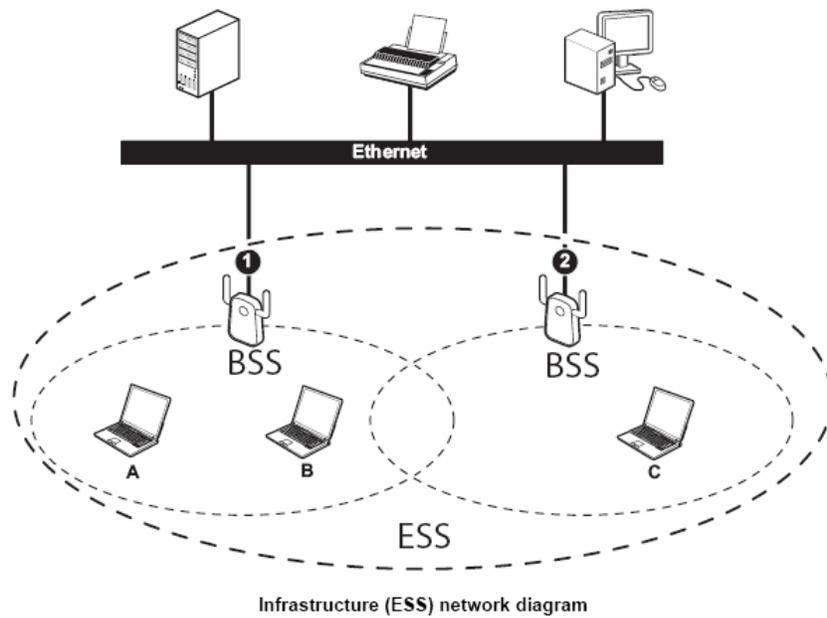
In an ESS environment, users are able to move from one access point to another without losing the

connection. In the diagram below, when the user moves from BSS (1) to BSS (2) the WAP-200A automatically switches to the channel used in BSS (2).
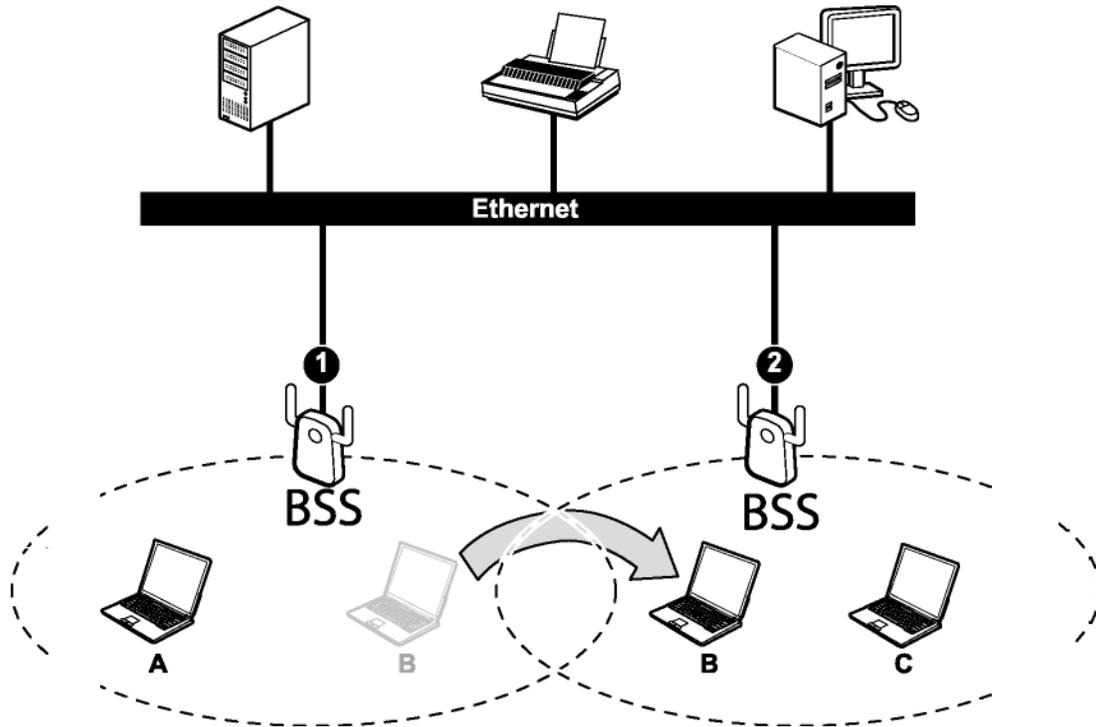
Roaming in an ESS network diagram

Introduction

The WAP-200A Wireless AP/Bridge is an 802.11g high-gain, wireless AP that supports high-speed wireless networking at home, at work or in public places.

The 802.11g standard is backwards compatible with 802.11b products. This means that you do not need to change your entire network to maintain connectivity. You may sacrifice some of 802.11g's speed when you mix 802.11b and 802.11g devices, but you will not lose the ability to communicate when you incorporate the 802.11g standard into your 802.11b network. You may choose to slowly change your network by gradually replacing the 802.11b devices with 802.11g devices.

Hardware Overview

At Real Panel

DC-IN

The DC power input connector is a single jack socket to supply power to the WAP-200A.
Please use the Power Adapter provided on the WAP-200A package.

Auto MDI/MDIX LAN Ports

This port automatically senses the cable type when connecting to Router.

Reset Button

Pressing the reset button restores the AP to its original factory default settings.

LEDs

- **PWR**

  ON: Power ON
  OFF: Power OFF

- **SYS**

Blinking: Device is not ready or system booting
ON: system ready after booting

- **ETHN**

  OFF: Has no Ethernet connection
  ON: 10M/100M connection
  Blinking: sending/receiving data

- **WLAN**

  Blinking: Data TX/RX through wireless access point
  OFF: PWR OFF or wireless module disconnected
  ON: Wireless Connected
  Flashing: Wireless is scanning, keeping trying to get associated with desired Access Point. In
                  Share Key mode, or WPA/WPA2 mode, the LED should keep flashing before
                  authenticated and associated. The Flashing frequency should be 1time/0.5 Sec.
                  It must be very easily to be distinguished from Blinking.

- **Signal**

  Flashing: The Signal LED is GPIO Configurable. Steady on: Link Quality > 80%;
                  Flashes 1 time/Sec: 80%<Link Quality <60%; 2times/Sec: 60%<Link Quaility<30%;
                  4times/Sec: Link Quality <30% Off: Wireless is Not connected

Installation Considerations

The WAP-200A Wireless AP/Bridge lets you access your network, using a wireless connection, from virtually anywhere within its operating range. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

1 Keep the number of walls and ceilings between the WAP-200A and other network devices to a minimum - each wall or ceiling can reduce your   wireless product's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.

2 Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.

3 Building Materials can impede the wireless signal - a solid metal door or aluminum studs may have a negative effect on range. Try to position wireless devices and computers with wireless adapters so that the signal passes through drywall or open doorways and not other materials.

4 Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate extreme RF noise.

Getting Started

For a typical wireless setup at home, please do the following:

1. Plug the power adapter to outlay, and connect the power jack to the WAP-200A.

2. Connect the Ethernet LAN port of the WAP-200A to your PC.

3. Open your web browser, and type http://192.168.0.100 to login WAP-200A.

4. When the authentication window is popped up, type the **admin** for the username, and leave the password as blank, then type enter to login the web page of the WAP-200A.

5. Configure the desired wireless setting.

6. Connect the Ethernet port of the WAP-200A to your router.

Using the Configuration Menu

Whenever you want to configure your WAP-200A, you can access the Configuration Menu by opening the Web-browser and typing in the IP Address of the WAP-200A. The WAP-200A's default IP Address is http://192.168.0.100.

➢   Open the Web browser.
➢   Type in the **IP Address** of the AP (http://192.168.0.100).
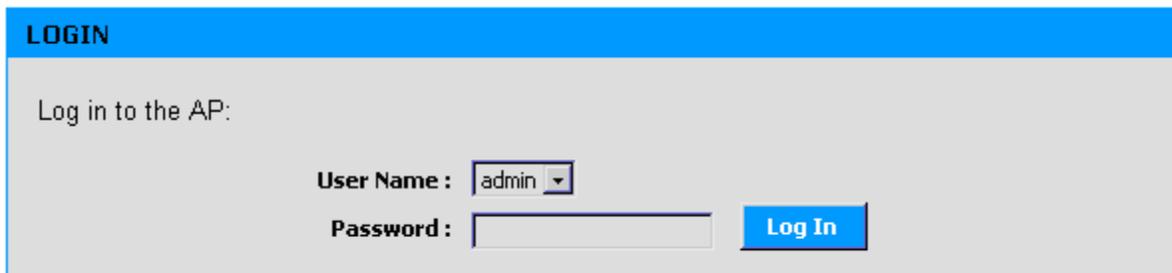
LOGIN

Log in to the AP:

        User Name : admin

        Password : [   ] **Log In**

NOTE   If you have changed the default IP Address assigned to the WAP-200A, make sure to enter the correct IP Address.

➢   Type **admin** in the **User Name** field.
➢   Leave the **Password** blank.
➢   Click **Login In.**

Information

Access Point Name

Model name of this Access Point

MAC Address

The Ethernet ID (MAC address) of the wireless client.

Firmware version

Current firmware version of this Access Point

SSID

When you are browsing for available wireless networks, this is the name that will appear in the list. For security purposes, it is highly recommended to change from the pre-configured network name.

Current transmit rate

Current setting for wireless transmit rate

Current channel

Current setting of wireless channel

Security

Current setting of wireless security mode

IP address

The IP address of the access point.

Stations

This section shows you a list of MAC address of stations that have associated to this Access Point.

Wireless

This wireless section is used to configure the wireless settings for your Wireless AP. Please note that changes made on this section may also need to be duplicated on your Wireless Client.

Wireless On/Off

This option turns off and on the wireless connection feature of the AP.

Wireless Network Name

When you are browsing for available wireless networks, this is the name that will appear in the list (unless Visibility Status is set to invisible, see below). This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the pre-configured network name.

Visibility Status

The Invisible option allows you to hide your wireless network. When this option is set to Visible, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When Invisible mode is enabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

Transmission Rate

By default the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.

802.11 Mode

If all of your devices can connect in 802.11g Mode, you can change the mode to 802.11g only. If you have some devices that are 802.11b, leave the setting at Mixed.

Adaptive Radio Selection

Check this box to enable Adaptive Radio feature in Dynamic Turbo mode.

Auto Channel Select

If you select this option, the AP automatically finds the channel with least interference and uses that channel for wireless networking. If you disable this option, the AP uses the channel that you specify with the following **Channel** option.

Channel

A wireless network uses specific channels in the 2.4GHz wireless spectrum to handle communication between clients. Some channels in your area may have interference from other electronic devices. Choose the clearest channel to help optimize the performance and coverage of your wireless network.

WDS

Wireless Distribution System (WDS). When WDS is enabled, this access point functions as a wireless repeater and is able to wirelessly communication with other APs.

Enable WDS

When WDS is enabled, this access point functions as a wireless repeater and is able to wirelessly communicate with other APs via WDS links. Note that WDS is incompatible with WPA -- both features cannot be used at the same time. A WDS link is bidirectional; so this AP must know the MAC Address (creates the WDS link) of the other AP, and the other AP must have a WDS link back to this AP.

AP MAC Address #

Specifies one-half of the WDS link. The other AP must also have the MAC address of this AP to create the WDS link back to this AP.

Security

On this section you can set the 802.11g security and encryption options. Any new settings will not take effect until the device is rebooted.

WPA Enable

Select to enable WPA function

WPA Mode

WPA is the older standard; select this option if the clients that will be used with the AP only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the "WPA2" option, the AP tries WPA2 first, but falls back to WPA if the client only supports WPA. With the "WPA2 Only" option, the AP associates only with clients that also support WPA2 security.

Cipher Type

The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per-packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption. With the "TKIP and AES" option, the AP negotiates the cipher type with the client, and uses AES when available.

PSK

The key is entered as a pass-phrase of up to 63 alphanumeric characters in ASCII (American Standard Code for Information Interchange) format at both ends of the wireless connection. It cannot be shorter than eight characters, although for proper security it needs to be of ample length and should not be a commonly known phrase. This phrase is used to generate session keys that are unique for each wireless client.

WPA Group Key Update Interval

The interval defines how frequent the key used for broadcast/multicast will be changed. Unit: second

Access

On this section you can enable Access Control. If enabled, only the MAC addresses entered into the "MAC address" boxes are allowed to associate to this AP. Note that you can cut and paste the addresses from the "Station List" page into MAC address boxes. Any new settings will not take effect until the device is rebooted.

Enable Access Control

> By default, the Access Control feature is disabled. If you need Access Control, check this option.

MAC Address #

> MAC addresses entered into the "MAC address" boxes are allowed to associate to this AP.

Admin

On this section you can configure the IP address used by the Web server running on this device. For "static" mode, the IP address settings are given here. For "DHCP" mode, these settings are supplied by a DHCP server on your network. You can also change the password, reboot the device, or reset all settings to their factory defaults. If you have changed any settings it is necessary to reboot the device for the new settings to take effect.

Firmware Upgrade

> **Note:** Firmware upgrade cannot be performed from a wireless device. To perform an upgrade, ensure that you are using a PC that is connected to the AP by wire.

> **Note:** Some firmware upgrades reset the AP's configuration options to the factory defaults.

> **Upload**

> Once you have a firmware update on your computer, use this option to browse for the file and then upload the information into the AP.

Device name

> This is the name that the device will use to identify itself.

IP Address Mode

> Select "DHCP" to get the IP settings from a DHCP server on your network. Select "Static" to use the IP settings specified on this section.

Default IP address

When configure as Static IP address mode, it defines the IP address of your device.

Default subnet mask

When configure as Static IP address mode, it defines the subnet mask specifies the network number portion of an IP address.

Default gateway

When configure as Static IP address mode, it defines the IP address of the gateway that connects you to the internet.

Security

User name

This is the user name that you must type when logging in to these web pages.

Administrator password

This is the password that you must type when logging in to these web pages. You must enter same password into both boxes, for confirmation.

Advanced

On this section you can configure the advanced 802.11g wireless settings. If you have changed any settings it is necessary to reboot the device for the new settings to take effect.

Fragmentation Threshold

This setting should remain at its default value of 2346. Setting the Fragmentation value too low may result in poor performance.

RTS Threshold

This setting should remain at its default value of 2346. If you encounter inconsistent data flow, only minor modifications to the value are recommended.

Beacon Period

Beacons are packets sent by a wireless AP to synchronize wireless devices. Specify a Beacon Period value between 20 and 1000. The default value is set to 100 milliseconds.

DTIM Interval

A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.

Glossary

Access Control List

ACL. This is a database of network devices that are allowed to access resources on the network.

Access Point

AP. Device that allows wireless clients to connect to it and access the network

Ad-hoc network

Peer-to-Peer network between wireless clients

Address Resolution Protocol

ARP. Used to map MAC addresses to IP addresses so that conversions can be made in both directions.

Advanced Encryption Standard

AES. Government encryption standard

Alphanumeric

Characters A-Z and 0-9

Antenna

Used to transmit and receive RF signals.

ASCII

American Standard Code for Information Interchange. This system of characters is most commonly used for text files

Attenuation

The loss in strength of digital and analog signals. The loss is greater when the signal is being transmitted over long distances.

Authentication

To provide credentials, like a Password, in order to verify that the person or device is really who they are claiming to be

Automatic Private IP Addressing

APIPA. An IP address that that a Windows computer will assign itself when it is configured to obtain an IP address automatically but no DHCP server is available on the network

Backward Compatible

The ability for new devices to communicate and interact with older legacy devices to guarantee interoperability

Bandwidth

The maximum amount of bytes or bits per second that can be transmitted to and from a network device

Beacon

A data frame by which one of the stations in a Wi-Fi network periodically broadcasts network control data to other wireless stations.

Bit rate

The amount of bits that pass in given amount of time

Bit/sec

Bits per second

BOOTP

Bootstrap Protocol. Allows for computers to be booted up and given an IP address with no user intervention

Broadcast

Transmitting data in all directions at once

Browser

A program that allows you to access resources on the web and provides them to you graphically

C

CAT 5

Category 5. Used for 10/100 Mbps or 1Gbps Ethernet connections

Client

A program or user that requests data from a server

Collision

When do two devices on the same Ethernet network try and transmit data at the exact same time.

Cookie

Information that is stored on the hard drive of your computer that holds your preferences to the site that gave your computer the cookie

D

Data

Information that has been translated into binary so that it can be processed or moved to another device

Data-Link layer

The second layer of the OSI model. Controls the movement of data on the physical link of a network

dBd

Decibels related to dipole antenna

dBi

Decibels relative to isotropic radiator

dBm

Decibels relative to one milliwatt

Decrypt

To unscramble an encrypted message back into plain text

Default

A predetermined value or setting that is used by a program when no user input has been entered for this value or setting

DHCP

Dynamic Host Configuration Protocol: Used to automatically assign IP addresses from a predefined pool of addresses to computers or devices that request them

Digital certificate:

An electronic method of providing credentials to a server in order to have access to it or a network

Direct Sequence Spread Spectrum

DSSS: Modulation technique used by 802.11b wireless devices

DNS

Domain Name System: Translates Domain Names to IP addresses

Domain name

A name that is associated with an IP address

Download

To send a request from one computer to another and have the file transmitted back to the requesting computer

Duplex

Sending and Receiving data transmissions at the sane time

Dynamic IP address

IP address that is assigned by a DHCP server and that may change. Cable Internet providers usually use this method to assign IP addresses to their customers.

E

EAP

Extensible Authentication Protocol

Encryption

Converting data into cyphertext so that it cannot be easily read

Ethernet

The most widely used technology for Local Area Networks.

F

File server

A computer on a network that stores data so that the other computers on the network can all access it

File sharing

Allowing data from computers on a network to be accessed by other computers on the network with different levels of access rights

Firewall

A device that protects resources of the Local Area Network from unauthorized users outside of the local network

Firmware

Programming that is inserted into a hardware device that tells it how to function

Fragmentation

Breaking up data into smaller pieces to make it easier to store

FTP

File Transfer Protocol. Easiest way to transfer files between computers on the Internet

Full-duplex

Sending and Receiving data at the same time

G

Gain

The amount an amplifier boosts the wireless signal

Gateway

A device that connects your network to another, like the internet

Gbps

Gigabits per second

Gigabit Ethernet

Transmission technology that provides a data rate of 1 billion bits per second

GUI

Graphical user interface

H

Half-duplex

Data cannot be transmitted and received at the same time

Hashing

Transforming a string of characters into a shorter string with a predefined length

Hexadecimal

Characters 0-9 and A-F

Hop

The action of data packets being transmitted from one AP to another

Host

Computer on a network

HTTP

Hypertext Transfer Protocol is used to transfer files from HTTP servers (web servers) to HTTP clients (web browsers)

HTTPS

HTTP over SSL is used to encrypt and decrypt HTTP transmissions

Hub

A networking device that connects multiple devices together

I

ICMP

Internet Control Message Protocol

IEEE

Institute of Electrical and Electronics Engineers

IGMP

Internet Group Management Protocol is used to make sure that computers can report their multicast group membership to adjacent APs

IIS

Internet Information Server is a WEB server and FTP server provided by Microsoft

Infrastructure

In terms of a wireless network, this is when wireless clients use an Access Point to gain access to the network

Internet

A system of worldwide networks which use TCP/IP to allow for resources to be accessed from computers around the world

Internet Explorer

A World Wide Web browser created and provided by Microsoft

Internet Protocol

The method of transferring data from one computer to another on the Internet

Internet Protocol Security

IPsec provides security at the packet processing layer of network communication

Internet Service Provider

An ISP provides access to the Internet to individuals or companies

Intranet

A private network

Intrusion Detection

A type of security that scans a network to detect attacks coming from inside and outside of the network

IP

Internet Protocol

IP address

A 32-bit number, when talking about Internet Protocol Version 4, that identifies each computer that transmits data on the Internet or on an Intranet

IPsec

Internet Protocol Security

IPX

Internetwork Packet Exchange is a networking protocol developed by Novel to enable their Netware clients and servers to communicate

ISP

Internet Service Provider

Java

A programming language used to create programs and applets for web pages

Kbps

Kilobits per second

Kbyte

Kilobyte

LAN

Local Area Network

Latency

The amount of time that it takes a packet to get from the one point to another on a network. Also referred to as delay

LED

Light Emitting Diode

Legacy

Older devices or technology

Local Area Network

A group of computers in a building that usually access files from a server

LPR/LPD

"Line Printer Requestor"/"Line Printer Daemon". A TCP/IP protocol for transmitting streams of printer data.

L2TP

Layer 2 Tunneling Protocol

MAC address

A unique hardware ID assigned to every Ethernet adapter by the manufacturer.

Mbps

Megabits per second

MDI

Medium Dependent Interface is an Ethernet port for a connection to a straight-through cable

MDIX

Medium Dependent Interface Crossover, is an Ethernet port for a connection to a crossover cable

MIB

Management Information Base is a set of objects that can be managed by using SNMP

Modem

A device that Modulates digital signals from a computer to an analog signal in order to transmit the signal over phone lines. It also Demodulates the analog signals coming from the phone lines to digital signals for your computer

MPPE

Microsoft Point-to-Point Encryption is used to secure data transmissions over PPTP connections

MTU

Maximum Transmission Unit is the largest packet that can be transmitted on a packet-based network like the Internet

Multicast

Sending data from one device to many devices on a network

N

NAT

Network Address Translation allows many private IP addresses to connect to the Internet, or another network, through one IP address

NetBEUI

NetBIOS Extended User Interface is a Local Area Network communication protocol. This is an updated version of NetBIOS

NetBIOS

Network Basic Input/Output System

Netmask

Determines what portion of an IP address designates the Network and which part designates the Host

Network Interface Card

A card installed in a computer or built onto the motherboard that allows the computer to connect to a network

Network Layer

The third layer of the OSI model which handles the routing of traffic on a network

Network Time Protocol

Used to synchronize the time of all the computers in a network

NIC

Network Interface Card

NTP

Network Time Protocol

O

OFDM

Orthogonal Frequency-Division Multiplexing is the modulation technique for both 802.11a and 802.11g

OSI

Open Systems Interconnection is the reference model for how data should travel between two devices on a network

OSPF

Open Shortest Path First is a routing protocol that is used more than RIP in larger scale networks because only changes to the routing table are sent to all the other APs in the network as opposed to sending the entire routing table at a regular interval, which is how RIP functions

P

Password

A sequence of characters that is used to authenticate requests to resources on a network

Personal Area Network

The interconnection of networking devices within a range of 10 meters

Physical layer

The first layer of the OSI model. Provides the hardware means of transmitting electrical signals on a data carrier

Ping

A utility program that verifies that a given Internet address exists and can receive messages. The utility sends a control packet to the given address and waits for a response.

PoE

Power over Ethernet is the means of transmitting electricity over the unused pairs in a category 5 Ethernet cable

Port

A logical channel endpoint in a network. A computer might have only one physical channel (its Ethernet channel) but can have multiple ports (logical channels) each identified by a number.

PPP

Point-to-Point Protocol is used for two computers to communicate with each over a serial interface, like a phone line

PPPoE

Point-to-Point Protocol over Ethernet is used to connect multiple computers to a remote server over Ethernet

PPTP

Point-to-Point Tunneling Protocol is used for creating VPN tunnels over the Internet between two networks

Preamble

Used to synchronize communication timing between devices on a network

Q

QoS

Quality of Service

R

RADIUS

Remote Authentication Dial-In User Service allows for remote users to dial into a central server and be authenticated in order to access resources on a network

Reboot

To restart a computer and reload it's operating software or firmware from nonvolatile storage.

Rendezvous

Apple's version of UPnP, which allows for devices on a network to discover each other and be connected without the need to configure any settings

Repeater

Retransmits the signal of an Access Point in order to extend it's coverage

RIP

Routing Information Protocol is used to synchronize the routing table of all the APs on a network

RJ-11

The most commonly used connection method for telephones

RJ-45

The most commonly used connection method for Ethernet

RS-232C

The interface for serial communication between computers and other related devices

RSA

Algorithm used for encryption and authentication

S

Server

A computer on a network that provides services and resources to other computers on the network

Session key

An encryption and decryption key that is generated for every communication session between two computers

Session layer

The fifth layer of the OSI model which coordinates the connection and communication between applications on both ends

Simple Mail Transfer Protocol

Used for sending and receiving email

Simple Network Management Protocol

Governs the management and monitoring of network devices

SIP

Session Initiation Protocol. A standard protocol for initiating a user session that involves multimedia content, such as voice or chat.

SMTP

Simple Mail Transfer Protocol

SNMP

Simple Network Management Protocol

SOHO

Small Office/Home Office

SPI

Stateful Packet Inspection

SSH

Secure Shell is a command line interface that allows for secure connections to remote computers

SSID

Service Set Identifier is a name for a wireless network

Stateful inspection

A feature of a firewall that monitors outgoing and incoming traffic to make sure that only valid responses to outgoing requests are allowed to pass though the firewall

Subnet mask

Determines what portion of an IP address designates the Network and which part designates the Host

Syslog

System Logger -- a distributed logging interface for collecting in one place the logs from different sources. Originally written for UNIX, it is now available for other operating systems, including Windows.

T

TCP

Transmission Control Protocol

TCP/IP

Transmission Control Protocol/Internet Protocol

TCP Raw

A TCP/IP protocol for transmitting streams of printer data.

TFTP

Trivial File Transfer Protocol is a utility used for transferring files that is simpler to use than FTP but with less features

Throughput

The amount of data that can be transferred in a given time period

Traceroute

A utility displays the routes between you computer and specific destination

U

UDP

User Datagram Protocol

Unicast

Communication between a single sender and receiver

Universal Plug and Play

> A standard that allows network devices to discover each other and configure themselves to be a part of the network

Upgrade

> To install a more recent version of a software or firmware product

Upload

> To send a request from one computer to another and have a file transmitted from the requesting computer to the other

UPnP

> Universal Plug and Play

URL

> Uniform Resource Locator is a unique address for files accessible on the Internet

USB

> Universal Serial Bus

UTP

> Unshielded Twisted Pair

V

Virtual Private Network

> VPN: A secure tunnel over the Internet to connect remote offices or users to their company's network

VLAN

> Virtual LAN

Voice over IP

> Sending voice information over the Internet as opposed to the PSTN

VoIP

> Voice over IP

W

Wake on LAN

> Allows you to power up a computer though it's Network Interface Card

WAN

> Wide Area Network

WCN

Windows Connect Now. A Microsoft method for configuring and bootstrapping wireless networking hardware (access points) and wireless clients, including PCs and other devices.

WDS

Wireless Distribution System. A system that enables the interconnection of access points wirelessly.

Web browser

A utility that allows you to view content and interact with all of the information on the World Wide Web

WEP

Wired Equivalent Privacy is security for wireless networks that is supposed to be comparable to that of a wired network

Wi-Fi

Wireless Fidelity

Wi-Fi Protected Access

An updated version of security for wireless networks that provides authentication as well as encryption

Wide Area Network

The larger network that your LAN is connected to, which may be the Internet itself, or a regional or corporate network

Wireless ISP

A company that provides a broadband Internet connection over a wireless connection

Wireless LAN

Connecting to a Local Area Network over one of the 802.11 wireless standards

WISP

Wireless Internet Service Provider

WLAN

Wireless Local Area Network

WPA

Wi-Fi Protected Access. A Wi-Fi security enhancement that provides improved data encryption, relative to WEP.

X

xDSL

A generic term for the family of digital subscriber line (DSL) technologies, such as ADSL, HDSL, RADSL, and SDSL.

Y

Yagi antenna

A directional antenna used to concentrate wireless signals on a specific location

Z

#

1

802.11

A family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE).