
A.1 Hardware Specifications

WAN Interface

- One Ethernet 10BaseT (IEEE 802.3) port (RJ-45).

LAN Interface

- **AG2000:** One 10BaseT (IEEE 802.3) Ethernet port (RJ-45).
- **AG2000S:** Four 10/100 BaseT Ethernet switching ports (RJ-45).

Wireless LAN Interface

- IEEE 802.11b High Rate compliant.
- Operating in the unlicensed 2.4GHz ISM band.
- Operation Frequency/Channels (Either one below):
 - North America/FCC: 2.412~2.462 GHz (11 channels).
 - Europe/ETS: 2.412~2.472 GHz (13 channels).
 - Japan TELEC: 2.412~2.472 GHz (14 channels).
- Modulation Technique: Direct Sequence Spread Spectrum (CCK, DQPSK, DBPSK).
- Dynamic Rate Shifting: 11, 5.5, 2 and 1Mbps.
- Media Access Protocol: CSMA/CA with ACK.
- Security Management: 40-bit, 128-bit WEP (wired equivalent privacy) Encryption.
- Maximum Output Power: 17dBm (50mW).

Antenna

- Removable 3-dBi diversity high gain dipole antenna.

LEDs

AG2000

- PWR
- DIAG
- WAN
- LAN
- WLAN

AG2000s

- PWR
- DIAG
- WAN

-
- LAN/LINK 1 - 4
 - LAN/ACT 1 - 4
 - WLAN

Mechanical

- Dimensions: 8" (w) x 5.75" (d) x 1.5" (h).
- Weight: 1.5 lbs.

Operating Environment

- Operating temperature: 0°C to 40°C (32°F to 104°F).
- Operating humidity: 0% to 95% non-condensing.

Power

External AC Power Adapter

- Input: 230V 85mA or 120V 155mA, 47-60 Hz.
- Output: 13.5V AC, 1A.
- Power consumption: 8.5 watts nominal.

Compliance / Regulatory

- EMI: FCC Part15 Class B & Part 15C, CE EN55022 Class B.
- Telecom: FCC Part 68.
- Wi-Fi Certified.
- Immunity: CE EN55024.
- Safety: CE EN60950

A.2 Software Features

Authentication

802.1x Authentication

- EAP/ MD5 (PPP Extensible Authentication Protocol, RFC 2284) mechanism for authentication.
- RADIUS server (RFC2865, RFC 2869).
- RADIUS Accounting (RFC 2866).

MAC Authentication

- Authentication through the client's MAC address (RFC 2865).

Web Re-direction

- Unauthorized users automatically re-direct to a configured web page for registration.

Radio Control

Automatic Channel Selection

- Automatically selects the optimal channel for minimal radio interference from other nearby APs.
- ON/OFF selectable.

Date Rate Selection

- Manually selects data rates from 1Mbps, 2Mbps, 5.5Mbps and 11Mbps.

Roaming

- IEEE 802.11b High Rate compliant.
- Automatic account roll-over.

RADIUS

- Up to two RADIUS authentication servers: Authentication and Accounting Servers.
- Configured port number and accounting port number.

Routing

- TCP/IP (RFC791, RFC792, RFC793), ARP (RFC826).
- Static routing on the LAN and/or WAN.
- Dynamic routing protocol supports RIP1 (RFC1058), RIP2 (RFC1723).

DHCP

- DHCP server (RFC 2131, RFC 2132): automatic to assign IP address, Subnet Mask, Gateway, and DNS to workstations.
- DHCP relay.
- DHCP pass-through.

Bridging

- IEEE 802.1d-compliant transparent bridging between wireless interface and wired LAN interface.
- Bridge Filters – Up to 32 filter entries, MAC address criteria setup.
- Supports up to 510 MAC learning addresses.
- RFC1483-bridged (LLC or VC MUX encapsulation) over ATM PVC.

Internet Access Sharing

- NAT/PAT (RFC 1631) proxy supports unlimited multi-user sharing via Ethernet LAN.
- NAT (Network Address Translation) supports PAT (Port Address Translation) for Web server hosting, multimedia applications, and Internet gaming.
- NAT supports PPTP and IPsec VPN pass through.

Security

- IEEE 802.1X port-based network access control.
- PAT (RFC 1334), CHAP (RFC 1994), and MS-CHAP user authentication.
- Username and password control for network management access.
- WEP (Wired Equivalent Privacy): 40/128-bit encryption keys and SSID.

Network Management

Access Interfaces

- Web browser-based manager.
- Command Line Interface through RS-232 console port.
- Telnet support.
- SNMP (Simple Network management Protocol): RFC 1157.

SNMP

- MIB II (RFC 1213).
- Wireless MIB (IEEE 802.11).
- Private MIB.
- SNMP traps (RFC 1215).

Functions

- Device configuration.
- Firmware upgrade available via FTP or locally.
- Real time status display and event report and Syslog.
- Remote reboot (hardware) and reset.

NOTE: Product specifications are subject to change without prior notice.

B.1 Connector Specifications

B.1.1 10/100 Ports

The 10/100 Ethernet ports use standard RJ-45 connectors and Ethernet pinouts with internal crossovers, as shown by an X in the port name. These ports have their transmit (Tx) and receive (Rx) signals internally crossed so that a straight-through Ethernet cable and an adapter can be attached to the port. The figure below shows the pinouts.

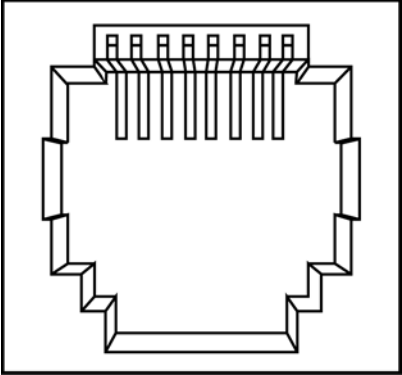
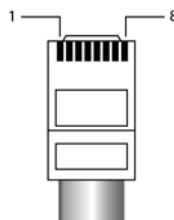
Pin	Label	1 2 3 4 5 6 7 8
1	Tx+	
2	Tx-	
3	Rx+	
4	NC	
5	NC	
6	Rx-	
7	NC	
8	NC	

Figure B.1 10/100 Ethernet Port Pinout

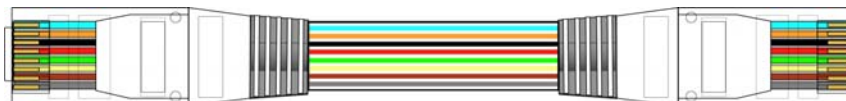
B.2 Cable Specification

B.2.1 RJ-45

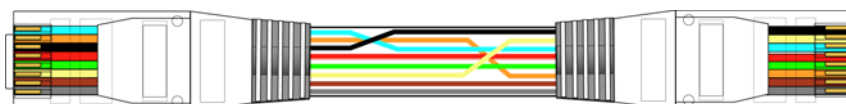
The pin assignment is as follows:



RJ-45 to RJ-45 Straight-through Ethernet Cable:



RJ-45 to RJ-45 Crossover Ethernet Cable:



802.1X	An IEEE standard for local and metropolitan area networks, called Port-based Network Access Control. It is used to securely establish an authenticated association between the client and the AP.
AP (Access Point)	A hardware device, or software used in conjunction with a computer, that serves as a communications “hub” for wireless clients and provides a connection to a wired LAN. An AP can double the range of wireless clients and provide enhanced security.
Ad-Hoc Mode	A client setting that provides independent peer-to-peer connectivity in a wireless LAN. An alternative set-up is where PCs communicate with each other through an AP (see also Infrastructure Mode).
Bandwidth	The amount of data that can be transmitted by the network “information highway”, used as an indication for speed of data transmission. An Ethernet link is capable of moving 10 million bits of data per second.
Bit	The term used to refer to a single unit of data in digital data communications. It takes 8 bits to make 1 byte, which is a unit of measurement for computer data.
Bps (Bits per second)	Refers to the unit of measurement used for data transmission speeds over a data communication link.
Bridge	A hardware device that passes packets between multiple network segments using the same networking protocol to connect the different network segments. Bridge operates at the hardware layer and has no routing capabilities.
Broadband	Any high-bandwidth (see also Bandwidth) data communication technology that runs at speeds of 200 Kbps or more and allows combined transmission of voice, data, and video over a single physical connection. Broadband is in contrast to narrowband such as traditional 56K analog modem. DSL, Cable, wireless, and satellite technology are all different types of broadband technology.
Byte	A unit of data equaling to 8 bits (1 Byte = 8 bits).
DHCP (Dynamic Host Configuration Protocol)	An Internet protocol that allows the DHCP server to dynamically assign IP addresses to any client workstation (any device connected to your LAN, such as a PC) for a set period of time and then sends them back so that they can be reassigned to other workstations. This feature saves the ISP and Network Managers from having to manually configure IP addresses for each PC on the LAN.
DNS (Domain Name System)	A mechanism that translates host domain names into its numeric IP Address and vice-versa. A domain name is an easy-to-remember nickname for numerical IP addresses required by a computer, such as janedoe@arescom.com.

Encapsulation	The encapsulating or enclosing data within a particular IP header. Sometimes the entire frame from one network is placed in the header used by the data link layer protocol of another network.
Encryption	A specific algorithm used to encrypt or encode the data so that it becomes unreadable to unauthorized users that do not know the decryption key. A good example of encryption technology is WEP (Wired Equivalent Private).
Ethernet	Most popular LAN (Local Area Network) technology that uses CSMA/CD (Collision Detection) and transfers data between workstations over a variety of cable types at 10Mbps, also called 10BaseT. Most Ethernet LANs use twisted pair 10BaseT cables and support both Ethernet as well as Fast Ethernet at 100Mbps (100BaseT).
Firewall	A security device (either hardware, software, or a combination of both) that selectively blocks out or filters unwanted IP traffic from a public network. Firewall allows the private LAN network to be invisible to the public network outside, preventing intrusion from unauthorized users.
Hub	A hardware device that repeats all data traffic to all CPE (Customer Premises Equipment) ports. A hub functions as the center of a LAN and all other network devices on the LAN, including PCs, printers, DSL modem or Gateways, are connected to the hub through cabling.
Infrastructure Mode	A client setting providing connectivity to an AP. As compared to Ad-Hoc Mode, where PCs communicate directly with each other, clients set in Infrastructure Mode all pass data through a central AP. The AP not only mediates wireless network traffic in the immediate neighborhood, but it also provides communication with the wired network (see also Ad-Hoc Mode and Access Point).
Internet	A massive worldwide network of computer networks interconnecting thousands of computers and networks around the world and readily accessible from any computer with a modem or router connection and the corresponding software.
IP (Internet Protocol)	A protocol standard for the Internet. A kind of Internet software that keeps track of all the addresses on the Internet for different nodes, forwards outgoing IP traffic, and recognizes incoming IP traffic.
IP Address	Numeric address assigned to each machine on the Internet. Consists of four sets of one, two, or three octal digits separated by periods.
ISP (Internet Service Provider)	The telecommunication company that provides Internet service for the subscriber. The ISP can be a telephone company, a CLEC or ILEC, or any other company that provides Internet access to the end user such as AOL, Earthlink or MSN.
LAN (Local Area Network)	A collection of privately-owned, interconnected computers within a confined service area.
WEP (Wired Equivalent Privacy)	WEP data encryption is defined by the 802.11 standard to prevent (i) access to the network by “intruders” using similar wireless LAN equipment and (ii) capture of wireless LAN traffic through eavesdropping. WEP allows the administrator to define a set of respective “Keys” for each wireless network user based on a “Key String” passed through the WEP encryption algorithm. Access is denied by anyone who does not have an assigned key.