GateOne 500A

High Speed, Long Range Ethernet Wireless Bridge

User's Guide

Ver 1.1
July, 2004

ZyGATE
Wireless·Mobile·Broadband

Copyright

GateOne 500A
Secure Outdoor Ethernet Radio Link

Disclaimer

ZyGATE does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyGATE further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Federal Communications Commission (FCC) Interference Statement

This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

This device may not cause harmful interference.

This device must accept any interference received, including interference that may cause undesired operations.

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 commercial environment. 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.

If this equipment does cause harmful interference to radio/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 or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and the 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.

Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Notice 2

Shielded RS-232 cables are required to be used to ensure compliance with FCC Part 15, and it is the responsibility of the user to provide and use shielded RS-232 cables.

Information for Canadian Users

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operation, and safety requirements. The Industry Canada does not guarantee that the equipment will operate to a user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly. The customer should be aware that the compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

For their own protection, users should ensure that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution

CAUTION:

Notes and Warnings to the User and Installer

Caution:

- This Installation Guide is intended for use by the professional wireless LAN system installer.
- The device cannot be sold retail, to the general public or by mail order. It must be sold to dealers or have strict marketing control.

WARNING: It is the responsibility of the professional installer to ensure that the system is used exclusively for fixed, point-to-point operations.

Warning: When using the GateOne 500A in the United States (or where FCC rules apply), it is the responsibility of the professional installer to ensure to control the output power not greater then the application (GateOne 500A: 126.77mW)

Who Should Use this Guide

Installation of this device should be accomplished only by a qualified wireless LAN system installer who is:

- Knowledgeable of the use, installation and configuration procedures and associated networking components.
- Knowledgeable of each system component’s equipment User and Installation Guide.
- Knowledgeable of the installation and configuration procedures for the site’s network infrastructure system and wiring.
- Knowledgeable of the installation procedures, safety, and code requirements for the site’s antenna, antenna mast, antenna cabling, and installation. Teletronics highly recommends that the antenna installation be performed by a qualified antenna installation professional.

Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

Note

This digital apparatus does not exceed the class A limits for radio noise emissions from digital apparatus set out in the radio interference regulations of Industry Canada.

ZyGATE Limited Warranty

ZyGATE warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyGATE will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal value, and will be solely at the discretion of ZyGATE. This warranty shall not apply if the product is modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyGATE shall in no event be held liable for indirect or consequential damages of any kind of character to the purchaser.

To obtain the services of this warranty, contact ZyGATE's Service Center; refer to the separate Warranty Card for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyGATE) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyGATE to the corresponding return address, Postage Paid (USA and territories only). If the customer desires some other return destination beyond the U.S. borders, the customer shall bear the cost of the return shipment. This warranty gives you specific legal rights, and you may also have other rights that vary from state to state.

Customer Support

Before contact ZyGATE customer support/representative, please record the following information for customer support:

- Model name (GateOne 500A) and serial number.
- Information in web page –System Information.
- Warranty Information.
- Date of receiving GateOne 500A
- Brief description of the problem and the troubleshooting procedures performed by technical personnel.

Method / Location	e-mail – Support/Sales	Telephone/Fax	Web Site/FTP Site	Regular Mail
Taiwan	support@zygate.com.tw	+886-3-480-8163 +886-3-499-3173	www.zygate.com.tw	ZyGATE Communications Inc. 48 Lung-Chin Road, Lung-Tan, Taoyuan, Taiwan.

Table of Contents

List of Figures

List of Tables

Chapter 1 Getting to Know Your GateOne

This chapter introduces the main features and applications of the GateOne.

1.1 Introduction to the GateOne 500A

The ZyGATE GateOne 500A is a Wireless Bridge for Inter-building Point to Point Ethernet connection. With enhanced wireless security feature, GateOne 500A is a Point to Point solution in the world today. By supporting AES/TKIP/WEP, GateOne 500A is particularly suited for financial banks, businesses and government agencies to deploy wireless networks for most sensitive data transmission. System privacy is inherent through the MAC & 802.1x based mutual authentication functionality by preventing unauthorized intrusion to the radio link. GateOne 500A has been design to minimize the RF cable loss for outdoor application, thus it shows outstanding performance in the longer communication distance. Supplying the power and Ethernet connectivity concurrently via a single Ethernet cable, the power over Ethernet (POE) technology makes quick outdoor installation. The optional antenna alignment kit, showing relative signal strength index (RSSI) and signal to noise ratio (SNR), is uniquely designed to aid easy antenna alignment while operating in the point to point connection. GateOne 500A achieves rapid return on investment (ROI) for inter-building connection compared to T1 leased line with high capacity and high data throughput.
There are some special requirements for the product installation:
1. The GateOne 500A can only be installed by a licensed installer; training and access to technical requirements will be provided through the user guide and through training done by the business partnership agreements with respective customers.
2. The installation will be done in a controlled and licensed environment; and filing of the appropriate documentation as required by local law.
3. Installation requires special training (special programming, access to keypad, field strength measurements made) by ZyGATE of the installation and maintenance teams of the ZyGATE licensed service providers and operators.
4. ZyGATE licensed service providers will be required to have their installation teams trained to do installation of the GateOne 500A and antennas on high sited areas in order to meet the performance and regulatory requirements. This will require professional installation; the installation of the GateOne 500A must be controlled and installed by licensed professionals. Specially designed antennas and mounting procedures will be required and professional installation needed to ensure the equipment works reliably and compatibly with the complete ZyGATE infrastructure.
5. An intentional radiator shall be designed to ensure that no antenna other than that furnished by the ZyGATE . or its customer shall be used with the GateOne 500A . The use of a permanently attached antenna or of an antenna that uses a unique coupling to the intentional radiator shall be considered sufficient to comply. If the unit becomes broken, the antenna can be replaced by the user, but the use of a standard antenna jack or electrical connector is prohibited. Further, this requirement does not apply to intentional radiators that must be professionally installed, such as perimeter protection systems and some field disturbance sensors, or to other intentional radiators which must be measured at the installation site. However, the installer shall be responsible for ensuring that the proper antenna is employed so that the limits in this part are not exceeded.
6. This standard antenna may be used in a point-to-point application, and possibly may require a tower mount and/or directional antenna. Such use would be applicable in the following uses: data and control signal transmitter located in oil fields; transmitters mounted on trains and train stations; pole-mounted police and/or emergency vehicles.
7. Permanent attachment of the GateOne 500A can be achieved by various means such as factory application of a permanent cement or epoxy to a standard antenna connector. The GateOne 500A will specify the certification application type of adhesive to be used and must confirm that the adhesive will be applied at the factory – prior to shipment.
8. The installer must ensure that the GateOne 500A and antenna is properly installed so as not to exceed the limits for which it has been designed.
9. Compliance is required for special waterproofing procedures, insulation against lightening and other weather conditions.
10. Also requires special mounting brackets for instillation in professional environments.
11. Licensees will be recruited primarily from existing service providers and manufacturers that are already successful in Internet, paging, or mobile phone service industries.
12. ZyGATE. will provide products and services through service providers, its main sales strategies will be to empower service providers and to provide on-going service and support to service providers. Service providers will focus on local markets and offer flexible services to niche markets.
13. Multiple service providers can be started with a relatively low cost of entry. ZyGATE. will
provide licensing companies already in the service industry (such as Internet, paging, or mobile telephone service companies), it will be possible to qualify and license service provides in a short space of time.

14. ZyGATE will provide all starter ingredients (such as prototypes) on a discounted basis to Widenet service providers for smooth transition and integration into existing client bases, authorization, and billing.
15. All equipment will be sold only to ZyGATE qualified network operators that will be purchasing the equipment as a part of an infrastructure to provide services. The intended use and design of the GateOne 500A is for use by utility companies, large telecom corporations to build out or compliment their current infrastructure for radio frequency and telecommunications signaling.

GateOne 500A product types

GateOne 500A is current designed to be configured only for the point-to-point operation mode, one access point (AP) and one access client (AC) are needed. Point to 2 point feature will be available in the near future. When operated in the point-to-two-points mode, one AP and two ACs are needed.

1.2 Physical Features of the GateOne 500A

The GateOne 500A is used for long-range wireless outdoor application. GateOne 500A equips with a robust outdoor weather-proof housing. The key physical features are listed below:

- Outdoor-mounted design minimizes RF cable loss connecting to antenna and thus has outstanding performance in the longer communication distance.
- Power over Ethernet (POE) connection & special antenna alignment kit provide fast installation and easy operation.

1.3 Non-physical Features of the GateOne 500A

.

- **Full Network Management**

Most functions of the GateOne 500A are also software configurable via the WEB interface. The WEB interface is a software that you can access from a PC through the WEB browser.

- **Event Logging**

Built-in message logging for troubleshooting information.

- **Upgrade GateOne Firmware via WEB**

The firmware of the GateOne 500A can be upgraded via the WEB.

1.4 Benefits of the GateOne 500A

- AES/TKIP/WEP protect sensitive data transmission on air.
- MAC & 802.1x based mutual link authentication enhance system privacy
- Outdoor-mounted design minimizes RF cable loss connecting to antenna and thus has outstanding performance in longer communication distance
- High data throughput achieves rapid return on investment for inter-building connection compared to T1 leased line.
- Graded AES/TKIP/WEP security level through WEB server offers easy configuration and usage.
- Power over Ethernet (POE) connection & special antenna alignment kit provide fast installation and easy operation

1.5 Applications of the GateOne 500A

With GateOne 500A Secure Wireless Point to Point Solution, you can extend and enhance your network virtually overnight without natural or man-made barriers to overcome. Easy installation, operation, guaranteed security and outstanding performance in communication distance allow you to quickly provide secure wireless inter-building connection and make GateOne 500A the ideal solution for:

- Internet Service Provider, Cable Operators and Telco to build up inter-building wireless backhaul connection to the point of presence (POP) without paying higher cost and fee for T1 leased line.
- Use in the following applications:
  - Financial banks and brokerage houses sensitive data transmission
  - Government agencies data connection among buildings
  - Central office to branch office(s) connection
  - Education schools and Universities inter-building connection
  - Business companies with multiple dwelling buildings connection
  - Medical hospitals and clinics wireless connection
  - Remote wireless monitoring

1.6 Specifications of the GateOne 500A

Table 1-1 lists the specification of the GateOne 500A.

Table 1-1 Specification of GateOne 500A

System topology	
Point to point (PTP)	1 access point (AP), 1 access client (AC)
Radio	
Frequency range	GateOne 500A:4.9-5.850GHz (5.725-5.850GHz for U.S.A) UNII band
RF modulation	OFDM with BPSK, QPSK, 16QAM, 64QAM
Channel width	500A: 20 MHz
Channel of center frequency	
North America	5725,5745,5765,5785,5805,5825 MHz
Europe	5735,5745,5755,5765,5775,5785,5795,5805,5815,5825,583,5845 MHz(10MHz channel spacing) 5740,5760,5780,5800,5820,5840 (20MHz channel spacing)
Transmit power	0 ~ 20dBm (typical)
Receive sensitivity (PER 8%)	-67 dBm @ 108 Mbps -70 dBm @ 54 Mbps -73 dBm @ 48 Mbps -80 dBm @ 36 Mbps -83 dBm @ 24 Mbps -86 dBm @ 18 Mbps -88 dBm @ 12 Mbps -89 dBm @ 9Mbps -90dBm @ 6 Mbps
Antenna alignment	Built-in diagnostics utility, optional external tool kit through console cable
Networking Features	

Operation mode	Bridge mode (PTP)
Media access control	CSMA/CA
Network protocols	IP, UDP, TCP, ICMP, ARP, IGMP
SECURITY	
System privacy protection	SSID, WEP(64/128 Bits), MAC access control, 802.1x based mutual authentication
Wireless data encryption and authentication	AES/TKIP/WEP
CONFIG. AND MANAGEMENT	
Management and setup	Web/Telnet based management interface
Local console management	System configuration & access control with password protection
Software upgrade	WEB GUI
Mechanical & Operating Features	
Dimension	250(H) × 198(W) × 75(D) mm (not including antenna)
Weight	2050 gm
Operating temperature	-30°C ~ +60°C
Relative humidity	0~ 95% (non-condensing)
Physical interfaces	
Antenna connection	N male RF connector
Network & power connection	8-pin female connector with special water proof
Alignment kit connection	8-pin male connector with special water proof
Antenna connection cable	LMR400 2m, N female/male connectors with special water proof
Alignment kit cable	DB-9 female/8-pin female connectors with special water proof, 2m
Grounding cable	Electric wire with shielded cover, 3m
Electrical Features	
Power consumption (maximum)	15.0 W maximum @ 15 VDC
Network/Power injector	
Power adaptor	INPUT:100~240VAC, 50~60 Hz,OUTPUT:15V DC
Dimension	181mm(W) X 128mm(L) X 36mm(H)
Connectors	PWR (jack), TO LAN (RJ45), TO RADIO (RJ45)
LEDs	PWR,SYS,RSSI,SNR,LAN
Cat. 5 cable	RJ-45/ 8-pin male connectors with special water proof
Cat. 5 cable length	default :20m, optional: 50m/90m
Regulatory Approvals	
Electromagnetic emission	FCC Part 15.247 FCC Part 15.407 EN 301 893 EN 300 328-2 EN 301 489-17
Safety approval	CAN/CSA-C22.2 No 60950, ANSI/UL No.60950, EN 60950, IEC 60950
Installation	
Mast mount kit	Stainless steel for 40~50 mm diameter mast, outdoor
Optional Accessories	
Lightning arrestor	200W power rating

22 dBi flat panel antenna	338 x 338 mm
Antenna alignment tool kit	
Connector	TO RADIO (DB-9 male)
Display	RSSI, SNR
Dimension	95.5 x 59.6 x 26 mm

Chapter 2 Hardware Installation

This chapter explains the physical ports and how to connect the hardware of GateOne.

2.1 Hardware Description

The content of the GateOne 500A are described below.

1. **The outdoor unit**

The outdoor unit has one antenna port, one data/power port and one console port. The antenna port is N-Type female connector used to connect to the omni-directional antenna or to the RF cable then to the flat panel antenna. The data/power port is used to link to the cable from the power injector. When the outdoor unit and the network/power injector are connected together, the outdoor unit is turned on and initialized if the network/power injector in the indoor is also installed successfully. The console port is only used at the initial setup and is used to connect to the antenna alignment kit. The outward appearance of the outdoor unit are shown on Fig.2.1, 2.2 and 2.3.

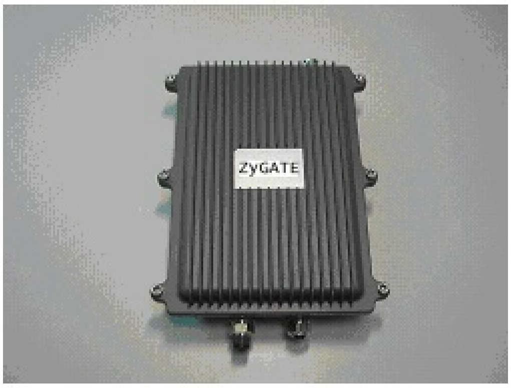


Figure 2-1 **Front view of GateOne 500A**

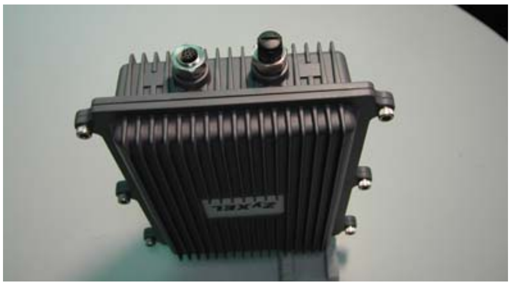


Figure 2-2 **Bottom view of GateOne 500A**

The physical interfaces on the bottom of GateOne 500A is the POE (Power over Ethernet) and RS-232 port. Both connectors are special designed for water-proof. Table 2-1 describes the function of those connectors

Table 2-1 Connectors of bottom

Function	Label	Interface	Description
Signal & Power	🖧	8-pin female connector with special water proof	Connecting to the indoor interface unit supplying the power and signal
Antenna alignment	|0|0|	8-pin male connector with special water proof	Connecting to AK-100 for antenna alignment

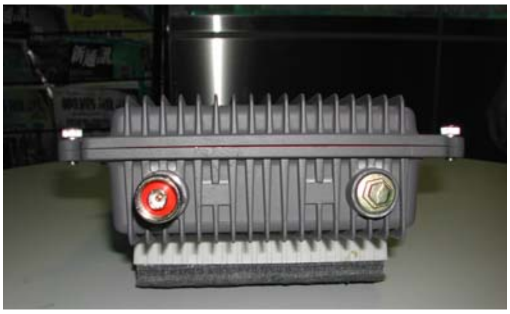


Figure 2-3 **Top view of GateOne 500A**

The major interfaces on top of GateOne 500A is the RF antenna connector with special design for water proof. Table 2-2 describes the antenna connector.

Table 2-2 Antenna connector of the top

Function	Label	Interface	Description
Antenna	Y1	N male RF connector with special water proof	Connecting to the outdoor antenna

2. **Antenna**
   The antenna used for point to point systems is 22 dBi flat panel antenna.

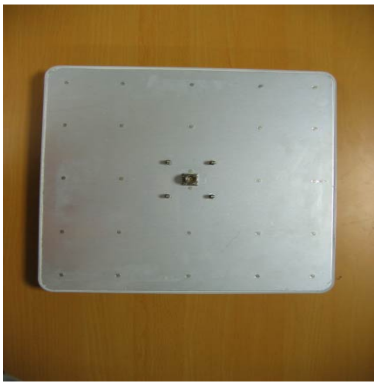


Figure 2-4 **Back view of Flat Panel Antenna**

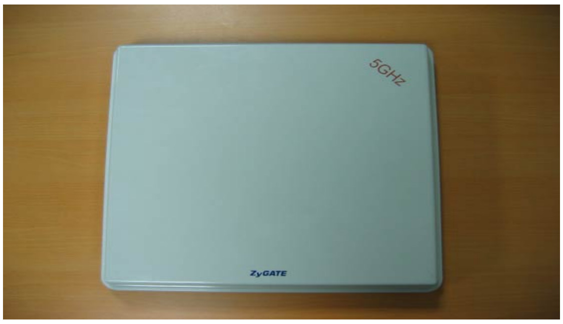


Figure 2-5 **Front view of flat panel antenna**

Besides the antenna types mentioned above, the 26 dBi grid antenna is also available which could be used for longer distance communication for those areas without regulation limitation.

3. **RF cable**
   The RF cable is used to connect the outdoor unit and the flat panel antenna. HDF 400 type RF cable with 2m length is provided. The appearance of the RF cable is shown below.

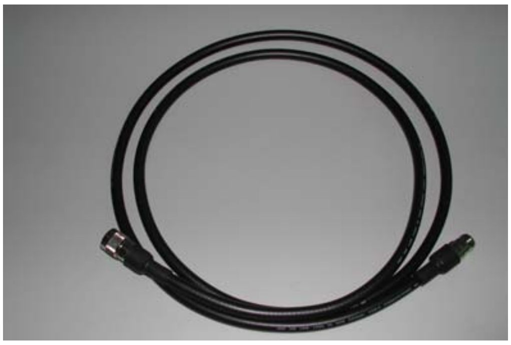


Figure 2-6 **HDF 400 RF cable**

4. **RS-232 cable**
   The RS-232 cable is used to connect the outdoor unit and the antenna alignment kit. The appearance of the RS-232 cable is shown below.

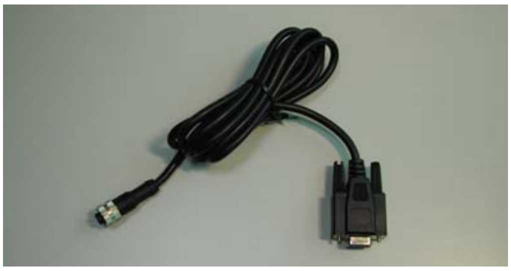


Figure 2-7 **RS-232 console cable**

5. **Cat-5 cable with special connector**
   The Cat-5 cable with special connector has 20m in length. It is used to provide the path to deliver power for the outdoor unit and the data communication. The optional cable length of 50m, and 90m are also available for specified application. The appearance is shown below.

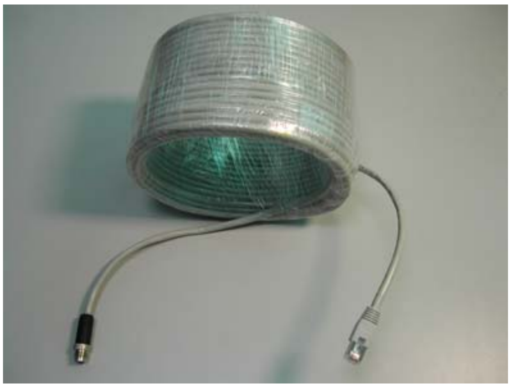


Figure 2-8 **Category 5 cable**

6. **Grounding wire**
   The grounding wire is used to provide the grounding path for the outdoor unit to minimize the impact of lightening and surge. The physical appearance of the grounding wire is shown below.

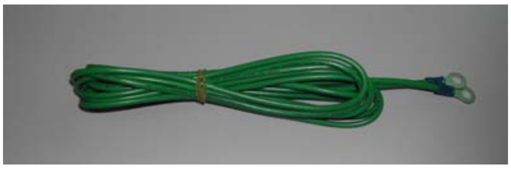


Figure 2-9 **Grounding wire**

7. **Mounting bracket**
The mounting kit is used to provide a good support for the outdoor unit and the flat panel antenna. Please follow the installation procedure to mount the outdoor unit and the flat panel antenna. The contents of the mounting kit are shown below.

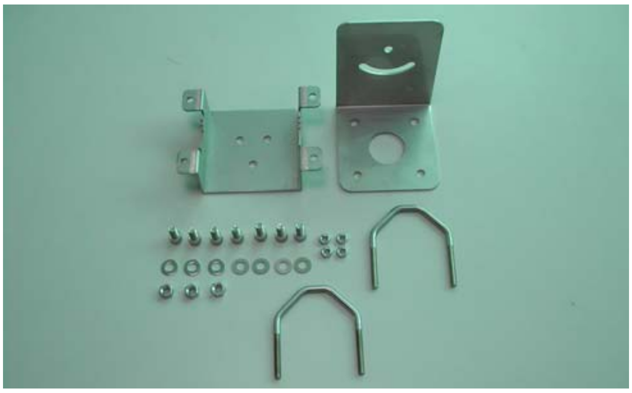


Figure 2-10 The Mounting kit

8. **Network/Power Injector**
The network /power injector is used to combine the data stream and power into one cable. It has three ports. The port named _POWER_ is for 15V power from the switching power adapter. The port named _TO LAN_ is connected the customer premises equipment (CPE) by Cat-5 cable. The port named _TO RADIO_ is connected to the outdoor unit by the cable described in item 5.
The appearance of the network/power injector is shown below.

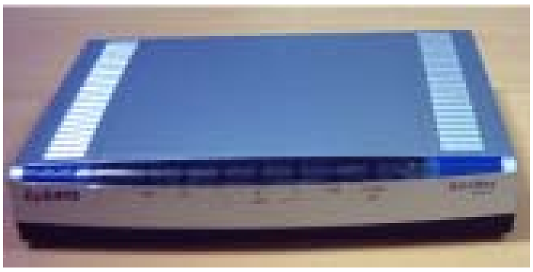


Figure 2-10 **Network/Power Injector**

9. **Antenna Alignment Kit**
Two flat panel antennas of the GateOne 500A should be well aligned before the normal operation. If the antenna alignment is not well done, the received signal strength will be small and the link quality will be not good enough to support high-speed data communication. The antenna alignment kit is connected to the outdoor unit through the RS-232 cable. You should modify the vertical and horizontal angle of the panel antenna according to the signal strength indicated on the AK-100. The outward appearance of the antenna alignment is shown below.

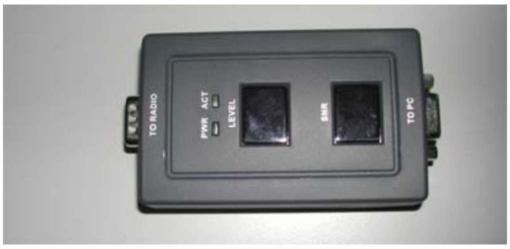


Figure 2-11 **Antenna Alignment Kit (AK-100)**

10. **CAT-5 Straight-through Ethernet cable**
    The CAT-5 STP cable is 2m in length. This cable is used to connect the network/power injector and the CPE. The picture of this cable is shown below.

Figure 2-12 Ethernet Cable

11. **Switching Power Adapter**
    The switching power adapter is to supply the power for the outdoor unit. The input to this adapter is 100~240VAC and the output is 15VDC. The picture is shown below.

Figure 2-13 **Switching Power Adaptor**

2.2 Hardware Installation

1. GateOne 500A Physical Connection

The physical cable connection of the GateOne 500A is shown in the following pictures.

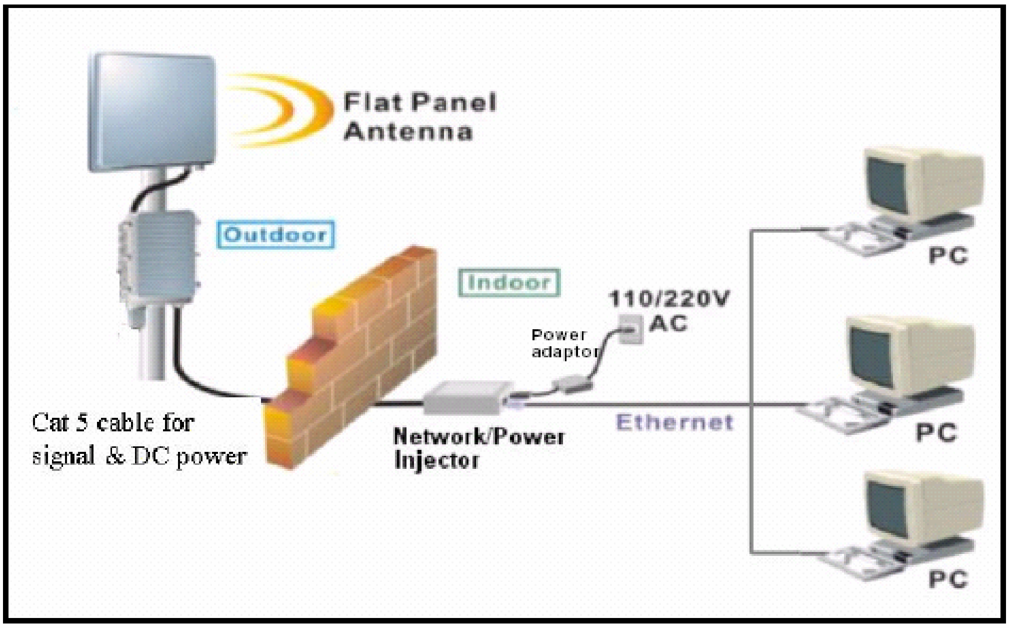


Figure 2-14 **Physical Installation of GateOne 500A with flat panel antenna**

2. **Installation of outdoor unit**

The installation procedures of GateOne 500A is described as below:

(1) Choose an appropriate place for the installation. The path between sites should be clear line-of-sight.

(2) Prepare a mast with a diameter of 40mm~50mm.

(3) Assemble mast mount bracket as shown in the picture below.

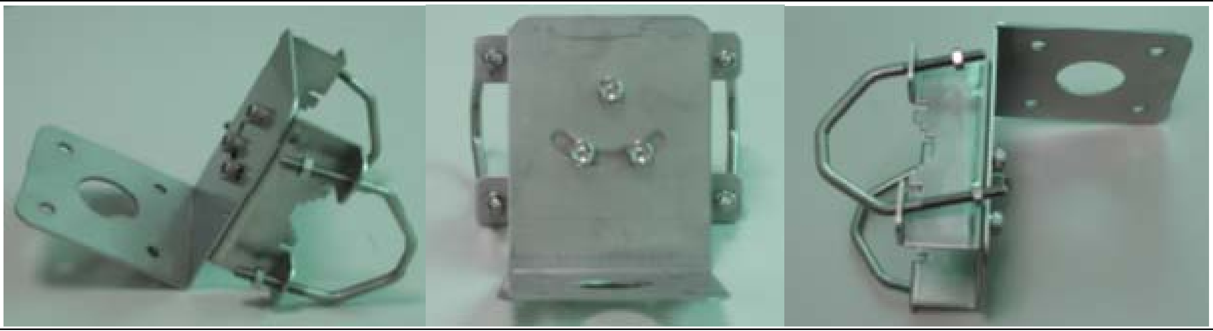


Figure 2-15 **Mounting Bracket Assembly**

(4) Attach the mounting bracket and the grounding wire to the back of the outdoor unit as shown in the picture below

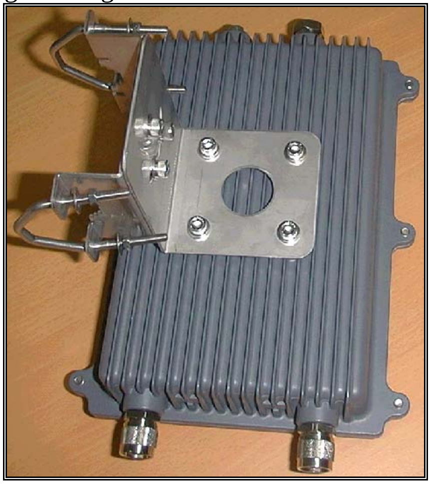


Figure 2-16 **Attach the Mounting Bracket to Outdoor Unit**

(5) Fasten the mounting bracket assembly to install outdoor unit on the mast

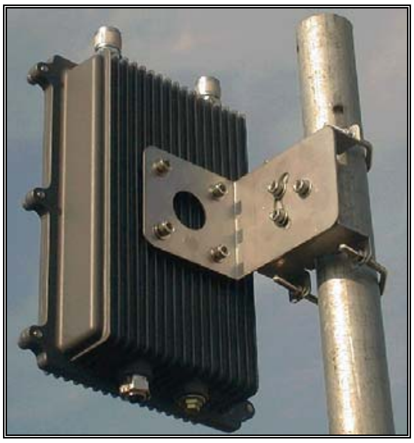


Figure 2-17 **Install Outdoor Unit to the Mast**

(6) Connect the antenna to the N-male connector port labeled Y1 on the top of outdoor unit. For the directional antenna installation, use the HDF 400 RF coaxial cable. The polarization of antenna for both AP and AC should be the same; otherwise, the installation will fail to communicate. At the same time, you have to point the directional antenna to that of the other unit.

Notice: The antenna must be installed by the professional installer to comply with the safety, electrical and radiation standards. The installer should properly configure the output power of transceiver according to related country regulation requirement and per antenna type.

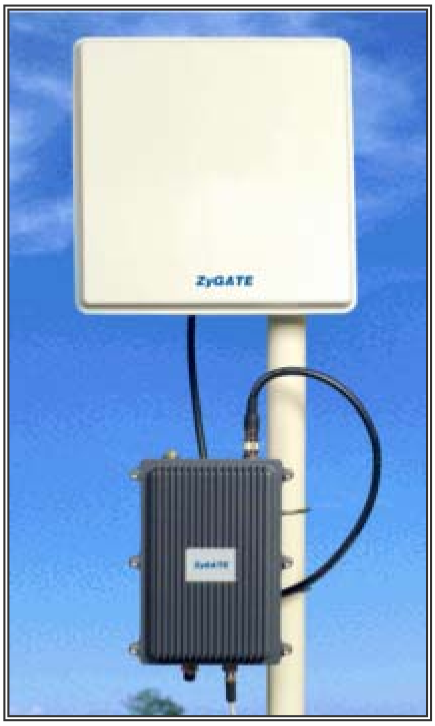


Figure 2-18 **Install Antenna to the Outdoor Unit**

Attach the end of 8-pin male connector of category-5 cable to the 8-pin female connector port labeled 🖧 on the bottom of outdoor unit. Then, the outdoor unit installation is completed.

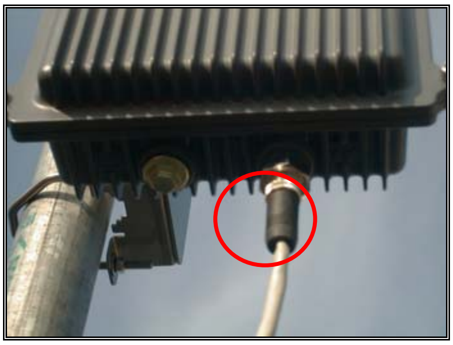


Figure 2-19 **Connect Cat-5 cable to the outdoor unit**

1.1. Indoor Unit Installation

After the outdoor unit installation is completed, you may follow the procedures below to install the indoor unit.

1. Choose an appropriate place for the network/power injector. You might hang it on the wall or just place it on the desk. Connect the other end of category-5 cable to the "**TO RADIO"** RJ-45 connector of network/power injector.
2. Connect one end of Ethernet cable to the "**TO LAN"** RJ-45 port of the network/power injector. Connect the other end of Ethernet cable to the workstation directly or through a switch/hub/router.
3. Connect the power jack of switching power adaptor to the power port labeled as " **POWER"** on the network/power injector.

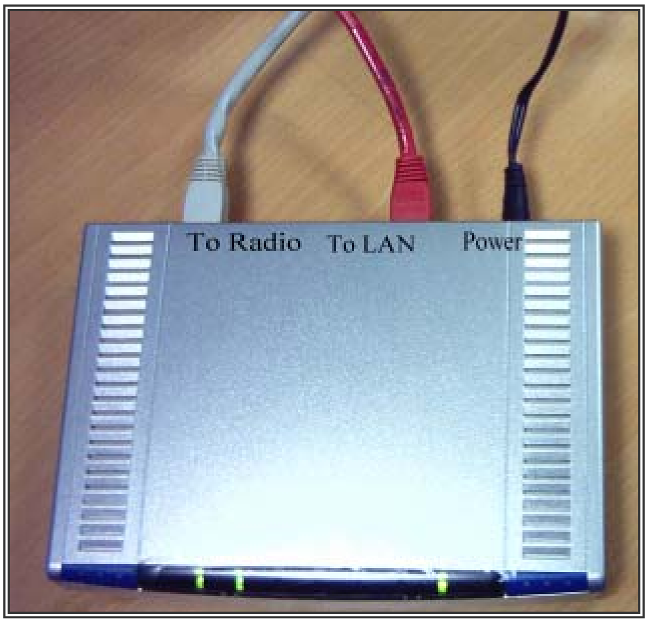


Figure 2-20 **Cable Connections of Network/Power Injector**

1.2. Initializing the GateOne 500A

1. When plugging the switching power adapter into the 110V/220V wall outlet, the LED named **PWR** on the network/power injector will light on.
2. When the power and signal connection to outdoor unit are complete, the **SYS** LED of the network/power injector will light on.

1.3. Antenna Alignment

To maximize the signal quality for GateOne 500A system , you had better align the directional antennas for both AP and AC. To perform the antenna alignment, you can use AK-100 which will show you the signal strength and link quality on its panel. The system data rate will drop to 6Mbps while using AK-100 to align the GateOne 500A. After the alignment is completed, it is required to reboot both AP and AC for regular data rate recovery. To do the alignment, follow the steps as below:

1. Open the cover of the console port labeled ▣ on the bottom of the **access client/access point (AC/AP)** and well reserve the cover.
2. Connect the RS-232 cable to this console port.
3. Connect the other end of the RS-232 cable to the antenna alignment kit AK-100. Adjust the horizontal angle of directional antenna to get the maximum reading in the **LEVEL** and **SNR** display of AK-100. You may also refer to the SNR and RSSI reading shown in the Wireless Information of the WEB server. Please be noticed that If you align the antenna according to the SNR and RSSI reading from the WEB server, the POE and NoteBook PC should be located near the antenna position. Use an extended power outlet to supply the AC source of POE and after the alignment is completed, put the POE back to the indoor position.

Note: The PWR and ACT LED will be ON when connect the AK-100 to the GateOne 500A.

4. Adjust the vertical angle of directional antenna to get the maximum reading in the **LEVEL** and **SNR** display or the **SNR** and **RSSI** reading shown in the Wireless Information of the WEB server.
5. Repeat step 3 and step 4 until achieving the best reading index, then remove the antenna alignment kit.

Note: The AK-100 will beep more rapidly while getting better link quality. It beeps continuously after the best link quality is achieved.

6. Put the console port cover back to the console port.

Note: The signal strength should be well aligned on both the Access client (AC) and Access point (AP).

Chapter 3 Initial Setup

This chapter explains how to perform the initial GateOne 500A setup and gives an overview of WEB menus.

3.1 Network Topology Planning

The GateOne 500A is designed for business companies to build up a secure Inter-building wireless communication system between offices' Ethernet connection. Your GateOne 500A can be applied for Point to Point (PTP) application. The GateOne 500A consists of access point (AP) and access client (AC). The GateOne 500A access point can communicate with one GateOne 500A access client for PTP connection on the air. The network topology for PTP wireless connection is shown below.

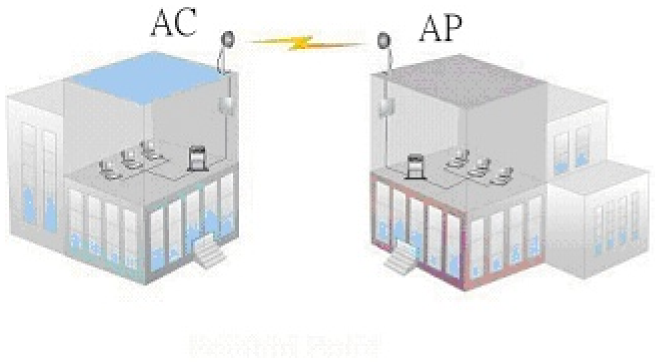


Figure 3-1 **GateOne 500A Networking Topology**

The networking operation mode of GateOne 500A is bridge mode. The bridge mode supports only the PTP connection. You have to appropriately configure your GateOne 500A Access Point and Access Client for normal operation according to your network topology and requirements before physical installation.

3.2 Configure GateOne 500A

This guide shows you the default factory configuration of Gateone 500A and how to configure the Gateone 500A for appropriate operation at the first time. See the User's Guide for configuration details.

3.2.1 Default Configuration

The GateOne 500A is shipped with following factory default configurations:

Table 3-1 Default configuration

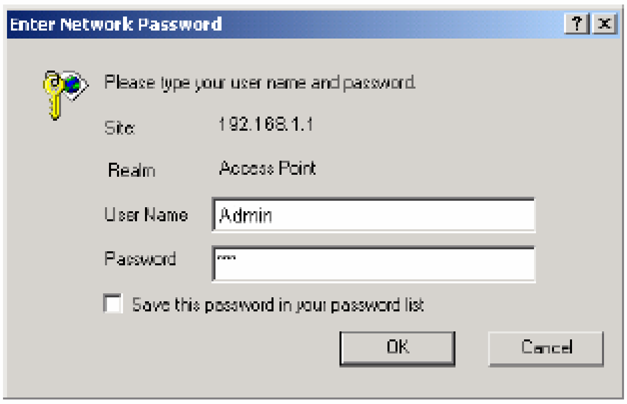
	AP	AC
LAN IP	192.168.1.1	192.168.1.1
Subnet Mask	255.255.255.0	255.255.255.0
Wireless ESSID	Wireless	Wireless
Username/Password	admin/1234	admin/1234

3.2.2 Access the GateOne 500A System WEB Server

There are three tags on left-top of the Web Server System Status window: Status, Configuration and Syslog. Each of the tag contains different functions of the GateOne 500A management.

Follow these steps to setup the channel frequency and SSID using a web browser:

1. Launch a web browser (Netscape Navigator or Internet Explorer are examples of commonly used web browsers).
2. From the HPC, enter the IP address that is assigned to the system as the URL address, for example http://192.168.1.1.
3. A dialog box appears requesting login authorization. When prompted, enter the following information to log in:



Please type your user name and password.

Site 192.168.1.1

Realm Access Point

User Name Admin

Password ****

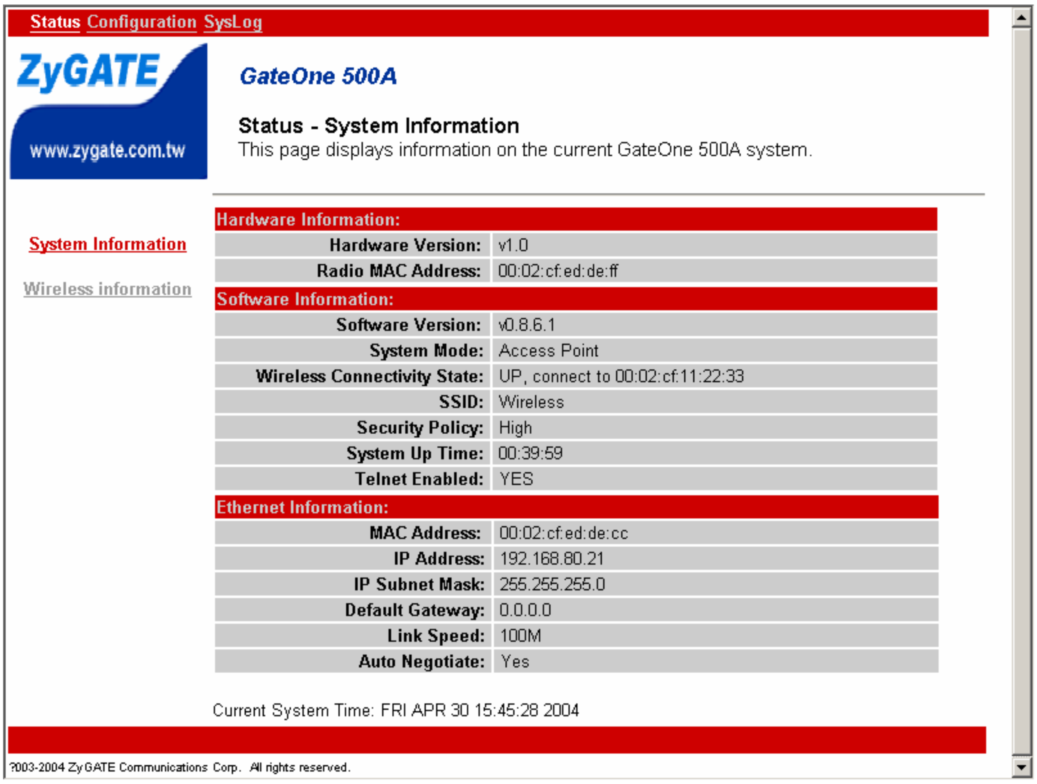
□ Save this password in your password list

Figure 3-2 **Login authorization**

Log in: **admin** (case-sensitive)
Password: 1234
Click OK to complete the login process.

NOTE: The web browser must support frames and Java script must be enabled.

4. The GateOne 500A Web Server System Status window appears as below:



GateOne 500A

Status - System Information

This page displays information on the current GateOne 500A system.

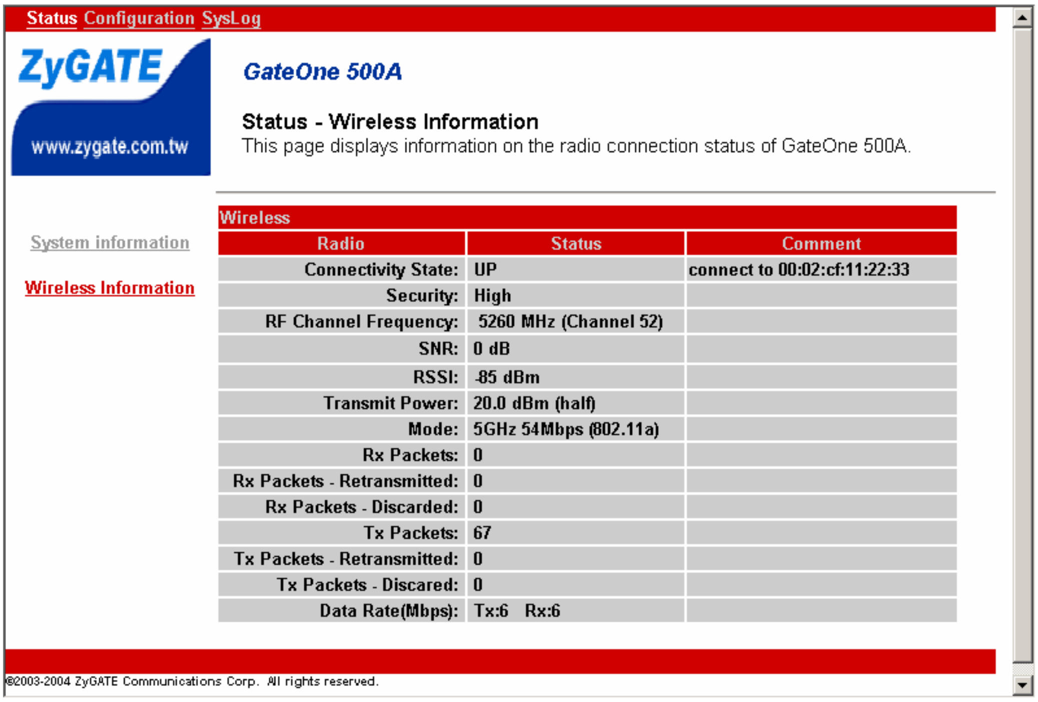
Hardware Information:	
Hardware Version:	v1.0
Radio MAC Address:	00:02:cf:ed:de:ff
Software Information:	
Software Version:	v0.8.6.1
System Mode:	Access Point
Wireless Connectivity State:	UP, connect to 00:02:cf:11:22:33
SSID:	Wireless
Security Policy:	High
System Up Time:	00:39:59
Telnet Enabled:	YES
Ethernet Information:	
MAC Address:	00:02:cf:ed:de:cc
IP Address:	192.168.80.21
IP Subnet Mask:	255.255.255.0
Default Gateway:	0.0.0.0
Link Speed:	100M
Auto Negotiate:	Yes

Current System Time: FRI APR 30 15:45:28 2004

?003-2004 ZyGATE Communications Corp. All rights reserved.

Figure 3-3 **System Status window**

5. Press the Wireless Information, then current Radio Status will be catched.



GateOne 500A

Status - Wireless Information

This page displays information on the radio connection status of GateOne 500A.

Wireless

Radio	Status	Comment
Connectivity State:	UP	connect to 00:02:cf:11:22:33
Security:	High	
RF Channel Frequency:	5260 MHz (Channel 52)	
SNR:	0 dB	
RSSI:	-85 dBm	
Transmit Power:	20.0 dBm (half)	
Mode:	5GHz 54Mbps (802.11a)	
Rx Packets:	0	
Rx Packets - Retransmitted:	0	
Rx Packets - Discarded:	0	
Tx Packets:	67	
Tx Packets - Retransmitted:	0	
Tx Packets - Discared:	0	
Data Rate(Mbps):	Tx:6 Rx:6	

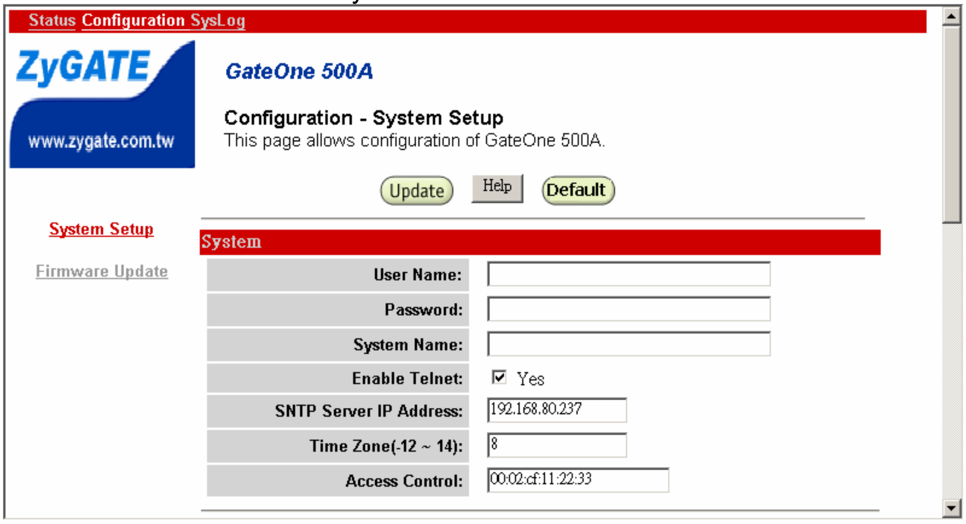
Figure 3-4 **Wireless Information**

3.2.3 System Configuration

The web server windows allow you to setup the configuration information for the AP. The web server provides functions for system setup and firmware updates by clicking the “ Configuration” tag on left-top of the WEB window. To access any of these system configuration screens, click on the desired hotlink from the navigation bar in the “Configuration” screen.

3.2.4 Working with Configuration Windows – System Setup

The Web Server configuration windows provide a user-friendly interface to aid in quick configuration of the system. After making any additions or changes to any configuration window, update the configuration file to save the changes. The new configuration is not in effect until the system reboots.



GateOne 500A

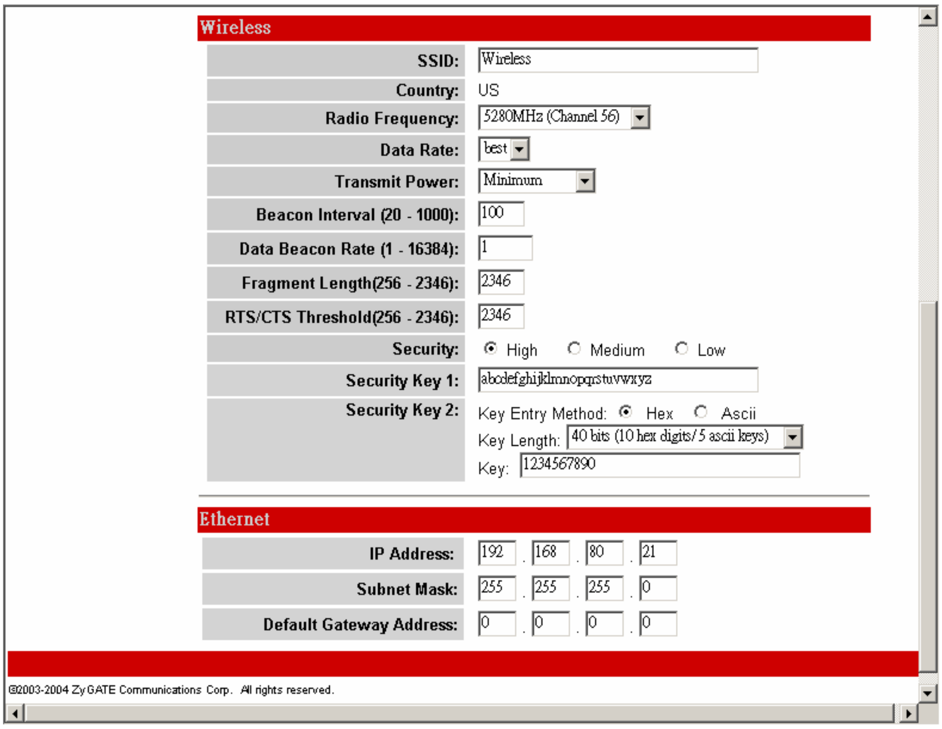
Configuration - System Setup

This page allows configuration of GateOne 500A.

System

User Name:	
Password:	
System Name:	
Enable Telnet:	☑ Yes
SNTP Server IP Address:	192.168.80.237
Time Zone(-12 ~ 14):	8
Access Control:	00:02:cf:11:22:33

Figure 3-5 **System Setup-configuration update**



Wireless

SSID:	Wireless
Country:	US
Radio Frequency:	5280MHz (Channel 56)
Data Rate:	best
Transmit Power:	Minimum
Beacon Interval (20 - 1000):	100
Data Beacon Rate (1 - 16384):	1
Fragment Length(256 - 2346):	2346
RTS/CTS Threshold(256 - 2346):	2346
Security:	● High ○ Medium ○ Low
Security Key 1:	abcdefghijklmnopqrstuvwxyz
Security Key 2:	Key Entry Method: ● Hex ○ Ascii Key Length: 40 bits (10 hex digits/ 5 ascii keys) Key: 1234567890

Ethernet

IP Address:	192 . 168 . 80 . 21
Subnet Mask:	255 . 255 . 255 . 0
Default Gateway Address:	0 . 0 . 0 . 0

©2003-2004 ZyGATE Communications Corp. All rights reserved.

Figure 3-6 **System Setup-Wireless**

To update configuration files:

1. Enter the configuration updates or changes in the appropriate configuration fields.
2. Click Update. Update After click Update, there will appear red string alarm to let you press the REBOOT AP to reboot system to make the changes effective.
3. Click Reboot AP to make the changes effective. REBOOT

The web server loses connectivity with the Web Server as the AP reboots. To reestablish the connection with the Web Server, wait until the AP has completed rebooting and navigate to the Web Server to resume

System Configuration	Description
User Name	Specifies the user name.
Password	Specifies the password.
Telnet Enable	Use the checkbox to allow telneting into the AP.
Access Control	Specifies the AC's MAC address allowed to join.

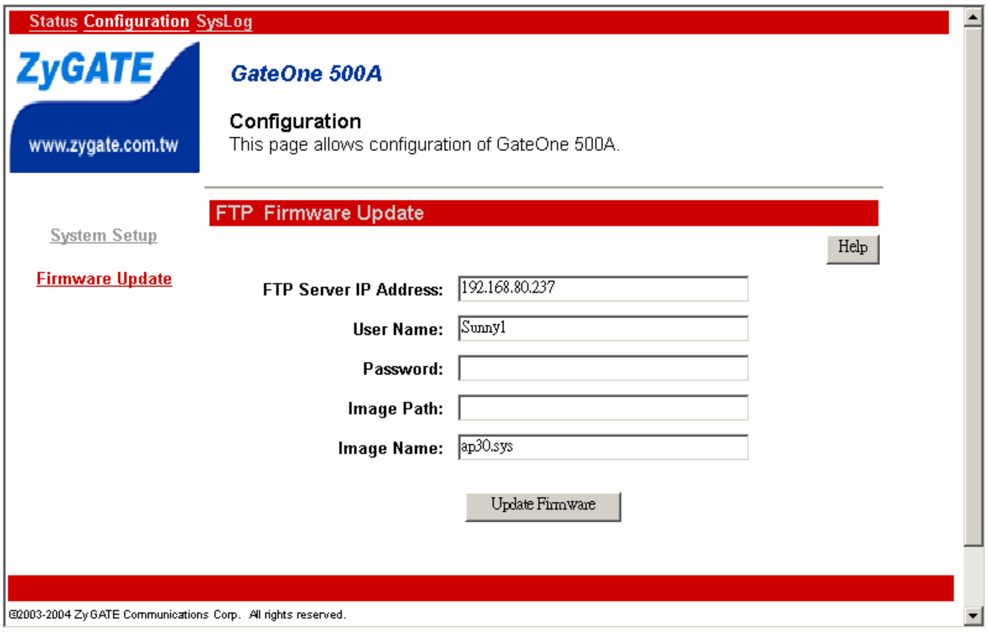
Wireless Configuration	Description
SSID	Identification of the AP. Enter a number or address between 1 and 32 characters in length that the AC is associating with. Use the System Name field to uniquely identify each AP..
Radio Frequency	Select the desired frequency of operation from the drop-down menu, or choose SmartSelect. The radio frequencies that appear in the Radio Channel drop-down menu are dependent on the wireless mode selection. Select "SmartSelect" to automatically search through the frequency list to find a used or less congested channel.
Data Rate	Specifies rate of data transmission. Select the desired rate from the drop-down menu. The Best selection will adapt the rate to the best available.

Transmit Power	Specifies the level of transmit power. Choose the value of the transmit power from the dropdown menu. Decrease the transmit power if more than one AP is co-located using the same channel frequency.
Beacon Interval	Specifies the beacon interval value. Enter a value between 20 and 1000.
Data Beacon Rate	Specifies the Data Beacon Rate. Enter a value between 1 and 16384 that specifies the delivery traffic indication message (DTIM).
Fragment Length	The fragment length is fixed at 2346.
RTS/CTS Threshold	Specifies the value of the RTS/CTS threshold. Enter a value between 256 and 2346.
Country	Display country name; it's related to channel frequency base.
Security	Specifies the security mode in High, Medium or Low security protection.
Security Key 1	Specifies key setting related to security policy
Security Key 2	Specifies key setting related to security policy. You can select input data type and key length. Input data type: Hexadecimal or ASCII.

Ethernet Configuration	Description
LAN IP Address	Specifies the IP address of the AP.
Subnet Mask	Specifies the subnet mask for the AP.
Default Gateway Address	Specifies the default gateway for the AP.

3.2.5 System Configuration Windows - Software Download

The Firmware Update configuration window allows viewing of the FTP location of new firmware. The default values for the FTP Host Name, User Name, Password, Image Path, Image Name appear in the window. To access the Firmware Update window, click on Update button. The Firmware Update configuration window appears as following.


Status Configuration SysLog
ZyGATE
www.zygate.com.tw
System Setup
Firmware Update
Help
Update Firmware
©2003-2004 ZyGATE Communications Corp. All rights reserved.

GateOne 500A

Configuration

This page allows configuration of GateOne 500A.

FTP Firmware Update

FTP Server IP Address: 192.168.80.237

User Name: Sunny1

Password:

Image Path:

Image Name: ap30.sys

Figure 3-7 **Software Download Windows**

The AP uses the file transfer protocol (FTP) to download the Operating image from the HPC. An FTP server utility is required to perform the data transfer between the AP and HPC.

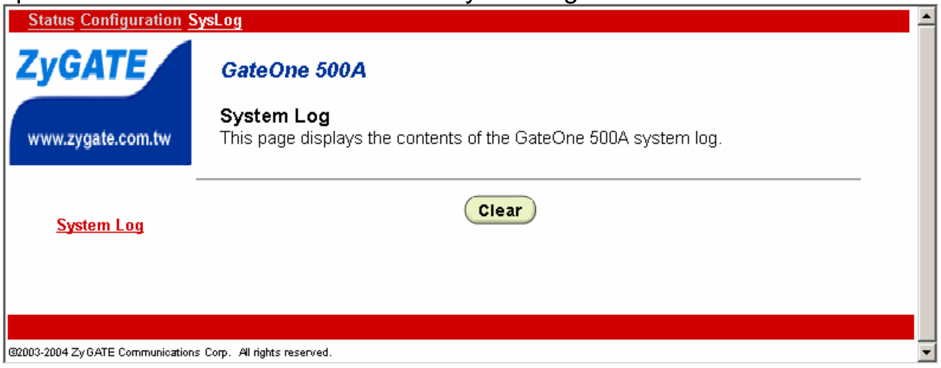
To enable firmware updates:

1. Enter the host PC's IP address, User Name, Password, Image Path, and Image Name data-entry fields.
2. Click Update Firmware to store the new firmware changes.

Note: The red reminders only appear if you update setting in Configuration/System Setup page.

3.2.6 System Log Windows

The System Log window logs system events for detail descriptions of system status log. This is very useful to track system. It shows important successful states and critical system logs.


Status Configuration SysLog
ZyGATE
www.zygate.com.tw
GateOne 500A
System Log
Clear
©2003-2004 ZyGATE Communications Corp. All rights reserved.

System Log

This page displays the contents of the GateOne 500A system log.

Figure 3-8 **System Log Windows**

Chapter 4 CLI commands

How to use CLI commands to get or set system information , frequency, and other different parameters, following pages give you detailed information for each command.
Use CLI commands to display the current system configuration, you may also set the system parameters to configure your system. Contents of the CLI commands are listed as below:.

Wlan State
Radio Frequency
Auto Channel Select
Data Rate
Antenna
Login Username
Name Server IP Address
Name Server Domain Suffix
SSID
SSID Suppress Mode
System Name
Beacon Interval
DTIM
RTS/CTS Threshold
Data Rate
IP Address
IP Mask
Host IP Address
Gateway IP Address
SNTP/NTP Server IP Address
Time Zone
HW Transmit Retry Limit
Transmit Power
Current Transmit Output Power
Encryption
Cipher Selection
Authentication Type
Default Transmit Key
Shared Key
Access Check
Aging Interval
Key Entry Method
Group Key Update Interval
Keysource
Telnet
Telnet Timeout

To display/modify the function of auto channel selection

Use the **get/set autochannelselect** command to get status or set functions of the auto channel selection. Examples are shown as below:

```
-> get autochannelselect
Auto Channel Select: Enabled

-> set autochannelselect disabled
Auto Channel Select: Disabled

-> set autochannelselect enabled
Auto Channel Select: Enabled
```

To display system configuration

Use the **get config** command to display the system configuration. For example:

```
-> get config
```

To display/modify frequency radio channel

Use the **get/set frequency** command to display or modify the radio channel. For example:

```
-> get frequency
Radio Frequency: 5250 MHz (IEEE 50)
-> set frequency 5250
```

```
Radio Frequency: 5250 MHz (IEEE 50)
```

To display/modify gateway IP address

Use the **get/set gateway** command to display or modify the gateway IP address.

```
-> get gateway
Gateway IP Address:
-> set gateway 192.168.0.1
Gateway IP Address: 192.168.0.1
```

To display hardware

Use the **get hardware** command to display the vendor ID and chip (MAC, PHY and analog) revisions.

```
-> get hardware
PCI Vendor ID: 0x168c, Device ID: 0x207, Sub Vendor ID: 04, Sub Device
ID: 0
WLAN revisions: mac 3.0 phy 2.0 analog 1.6
```

To display platform hardware version

Use the **get hardware** command to display the vendor ID and chip (MAC, PHY and analog) revisions.

```
-> get hw_ver
GateOne System Hardware Platform: 1.00a
```

To display/modify IP address

Use the **get/set ipaddr** command to display or modify the access point IP address.

```
-> get ipaddr
IP Address: 192.168.1.20
-> set ipaddr 192.168.1.40
IP Address: 192.168.1.40
```

To display/modify IP subnet mask

Use the get/set ipmask command to display or modify the access point IP subnet mask.

```
-> get ipmask
IP Subnet Mask: 255.255.255.0
-> set ipmask 255.255.0.0
IP Subnet Mask: 255.255.0.0
```

To display security policy

Use the **set security** command to view or modify the authentication type.

```
-> get security
Security Policy: High.
-> set security medium
Security Policy: Medium
```

To modify security policy

Use the **set security** command to view or modify the authentication type.

```
-> set security high
Security Policy: High.
-> set security medium
Security Policy: Medium
-> set security low
Security Policy: Low
```

Security Key Configuration

The CLI key commands enable configuration security keys. The keys must be input as hexadecimal digits. Choose between 40-bit, 104-bit, or 128-bit encryption keys. For 40-bit encryption, the key string is 10 characters long. For 104-bit encryption, the key string is 26 characters long. For 128-bit encryption, the key string is 32 characters long. The **get key** command will return the original key. Use **get/set key** command to display or modify key configuration. For examples:

```
get key Display keys
set key 1 [40|104|128] keystring Set key syntax
```

```
-> set key 1 40 aabbccddee
Shared Key 1, size 40: aabbccddee
-> set passphrase
Old PassPhrase: 12345678
New Passphrase: a0b1c2d3
```

Note: with mapping into WEB interface, cli command "set passphrase" actually means "Security Key 1" in WEB configuration page; cli command "set key 1" is related to "Security Key 2" in WEB configuration page.

System Configuration

Following table lists the steps to configure the system. Remember to reboot the system to make configuration works.

Command	Description
set factory	Sets the AP to factory defaults.
set ipaddr <*IP Address*>	Sets the IP address of the AP ethernet interface
set ipmask 255.0.0.0	Sets the subnet mask for the AP ethernet interface
set autochannel disable	Disables autochannel selection. (optional)
set channel <*channel number*>	Selects a channel. This command is only needed if autochannel selection is disabled. (optional)
set ssid <*desired SSID*>	Sets the desired SSID.
set system <*System Name*>	Sets the desired system name. (optional)
set key 1 40 1111111111	Sets a key in slot 1. This is not used, but it must be set.
set key 1 default	Sets the key as the default key. This key is not used.
set security high	Enables encryption on the AP.
reboot	Reboots the AP for the configuration to take effect.

Display/Modify Key Entry Method

Use the **get/set keyentrymethod** command to display or modify the method of entering encryption keys; either ASCII or hexadecimal.

```
-> get keyentrymethod
Key Entry Method: ASCII text
-> set keyentrymethod hex
Key Entry Method: Hexadecimal - Keys 0-9, A-F
-> set keyentrymethod ascii - All keyboard characters supported
Key Entry Method: ASCII text
```

To display/modify login user name

Use the **get/set login** command to display or modify the login user name. The login user name is a text string of up to 32 characters long. Control characters are not permitted.

```
-> get login
Login Username:
-> set login Foobar
Login Username: Foobar
-> get login
Login Username: Foobar
```

To modify login password

Use the **set password** command to modify the login password. Type the new password twice to confirm the use of the new password. The password is a text string of up to 32 characters long. Control characters are not permitted.

```
-> set password
Password: *******
Type password again to confirm: *******
```

```
Password confirmed
```

To display/modify power

Use the **get/set power** command set or modify the transmit power setting. Set the transmit power for full, half (-3 dBm), quarter (-6 dBm), eighth (-9 dBm), or minimum (0 dBm). Use this command to decrease the transmit power, and thereby reducing the range of the radio when more than one AP with the same channel frequency are located close together.

```
-> get power
Transmit Power: full
-> set power half
Transmit Power: half
-> set power quarter
Transmit Power: quarter
-> set power eighth
Transmit Power: eighth
-> set power min
Transmit Power: min
```

To display/modify data rate

Use the **get/set rate** command to display or modify the data rate. Select one of the following data rates: 6, 9, 12, 18, 24, 36, 48, 54, and best, respectively. The first 8 data rates are fixed rates and the last one is a variable rate. When choosing the best rate, the AP attempts to deliver unicast data packets at the highest possible optimum data rate. If there are obstacles or interference, the AP automatically steps down to an optimum data rate that allows for reliable data transmission. In addition, the optimum data rate is adjusted periodically by the AP, based on past performance of the data transmissions at different neighboring data rates.

```
-> get rate
Data Rate: best
-> set rate 36
Data Rate: 36
```

To display/modify SNTP Server

Use the **get sntpserver** command to display or modify the SNTP/NTP server IP address.

```
-> get sntpserver
SNTP/NTP Server IP address:
-> set sntpserver 192.168.1.20
SNTP/NTP Server IP address: 192.168.1.20
```

To display station status

Use the **get station** command to display station information and status.

```
-> get station
MacAddr: 00:03:7f:00:00:01, State: associated, AID: 1
Authentication Type: Open System
Encryption: ON, slot 4 shared[1] 40b key: aabbccddee
Power Save Mode: OFF
Rx Data Rate: 36, RxSignalStrength: 46, AckSignalStrength: 45
MSDU Data Mcast Mgmt Ctrl Errors
Rx 70 68 68 2 0 0
Tx 227 225 0 2 0 0
```

To display/modify SSID

Use the **get/set ssid** command to display or modify the SSID. The SSID is a text string of up to 32 characters in length. Control characters are not allowed.

```
-> get ssid
SSID: ZyGATE 802.11a Wireless Network
-> set ssid Internet Cafe Access Point
SSID: Internet Cafe Access Point
```

To display/modify SSID Suppress

Use the **get/set ssidsuppress** command to display or modify the SSID suppress mode. When enable, the SSID in beacons are not transmitted and only STAs with knowledge of an AP’s SSID are able to associate with the AP.

```
-> get ssidsuppress
SSID Suppress Mode: Disabled
-> set ssidsuppress enable
SSID Suppress Mode: Enabled
-> set ssidsuppress disable
SSID Suppress Mode: Disabled
```

To display/modify System Name

Use the **get/set systemname** command to display or modify the access point system name. The system name is the name of the access point, and is a text string of up to 32 characters in length. Control characters are not allowed.

```
-> get systemname
System Name:
-> set systemname My AP
System Name: My AP
My AP ->
```

To display/modify Telnet

Use the **get/set telnet** command to enable or disable telnet access to the AP.

```
-> get telnet
Telnet Access: Enabled
-> set telnet disable
Telnet Access: Disabled
-> set telnet enable
Telnet Access: Enabled
```

To display/modify Timeout

Use the **get/set timeout** command to display or modify the telnet timeout.

```
-> get timeout
Telnet Timeout:
-> set timeout
Telnet Timeout:
```

To display/modify Time Zone

Use the **get/set tzone** command to display or modify the time zone setting.

```
-> get tzone
SNTP/NTP Time Zone
-> set tzone
```

To display elapsed time

Use the **get uptime** command to To display the elapsed time the AP has been up and running.

```
-> get uptime
AP Uptime -- Day 0, 15:32:29
```

To display time and date

Use the **timeofday** command to to display the current time and date.. This command allows the AP to use the SNTP protocol to get the current time from the SNTP/NTP server. First set up the IP address of the SNTP/NTP server before using this command. If no time zone is defined, the GMT time is returned else local time for the specified time zone is returned. Use “set tzone” to set the local time zone. For example, use “set tzone —8” to set the time zone for the west coast. Once time zone is defined, the adjusted daylight saving local time of the time zone is returned. The daylight saving time applies only to the United States.

```
-> time
SNTP/NTP Server is not configured.
Use "set sntpServer" to configure the SNTP server IP Address
-> set sntpserver 129.6.15.28
SNTP/NTP Server IP Address: 129.6.15.28
```

```
SNTP/NTP Server returns GMT time. Use "set tzone" to set up your local
time zone
-> get sntpserver
SNTP/NTP Server IP Address: 129.6.15.28
-> time
THU FEB 23 01:55:35 2003 GMT
-> set tzone -8
SNTP/NTP Time Zone: -8
-> time
WED FEB 22 17:55:57 2003
```

To display software version

Use the **version** command to To display the version number of the current software.

```
-> version
version:0.9.0.1
Feb 19 2003 00:15:45
```

Chapter 5 Glossary of Terms

10BaseT	The 10-Mbps baseband Ethernet specification that uses two pairs of twisted-pair cabling (Category 3 or 5): one pair for transmitting data and the other for receiving data.
ARP	Address Resolution Protocol is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.
Authenticity	Proof that the information came from the person or location that reportedly sent it. One example of authenticating software is through digital signatures.
Back Door	A deliberately planned security breach in a program. Back doors allow special access to a computer or program. Sometimes back doors can be exploited and allow a cracker unauthorized access to data.
Backbone	A high-speed line or series of connections that forms a major pathway within a network.
BackOrifice	BackOrifice is a remote administration tool which allows a user to control a computer across a TCP/IP connection using a simple console or GUI application. BackOrifice is a potentially disastrous Trojan horse since it can provide the user unlimited access to a system.
Bandwidth	This is the capacity on a link usually measured in bits-per-second (bps).
Bit	(Binary Digit) -- A single digit number in base-2, in other words, either a 1 or a zero. The smallest unit of computerized data.
Brute Force Hacking	A technique used to find passwords or encryption keys. Force Hacking involves trying every possible combination of letters, numbers, etc. until the code is broken.
Byte	A set of bits that represent a single character. There are 8 bits in a Byte.
Camping Out	Staying in a "safe" place once a hacker has broken into a system. The term can be used with a physical location, electronic reference, or an entry point for future attacks.
Channel	A specific frequency and bandwidth combination. In the present context, it means TV channels for television services and downstream data for cable modems.
CHAP	Challenge Handshake Authentication Protocol is an alternative protocol that avoids sending passwords over the wire by using a challenge/response technique.
Cipher Text	Text that has been scrambled or encrypted so that it cannot be read without deciphering it. See Encryption
Client	A software program that is used to contact and obtain data from a Server software program on another computer. Each Client program is designed to work with one or more specific kinds of Server programs, and each Server requires a specific kind of Client. A Web Browser is a specific kind of Client.
Cookie	A string of characters saved by a web browser on the user's hard disk. Many web pages send cookies to track specific user information. Cookies can be used to retain information as the user browses a web site. For example, cookies are used to 'remember' the items a shopper may have in a shopping cart.
Countermeasure s	Techniques, programs, or other tools that can protect your computer against threats.
Cracker	Another term for hackers. Generally, the term cracker refers specifically to a person who maliciously attempts to break encryption, software locks, or network security.
Cracker Tools	Programs used to break into computers. Cracker tools are widely distributed on the Internet. They include password crackers, Trojans, viruses, war-dialers, and worms.
Cracking	The act of breaking into computers or cracking encryptions.

Crossover Ethernet cable	A cable that wires a pin to its opposite pin, for example, RX+ is wired to TX+. This cable connects two similar devices, for example, two data terminal equipment (DTE) or data communications equipment (DCE) devices.
Cryptoanalysis	The act of analyzing (or breaking into) secure documents or systems that are protected with encryption.
Decryption	The act of restoring an encrypted file to its original state.
Denial of Service	Act of preventing customers, users, clients or other machines from accessing data on a computer. This is usually accomplished by interrupting or overwhelming the computer with bad or excessive information requests.
DHCP	Dynamic Host Configuration Protocol automatically assigns IP addresses to clients when they log on. DHCP centralizes IP address management on central computers that run the DHCP server program. DHCP leases addresses for a period of time which means that addresses are made available to assign to other systems.
Digital Signature	Digital code that authenticates whomever signed the document or software. Software, messages, Email, and other electronic documents can be signed electronically so that they cannot be altered by anyone else. If someone alters a signed document, the signature is no longer valid. Digital signatures are created when someone generates a hash from a message, then encrypts and sends both the hash and the message to the intended recipient. The recipient decrypts the hash and original message, makes a new hash on the message itself, and compares the new hash with the old one. If the hashes are the same, the recipient knows that the message has not been changed. Also see Public-key encryption.
DNS	Domain Name System. A database of domain names and their IP addresses. DNS is the primary naming system for many distributed networks, including the Internet.
Domain Name	The unique name that identifies an Internet site. Domain Names always have 2 or more parts, separated by dots. The part on the left is the most specific, and the part on the right is the most general.
DRAM	Dynamic RAM that stores information in capacitors that must be refreshed periodically.
DTE	Originally, the DTE (data terminal equipment) meant a dumb terminal or printer, but today it is a computer, or a bridge or router that interconnects local area networks.
EMI	ElectroMagnetic Interference. The interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels.
Encryption	The act of substituting numbers and characters in a file so that the file is unreadable until it is decrypted. Encryption is usually done using a mathematical formula that determines how the file is decrypted.
Ethernet	A very common method of networking computers in a LAN. There are a number of adaptations to the IEEE 802.3 Ethernet standard, including adaptations with data rates of 10 Mbits/sec and 100 Mbits/sec over coaxial cable, twisted-pair cable, and fiber-optic cable. The latest version of Ethernet, Gigabit Ethernet, has a data rate of 1 Gbit/sec.
Events	These are network activities. Some activities are direct attacks on your system, while others might be depending on the circumstances. Therefore, any activity, regardless of severity is called an event. An event may or may not be a direct attack on your system.
FCC	The FCC (Federal Communications Commission) is in charge of allocating the electromagnetic spectrum and thus the bandwidth of various communication systems.
Firewall	A hardware or software "wall" that restricts access in and out of a network. Firewalls are most often used to separate an internal LAN or WAN from the Internet.

Flash memory	The nonvolatile storage that can be electrically erased and reprogrammed so that data can be stored, booted, and rewritten as necessary.
FTP	File Transfer Protocol is an Internet file transfer service that operates on the Internet and over TCP/IP networks. FTP is basically a client/server protocol in which a system running the FTP server accepts commands from a system running an FTP client. The service allows users to send commands to the server for uploading and downloading files. FTP is popular on the Internet because it allows for speedy transfer of large files between two systems.
Gateway	A gateway is a computer system or other device that acts as a translator between two systems that do not use the same communication protocols, data formatting structures, languages, and/or architecture.
Hacker	Generally, a hacker is anyone who enjoys experimenting with technology including computers and networks. Not all hackers are criminals breaking into systems. Some are legitimate users and hobbyists. Nevertheless, some are dedicated criminals or vandals.
HDLC	HDLC (High-level Data Link Control) is a bit-oriented (the data is monitored bit by bit), link layer protocol for the transmission of data over synchronous networks.
Host	Any computer on a network that is a repository for services available to other computers on the network. It is quite common to have one host machine provide several services, such as WWW and USENET.
HTTP	Hyper Text Transfer Protocol. The most common protocol used on the Internet. HTTP is the primary protocol used for web sites and web browsers. It is also prone to certain kinds of attacks.
IANA	Internet Assigned Number Authority acts as the clearinghouse to assign and coordinate the use of numerous Internet protocol parameters such as Internet addresses, domain names, protocol numbers, and more. The IANA Web site is at http://www.isi.edu/iana.
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and are not directly apparent to the application user.
Integrity	Proof that the data is the same as originally intended. Unauthorized software or people have not altered the original information.
internet	(Lower case i) Any time you connect 2 or more networks together, you have an internet.
Internet	(Upper case I) The vast collection of inter-connected networks that all use the TCP/IP protocols and that evolved from the ARPANET of the late 60’s and early 70’s. The Internet now (July 1995) connects roughly 60,000 independent networks into a vast global internet
Internet Worm	See Worm.
Intranet	A private network inside a company or organization that uses the same kinds of software that you would find on the public Internet, but that is only for internal use.
Intruder	Person or software interested in breaking computer security to access, modify, or damage data. Also see Cracker.
IP	Internet Protocol, is the underlying protocol for routing packets on the Internet and other TCP/IP-based networks.
IPCP (PPP)	IP Control Protocol allows changes to IP parameters such as the IP address.
IPX	Internetwork Packet eXchange The native NetWare internetworking protocol is IPX (Internetwork Packet Exchange). Like IP (Internet Protocol), IPX is an internetworking protocol that provides datagram services.
IRC	Internet Relay Chat. IRC was developed in the late 1980s as a way for multiple users on a system to “chat” over the network. Today IRC is a very popular way to “talk” in real time with other people on the Internet. However, IRC is also one avenue hackers use to get information from you about your system and your company. Moreover, IRC sessions are prone to numerous attacks that while not

	dangerous can cause your system to crash.
ISP	Internet Service Providers provide connections into the Internet for home users and businesses. There are local, regional, national, and global ISPs. You can think of local ISPs as the gatekeepers into the Internet.
LAN	Local Area Network is a shared communication system to which many computers are attached. A LAN, as its name implies, is limited to a local area. This has to do more with the electrical characteristics of the medium than the fact that many early LANs were designed for departments, although the latter accurately describes a LAN as well. LANs have different topologies, the most common being the linear bus and the star configuration.
Linux	A version of the UNIX operating system designed to run on IBM Compatible computers.
Logic Bomb	A virus that only activates itself when certain conditions are met. Logic bombs usually damage files or cause other serious problems when they are activated.
MAC	On a local area network (LAN) or other network, the MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address.) The MAC layer frames data for transmission over the network, then passes the frame to the physical layer interface where it is transmitted as a stream of bits.
Name Resolution	The allocation of an IP address to a host name. See DNS
NAT	Network Address Translation is the translation of an Internet Protocol address used within one network to a different IP address known within another network - see also SUA.
NDIS	Network Driver Interface Specification is a Windows specification for how communication protocol programs (such as TCP/IP) and network device drivers should communicate with each other.
NetBIOS	Network Basic Input / Output System. NetBIOS is an extension of the DOS BIOS that enables a PC to connect to and communicate with a LAN.
Network	Any time you connect 2 or more computers together so that they can share resources, you have a computer network. Connect 2 or more networks together and you have an internet.
NIC	Network Interface Card. A board that provides network communication capabilities to and from a computer system. Also called an adapter.
Node	Any single computer connected to a network
Packet Filter	A filter that scans packets and decides whether to let them through.
PAP	Password Authentication Protocol PAP is a security protocol that requires users to enter a password before accessing a secure system. The user’s name and password are sent over the wire to a server, where they are compared with a database of user account names and passwords. This technique is vulnerable to wiretapping (eavesdropping) because the password can be captured and used by someone to log onto the system.
Password Cracker	A program that uses a dictionary of words, phrases, names, etc. to guess a password.
Password encryption	A system of encrypting electronic files using a single key or password. Anyone who knows the password can decrypt the file.
Password Shadowing	The encrypted password is no visible in the passwd file but stored in a shadow file that is only readable by root. This prevents brute force attacks on the encrypted field to guess the password. see e.g.: http://whatis.com/shadowpa.htm
Penetration	Gaining access to computers or networks by bypassing security programs and passwords.
Phreaking	Breaking into phone or other communication systems. Phreaking sites on the Internet are popular among crackers and other criminals

Ping Attack	An attack that slows down the network until it is unusable. The attacker sends a "ping" command to the network repeatedly to slow it down. See also Denial of Service.
Pirate	Someone who steals or distributes software without paying the legitimate owner for it. This category of computer criminal includes several different types of illegal activities Making copies of software for others to use. Distributing pirated software over the Internet or a Bulletin Board System. Receiving or downloading illegal copies of software in any form.
Pirated Software	Software that has been illegally copied, or that is being used in violation of the software's licensing agreement. Pirated software is often distributed through pirate bulletin boards or on the Internet. In the internet underground it is known as Warez.
Plain Text	The opposite of Cipher Text, Plain Text is readable by anyone.
PNS	PPTP Network Server. A PNS must have IP connectivity.
POP	Post Office Protocol. This is a common protocol used for sending, receiving, and delivering mail messages.
Port	An Internet port refers to a number that is part of a URL, appearing after a colon (:) right after the domain name. Every service on an Internet server listens on a particular port number on that server. Most services have standard port numbers, e.g. Web servers normally listen on port 80.
Port (H/W)	An interface on a computer for connecting peripherals or devices to the computer. A printer port, for example, is an interface that is designed to have a printer connected to it. Ports can be defined by specific hardware (such as a keyboard port) or through software.
POTS	Plain Old Telephone Service is the analog telephone service that runs over copper twisted-pair wires and is based on the original Bell telephone system. Twisted-pair wires connect homes and businesses to a neighborhood central office. This is called the local loop. The central office is connected to other central offices and long-distance facilities.
PPP	Point to Point Protocol. PPP encapsulates and transmits IP (Internet Protocol) datagrams over serial point-to-point links. PPP works with other protocols such as IPX (Internetwork Packet Exchange). The protocol is defined in IETF (Internet Engineering Task Force) RFC 1661 through 1663. PPP provides router-to-router, host-to-router, and host-to-host connections.
PPTP	Point-to-Point Tunneling Protocol.
Promiscuous Packet Capture	Actively capturing packet information from a network. Most computers only collect packets specifically addressed to them. Promiscuous packet capture acquires all network traffic it can regardless of where the packets are addressed.
Protocol	A “language” for communicating on a network. Protocols are sets of standards or rules used to define, format, and transmit data across a network. There are many different protocols used on networks. For example, most web pages are transmitted using the HTTP protocol.
Proxy Server	A server that performs network operations in lieu of other systems on the network. Proxy Servers are most often used as part of a firewall to mask the identity of users inside a corporate network yet still provide access to the Internet. When a user connects to a proxy server, via a web browser or other networked application, he submits commands to the proxy server. The server then submits those same commands to the Internet, yet without revealing any information about the system that originally requested the information. Proxy servers are an ideal way to also have all users on a corporate network channel through one point for all external communications. Proxy servers can be configured to block certain kinds of connections and stop some hacks.
Public Key Encryption	System of encrypting electronic files using a key pair. The key pair contains a public key used during encryption, and a corresponding private key used during decryption.
PVC	Permanent Virtual Circuit. A PVC is a logical point-to-point circuit between customer sites. PVCs are low-delay circuits because routing decisions do not

	need to be made along the way. Permanent means that the circuit is preprogrammed by the carrier as a path through the network. It does not need to be set up or torn down for each session.
Reconnaissance	The finding and observation of potential targets for a cracker to attack.
RFC	An RFC (Request for Comments) is an Internet formal document or standard that is the result of committee drafting and subsequent review by interested parties. Some RFCs are informational in nature. Of those that are intended to become Internet standards, the final version of the RFC becomes the standard and no further comments or changes are permitted. Change can occur, however, through subsequent RFCs.
RIP	Routing Information Protocol is an interior or intra-domain routing protocol that uses the distance-vector routing algorithms. RIP is used on the Internet and is common in the NetWare environment as a method for exchanging routing information between routers.
Router	A device that connects two networks together. Routers monitor, direct, and filter information that passes between these networks. Because of their location, routers are a good place to install traffic or mail filters. Routers are also prone to attacks because they contain a great deal of information about a network.
SAP	In NetWare, the SAP (Service Advertising Protocol) broadcasts information about available services on the network that other network devices can listen to. A server sends out SAP messages every 60 seconds. A server also sends out SAP messages to inform other devices that it is closing down. Workstations use SAP to find services they need on the network.
SATAN	A UNIX program that gathers information on networks and stores it in databases. It is helpful in finding security flaws such as incorrect settings, software bugs and poor policy decisions. It shows network services that are running, the different types of hardware and software on the network, and other information. It was written to help users find security flaws in their network systems.
Server	A computer, or a software package, that provides a specific kind of service to client software running on other computers.
Set-Top Box	A set-top box is a device that enables a television set to become a user interface to the Internet and also enables a television set to receive and decode digital television (DTV) broadcasts.
SNMP	System Network Management Protocol is a popular management protocol defined by the Internet community for TCP/IP networks. It is a communication protocol for collecting information from devices on the network.
Snooping	Passively watching a network for information that could be used to a hacker's advantage, such as passwords. Usually done while Camping Out.
SOCKS	A protocol that handles TCP traffic through proxy servers.
SPAM	Unwanted e-mail, usually in the form of advertisements.
Splitter	Passive devices that divide the traffic on trunk cables and send it down feeder cables.
Spoofing	To forge something, such as an IP address. IP Spoofing is a common way for hackers to hide their location and identity
SSL (Secured Socket Layer)	Technology that allows you to send information that only the server can read. SSL allows servers and browsers to encrypt data as they communicate with each other. This makes it very difficult for third parties to understand the communications.
STP	Twisted-pair cable consists of copper-core wires surrounded by an insulator. Two wires are twisted together to form a pair, and the pair form a balanced circuit. The twisting prevents interference problems. STP (shielded twisted-pair) provides protection against external crosstalk.
Straight through Ethernet cable	A cable that wires a pin to its equivalent pin. This cable connects two dissimilar devices, for example, a data terminal equipment (DTE) device and a data communications equipment (DCE) device. A straight through Ethernet cable is

	the most common cable used.
SUA	Single User Account – The Prestige's SUA (Single User Account) feature allows multiple user Internet access for the cost of a single ISP account - see also NAT.
TCP	Transmission Control Protocol handles flow control and packet recovery and IP providing basic addressing and packet-forwarding services.
Telnet	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
Tempest	Illegal interception of data from computers and video signals.
Terminal	A device that allows you to send commands to a computer somewhere else. At a minimum, this usually means a keyboard and a To display screen and some simple circuitry.
Terminal Software	Software that pretends to be (emulates) a physical terminal and allows you to type commands to a computer somewhere else.
TFTP	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP (File Transfer Protocol), but it is scaled back in functionality so that it requires fewer resources to run. TFTP uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
Trojan or Trojan Horse	Like the fabled gift to the residents of Troy, a Trojan Horse is an application designed to look innocuous. Yet, when you run the program it installs a virus or memory resident application that can steal passwords, corrupt data, or provide hackers a back door into your computer. Trojan applications are particularly dangerous since they can often run exactly as expected without showing any visible signs of intrusion.
UDP	UDP is a connectionless transport service that dispenses with the reliability services provided by TCP. UDP gives applications a direct interface with IP and the ability to address a particular application process running on a host via a port number without setting up a connection session.
UNIX	A widely used operating system in large networks.
URL	(Uniform Resource Locator) URL is an object on the Internet or an intranet that resides on a host system. Objects include directories and an assortment of file types, including text files, graphics, video, and audio. A URL is the address of an object that is normally typed in the Address field of a Web browser. The URL is basically a pointer to the location of an object.
VPN	Virtual Private Network. These networks use public connections (such as the Internet) to transfer information. That information is usually encrypted for security purposes.
Vulnerability	Point where a system can be attacked.
WAN	Wide Area Network s link geographically dispersed offices in other cities or around the globe. Just about any long-distance communication medium can serve as a WAN link, including switched and permanent telephone circuits, terrestrial radio systems, and satellite systems.
War Dialer	A program that automatically dials phone numbers looking for computers on the other end. They catalog numbers so that hackers can call back and try to break in.
Warez	A term that describes Pirated Software on the Internet. Warez include cracked games or other programs that software pirates distribute on the Internet
Web Configurator	This is a web-based router (not all) configurator that includes an Internet Access Wizard, Advanced.
Wire Tapping	Connecting to a network and monitoring all traffic. Most wire tapping features can only monitor the traffic on their subnet.
Worm	A program that seeks access into other computers. Once a worm penetrates another computer it continues seeking access to other areas. Worms are often equipped with dictionary-based password crackers and other cracker tools that enable them to penetrate more systems. Worms often steal or vandalize computer data.

WWW	(World Wide Web) -- Frequently used when referring to "The Internet", WWW has two major meanings - First, loosely used: the whole constellation of resources that can be accessed using Gopher, FTP, HTTP, telnet, USENET, WAIS and some other tools. Second, the universe of hypertext servers (HTTP servers).