Triple Play Service

IAD (DV-2010)

USER Manual

DAVOLINK

COPYRIGHT

TRADEMARKS

This manual should be read before the installation and operation, and the operator should correctly install and operate the product by using this manual.

This manual may be changed for the system improvement, standardization and other technical reasons without prior notice.

For further information on the updated manual or have a question the content of manual, contact **Document Center** at the address below .

Address : 1591-9, Anyang K-Center, Burim-dong, Dongan-gu, Anyang-si, Gyeonggi-do, Korea
e-mail : kubs15@davolink.co.kr

Or contact **Call Center** at the telephone below if you have any questions or concerns regarding the operation of your system.

Phone : 81-31-387-3240. ext 206

htDV-2010://www.davolink.com

SAFETY CONCERNS

Introduction

This document is User Manual of DV-2010S IAD. This manual describes how to operate and maintain the DV-2010 (Integration Access Device).

Structure

This document is composed of three chapters as follows :

Chapter 1. Introduction

System feature is outlined. Hardware specification and Software specification (i.e., interface type, service diagram, H/W function and S/W function) are in the DV-2010.

Chapter 2. Installation

It is a procedure for installation of DV-2010. It shows how to connect each cable to proper port of IAD. This chapter describes how to read the front LED for system status as well.

Chapter 3. Service Setup

DV-2010 is a doorway to let customer enjoy various multimedia services from . Internet Service, Voice Service, Video Service and Multimedia Broadcast service are affected by IAD configuration. Therefore this chapter describes how those are related with this IAD and how to configure each service parameter on DV-2010.

Chapter 4. Maintenance

Methods of checking and Maintain the service in the DV-2010 are described in this chapter.

Conventions

For product safety and correct operation, the following information must be given to the operator/user and shall be read before the installation and operation. This information may be set-off from the surrounding text, but is always preceded by a bold title in capital letters.

WARNING

Indicate a potentially hazardous situation which if not avoided, could result in death or serious injury.

CAUTION

Indicate a potentially hazardous situation which if not avoided, may result in minor or moderate injury. It may also be used to alert against unsafe practices and give a general caution

NOTE

Indicates additional information as a reference

Instruction

Indication for commanding a specifically required action

Revision History

EDITION	DATE OF ISSUE	REMARKS
I	April, .2005	

SAFETY CONCERNS

For product safety and correct operation, the following information must be given to the operator/user and shall be read before the installation and operation.

Symbols

Caution
Indication of a general caution

Restriction
Indication for prohibiting an action for a product

Instruction
Indication for commanding a specifically required action

This page intentionally left blank

TABLE OF CONTENTS

CHAPTER 1. INTRODUCTION

1 System Overview

DV-2010 is a kind of Home gateway for Triple Play service at home and SOHO environment. This device works like a central gateway for all the service enabling devices such as the VOIP, Internet and IP-TV functions. The IAD is a doorway where all services find their outlet to the service platforms, such as Internet Access concentrator, Call Switch and Media Farm.

1.1 DV-2010 Overview

DV-2010 is a residential access gateway which is integrated ADSL modem, VoIP terminal and Wireless AP (Access Point) into one compact Box.
It provides high speed wired/wireless internet service and excellent voice quality over high traffic Internet using efficient voice QoS mechanisms. It brings a seamless VoD (Video On Demand), IP-TV and TV and Radio broadcast services as well.
Many other intelligent functions as a home gateway are introduced in this document..

1.1.1 System Feature

- Voice over IP
- Video on Demand
- IP multicast (Converge legacy TV and Radio)
- High speed ADSL Interface(ADSL/ADSL2/ADSL2+)
- Supports 16 PVCs with different configurations
- Auto-Provisioning
- RFC2364 PPP over AAL5
- IPOA, MER (a.k.a IP over Ethernet over AAL5)
- Transparent bridging between all LAN and WAN interfaces
- Support s NAPT with ALG and stateful Inspection Firewall
- Supports Port Forwarding, Port Triggering, DMZ Host
- Analog FXS Interface
- Wireless Access Point
- Supports MGCP
- Supports fixed IP and dynamic IP
- USB1.1 slave port
- Supports standard Internet protocols including TCP/IP, UDP, and RTP/RTCP G.168 compliant echo cancellation
- Easy Installation and maintenance

1.2 System Specification

1.2.1 Basic Specification

Service		Specification	Remarks
Interface	ADSL Interface	ADSL/ADSL2/ADSL2	Auto Training
	Analog Interface	FXS, RJ-11	2 port Feeding : -48V, 25mA Ringing : 45Vrms, 3 REN
	Ethernet Interface	10/100base-T(X), RJ-45 with Auto-MDIX function	4 port (2 ports for STB, 2 ports for PC)
	Wireless LAN	802.11b/g PCMCIA Type-II	1 Antenna
	USB	USB 1.1 device	1 port
Signaling and Protocol	Voice Analog interface	FXS FXO (Optional)	Supports various country specifications
	VoIP	MGCP, SIP	Provision, Auto upgrade
Voice Capability		G.711, G.729.a, G.723.1 Echo Cancellation (G.168) VAD/CNG	
Fax Capabilities		Fax/Modem pass-through, T.38	Optional
Power		DC +12V/1.2A	External adaptor (Input voltage: 230~VAC OuDV-2010ut: +12VDC / 1.2A)

<Table 1> DV-2010 Basic Spec

1.2.2 Operation Environment Conditions

Item		Requirements
Temperature	Normal Operation	5 ~ 40℃
	Optimal Operation	18 ~ 26℃
	Limited Operation	2 ~ 50℃
Humidity	Normal Operation	20 ~ 65%
	Optimal Operation	45 ~ 55%
	Limited Operation	20 ~ 80%

<Table 2> Conditions

2 Software Features

2.1 IP Function

- Bridge Function
- PPPOE(LLC/SNAP)
- DHCP(Client, Server)
- IPCP
- Static IP Routing
- IP Filtering / MAC Filtering
- ICMP
- Proxy DNS
- UPnP
- SNMP (Agent & Tool)
- IGMP Proxy
- NAPT
- ALG (Application Layer Gateway)

2.2 Qos Function

- ToS
- Priority Queuing for Voice
- Dynamic Jitter Buffer Control
- VAD/CNG
- Echo cancellation
- ATM Traffic Management

2.3 Voice Functions

- MGCP(RFC3435)
- G.711a/u-law, G.729A, G.723.1
- Echo cancellation : G.165, G.168
- Fax Relay : Bypass fax and T.38
- DTMF Relay : Bypass, RFC2833
- Call Progress Tone Generation
- VoIP/PSTN selective or Prefix Dialing, Emergency call routing etc.
- Emergency call transfer (Power fail, CA connection fail etc.)
- IVR for announcement of system and call status

2.4 DSL Interface

- T1.413i2, G.992.1/2/3, 992.5(ADSL2+)
- Annex A/B
- Annex L (Reach Extended ADSL2)
- CBR, VBR, UBR(16VCs)
- RFC2684 VC-MUX, LLC/SNAP encapsulation

- RFC2364 PPP over AAL5 (PPPoA)
- RFC1577 (IPOA)

2.5 WLAN Interface

- IEEE 802.11b/g (Up to 54Mbps)
- Encrypted by WPA or WEB 64/128 bits
- 2dBi dipole antenna
- Wireless Bridge

2.6 Security Functions

- PAP/CHAP, PPDV-2010/L2DV-2010, IPSec ALG
- DIGEST authentication and encryption(MD5)
- Firewall (IP packet filtering, MAC filtering, DMZ)
- Service access control based on source and destination IP addresses

2.7 Management Function

- Web based GUI management
- SNMP, SNTP, Telnet, FTP/TFTP, UPnP
- Traffic statistics, tracing, debugging
- Configuration backup and restore
- Auto Software upgrade
- Auto Provisioning

서식 있음: 글꼴: (영어) Times New Roman, 네덜란드어(네덜란드)

CHAPTER 2. INSTALLATION

1 Installation

Welcome to the DV-2010 which is based on Residential Gateway with integrated VoIP terminal and ADSL modem, router, firewall, and 54g AP (Access Point) all in one compact hardware and firmware platform. This section contains instructions that would allow you to configure user security setting and pleasant wireless setting quickly. DV-2010 works like PnP (Plug & Play) in order to get rid of complex setting for user convenience. Auto provisioning and Auto Software upgrade functions are enabled on DV-2010. IAD downloads all user specific setting as soon as it connects to the high-speed ADSL line,

1.1 Hardware Installation

1.1.1 Before Start

This section describes the hardware features and installation of the DV-2010. It is handset-to-Internet adaptors that allow regular analog telephones to operate on IP-based telephony networks. DV-2010 supports two FXS (Foreign Exchange Station) port and four Ethernet interfaces for STB and PC. Two ports is dedicated for STB (Set-Top Box) and the other ports for PC. IAD support the Internet, IPTV, VoD and VoIP at the same time using High speed internet and specific QoS mechanism. It also has a WLAN AP (Access Point) to offers you the freedom to roam without the burden of cables

1.1.2 Safety Recommendations

When installing and operating the DV-2010 system, follow the safety guideline provided below to help prevent serious injury and/or damage to DV-2010 system.

(1) Do not open or disassemble this product. This system does not contain any user serviceable parts. Maintenance is to be only performed by qualified personnel.

(2) Do not get this product wet or pour liquids into this device.

(3) Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.

(4) Use only the power supply that comes with the DV-2010.

(5) Maintain between 0℃ and 40℃ and it must be well ventilated

(6) When removing or connecting cables, always unplug DV-2010 power.

(7) Check the electric quality, especially when the device is located by a big motor

(8) Be sure all ventilation chambers are not obstructed at all times.

(8) Do not put on heavy equipment and machinery on the system.

(9) Keep away from IAD at least 5cm in normal condition.

Instruction

Read the manual before you connect the system to its power source

1.2 Hardware Installation Procedure

The DV-2010 includes the following items.

- Two Analog Telephone Line and four 10/100Base-T Ethernet Cables
- User Guide
- A strut and an Wi-Fi antenna
- A splitter
- 12V power Adaptor

1.2.1 DV-2010 Installation steps

After the equipment is in place, see Figure 2 and follow the next procedure to install the DV-2010.

Step 1. Connect one end of a telephone line cord into the wall jack and plug the other end to the LINE input on the rear of the splitter.

Step 2. Connect one end of a telephone line cord into the PC of the splitter and plug the other end to the ADSL input on the rear of DV-2010.

Step 3. Connect one end of a telephone line cord to the TEL input on the rear panel of the IAD. Connect the other end to an analog telephone set

CAUTION

Connect the TEL port to a telephone only, never to a telephone wall jack

.

NOTE

The telephone must be switched to tone setting (not pulse) for the DV-2010 to operate properly.

Step 4. Connect a straight-through Ethernet cable from your PC and STB to the 10/100 PC RJ-45 LAN port and STB ports on DV-2010.

CAUTION

LAN port 1 and 2 are only dedicated for STB. So do not connect PC to these ports. PC can only connect to LAN 3 and 4 port for the Internet.

Step 5. Insert the power adaptor cable into the power connector on the DV-2010.

WARNING

Use only supplied power adaptor

Step 6. Connect the plug end of the 12V DC power adaptor cord into an electrical power outlet.

Step 7. When the DV-2010 is properly connected and powered up, the green power (PWD) lights and the green status (STS) LED flashes to indicate that DV-2010 is in initial processing.

CAUTION

Do not cover or block the air vents on either the top or the bottom surface of DV-2010 when IAD is in horizontal location. Overheating can cause permanent damage to the IAD

.

NOTE

Power LED and INET LED are orange color blinking at the same time when IAD is on software downloading process.

1.3 Cable connection

After the equipment is in place, see Figure 1 how to connect cable to the rear of the DV-2010.

<Figure 2> DV-2010 Cable connection

Instruction

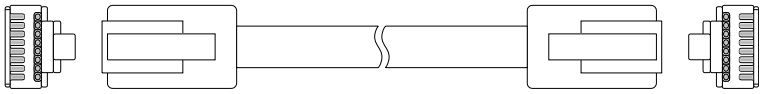
LAD 1,2 port is dedicated for STB. Don¡t connect PC to these ports.

PC can¡t get any IP address from IAD if PC is connected to STB port.

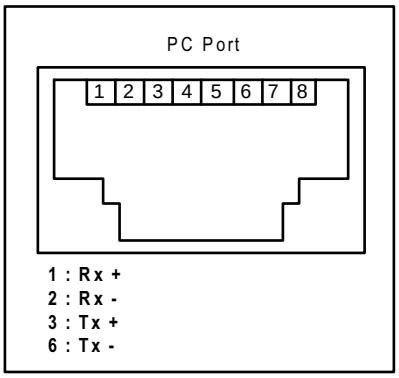
1.3.1 Connecting Ethernet cable

The Straight cable is used for connecting LAN port to a terminal such as workstation, PC, laptop and STB. Actually, Straight and cross-over cable are possible for LAN connection

because DV-2010 supports Auto MDI-X function on LAN port.
Maximum length of RJ-45 should be less than 85m.



<Figure 3> RJ-45 cable (UDV-2010 cable)



<Figure 4> Ethernet Port pin connection

RJ-45 Plug (PC)		connect	RJ-45 Plug (PC Port)	
Pin	**Signal**		**Pin**	**Signal**
1	TX+	⟷	1	TX+
2	TX-	⟷	2	TX-
3	RX+	⟷	3	RX+
4	NC		4	NC
5	NC		5	NC
6	RX-	⟷	6	RX-
7	NC		7	NC
8	NC		8	NC

<Table 3> Connection between WAN port and modem

1.3.2 FXS port

FXS port is for telephone or FAX connection using RJ-11 connector to the terminal.

RJ-11 Plug (Analog phone/Fax)		Connect	RJ-11 Plug (FXS port)	
Pin	**Signal**		**Pin**	**Signal**
1	NC		1	NC
2	NC		2	NC
3	Ring	← →	3	Ring
4	Tip	← →	4	Tip
5	NC		5	NC
6	NC		6	NC

<Table 4> FXS port cable pin connection

1.3.3 ADSL port

This port is used for connecting to CO(Central Office) Trunk, or connect to splitter.
It use RJ-11 Connector.

RJ-11 Plug (PSTN)		Connect	RJ-11 Plug (PSTN port)	
Pin	**Signal**		**Pin**	**Signal**
1	NC		1	NC
2	NC		2	NC
3	Ring	← →	3	Ring
4	Tip	← →	4	Tip
5	NC		5	NC
6	NC		6	NC

<Table 5> ADSL port pin connection

1.3.4 Cable Length

Maximum Length of cable, which is connected to DV-2010n, must comply with the following:

1) Ethernet

Maximum length of 10/100BaseT Ethernet is 330 feets/100 meters. (complies with IEEE802.3 Recommendation)

2) Analog line

Maximum length of analog line is defined by loop resistance. Maximum loop resistance is up to 600Ω (included telephone/voice switch).

2 LED Status

When DV-2010 comes up, you can judge the operation status of system by LED status.

LED	State	Description
PWR	ON (Green)	When power is present,
	OFF	When power is not present or fatal error
	Solid Red	POST failure or device malfunction
	Flashing Orange	Updating S/W image
STS	Blink per 0.1 sec	Running system, not starting VoIP service yet
	Blink per 1 sec	Start VoIP service, not registered yet
	3 sec ON, 1 sec OFF	Registered to VoIP Server and can make VoIP call
ADSL	Solid Green	In Sync with DSL line
	OFF	Modem power off
	Blink per 0.1 sec	Attempting to sync with DSL line
	Solid Red	DSL connection failure
INET	Solid Green	DSL is up and get IP address per PVC
	OFF	Modem power off or ADSL link down
	Blinking Green	Provision is completed and Data traffic is going through
	Blinking Orange	Provision is completed but there is a PVC not allocated IP address. Traffic is on the available PVC. Updating S/W image
	Solid Red	Provision is not completed
TEL	Solid Green	OFF-Hook phase
	OFF	ON-Hook phase
LAN	ON	Ethernet connection is established
	Blinking	Data is transmitting or receiving data
USB	ON	USB is connected to a host PC
	Blinking	Data is being transferred over the USB connection
WLAN	ON	Wireless Access Point(AP) is enabled
	Blinking	Data is being transferred over the WLAN connection

<Table 6> LED Status

- If there is no LED light, check the power cable connection.
- Device will be restarted when you push the Init button at the rear of DV-2010.
  - Power LED will be OFF
- When you keep pushing init button about 2~3 sec, It will reload Factory default value.

Power LED and PPP LED will be ON concurrently.

- Power LED and INET LED are orange blinking at the same time during S/W updating
- IAD booting time (all services up) : approximately one minute.
- IAD configuration file download time: approximately 2 seconds.
- IAD software image file download time: approximately 10 minute.
- IAD software image file burning time: approximately 2 minutes.

CHAPTER 3. CONFIGURATION

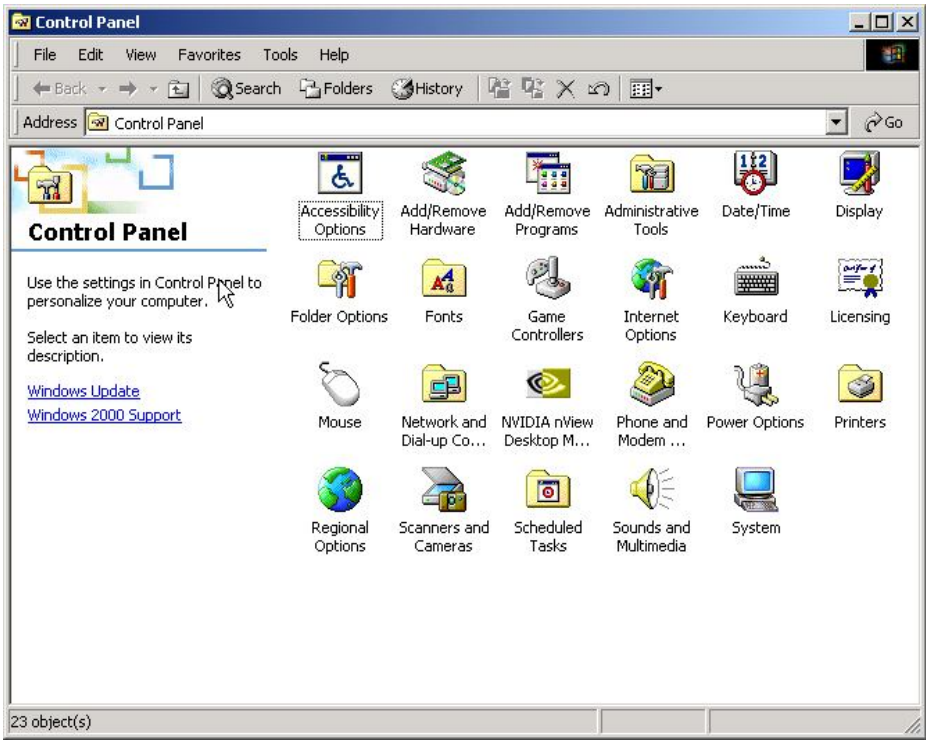
1 Basic configuration

After installing system as like service network diagram 1, you should have to assigne IP address on the connected PC between 192.168.1.2 and 192.168.1.253 to access the DV-2010 using Web browser. But DHCP Server is enabled by default on IAD so user does not need to set IP address on PC manually.

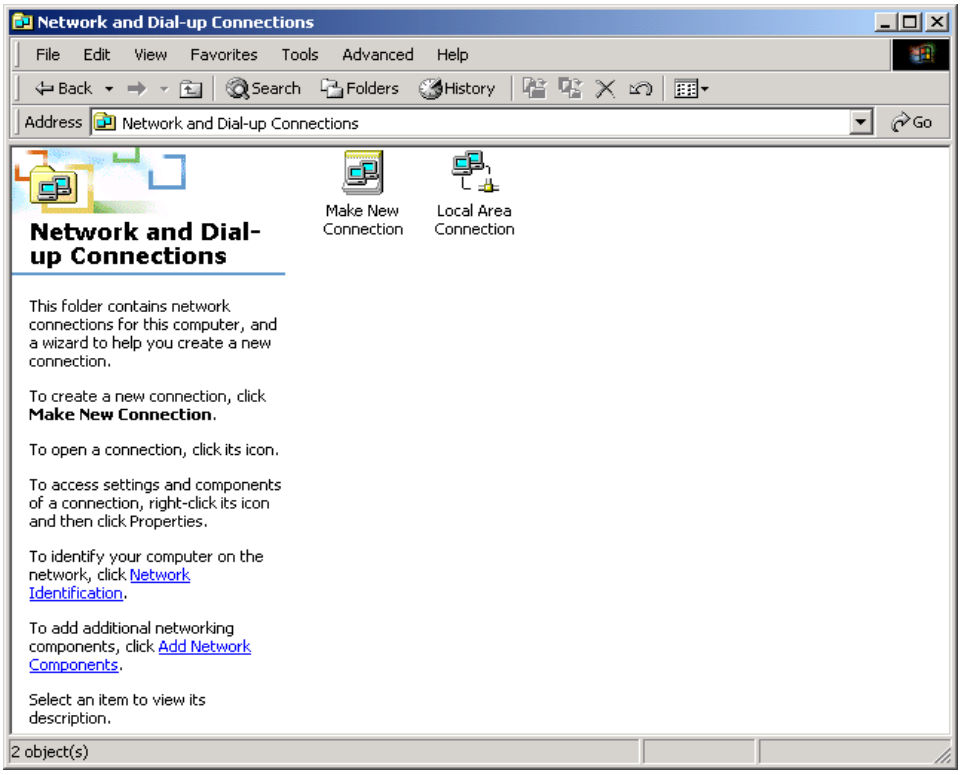
1.1 IP configuration on PC

DV-2010 supports DHCP server function to assign private IP to PCs. User can assign an IP address manually as like 192.168.1.XXX. The default LAN IP address is 192.168.1.1

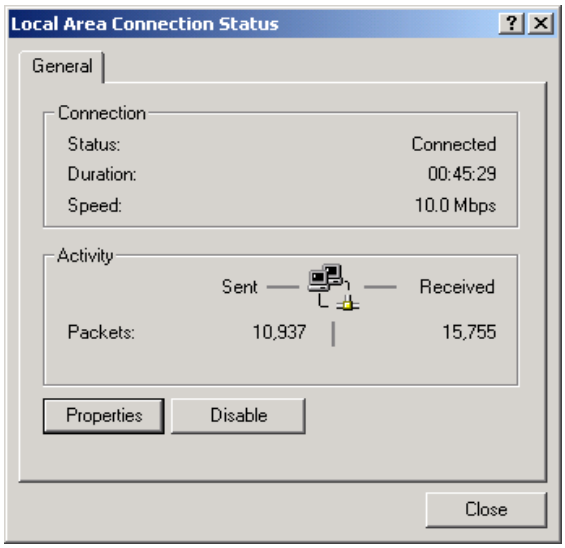
1. Open ¡Control Panel¡ and double click ¡Network and Dial-up connection¡ icon.



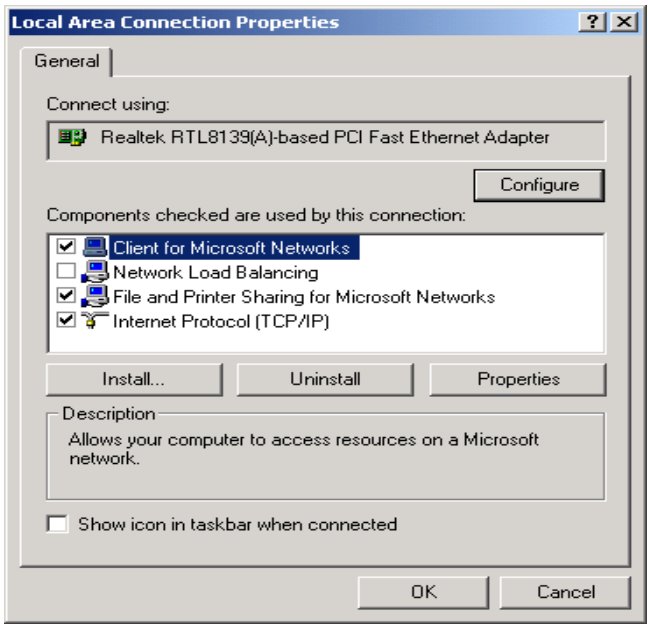
2. Double click ¡Local area connection¡ in network connection window.



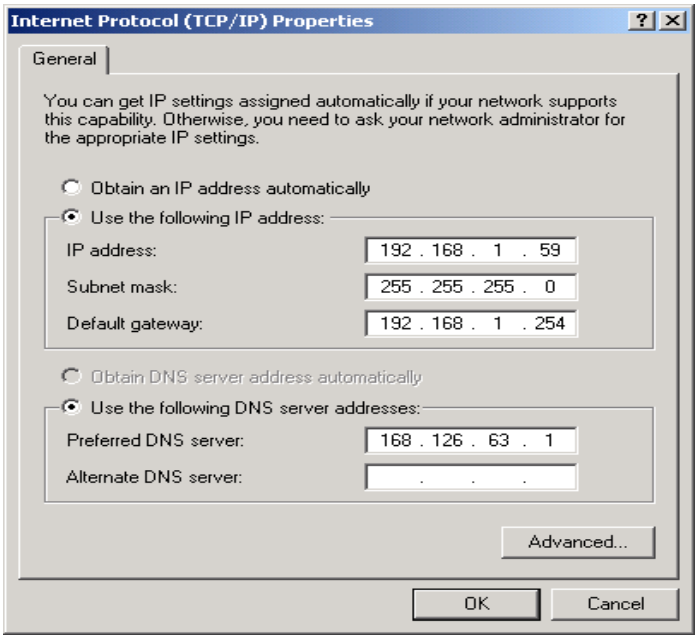
3. Click on ¡Properties¡ button.



4. Select ¡Internet protocol (TCP/IP)¡ and click on ¡Properties¡ button.



5. Select ¡IP address automatically and ¡DNS address automatically¡ in internet protocol attribute window.



If you want to get a dynamic IP address from DV-2010, Click the ¡obtain an IP address automatically. Otherwise you should select the ¡Use the following IP address when you want to set an static IP on your computer.

Instruction

Do not assign the first 4 IP addresses for PC. The first four IP addresses are dedicated for STB.

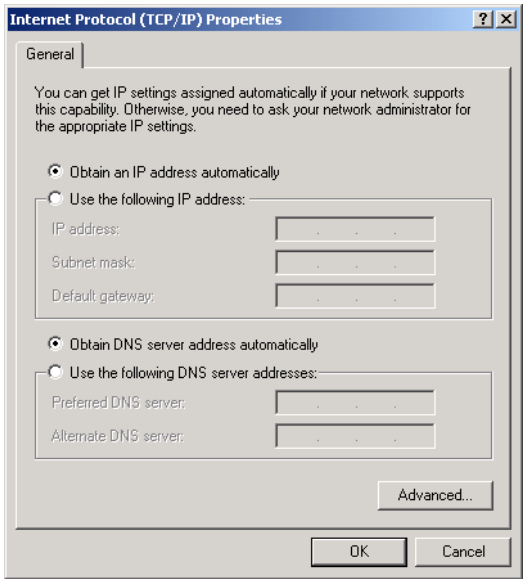
Instruction

IP pool for local host should be more than 4

NOTE

User can not disable DHCP function for VoD

6. Click ¡OK¡ button in internet protocol attribute window and then close all windows opened.



NOTE

Windows XP and 2000 do not need to restart PC for reloading the new IP address. Other Windows OS have to restart for activation the changes.

7. Open ¡COMMAND PROMPT¡ window and Execute ¡ipconfig¡ command to make sure that your PC is assigned IP address, subnet mask and default gateway value.

NOTE

Window98 and Window ME version support ¡winipcfg¡

Remember the IP Address value should be in 192.168.1.2~ 192.168.1.254, subnet mask should be 255.255.255.0, and Default Gateway should be 192.168.1.1

8. From windows system, go to ¡run¡. Type in ¡command¡.
   From ¡Command Prompt¡ screen, type ¡ping 192.168.1.1¡ and press ¡Enter¡.
   If the following message is displayed, your computer is properly connected to the PC port of DV-2010.

```
[c:\]ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 2ms

[c:\]
```

1.2 Access to WEB UI of IAD

All Triple related configurations will be downloaded from TFTP server after DV-2010 is connected on DSL line and DSL connection is established completely. Configuration file includes PPP user name, password, voice setting and son on. User doesn¡t need to set complex settings to enjoy Triple Play service. Just plug and enjoy service.
When you need set user specific setting like WLAN and Virtual server, access IAD using HTTP.

Instruction

Before accessing Web Manager, verify the state of the DV-2010 LED is blinking properly. This indicates that the DV-2010 is ready to be configured

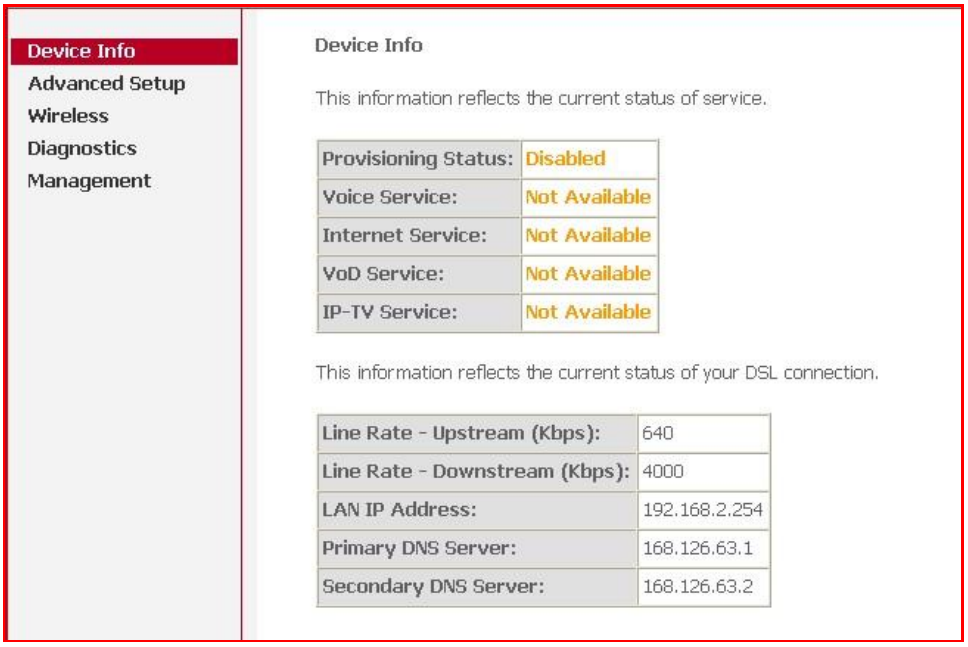
1. In order to configure this device, you should understand port forwarding, DMZ and port triggering. If you don¡t understand properly, contact service center.

2. Open a new Web browser window and enter the DV-2010¡s IP address, Enter ¡htDV-2010://192.168.1.1¡ for the URL
   At this point, the PC should present an authentication window similar to this one

Enter ¡user¡ in the User name and Password field.

Instruction

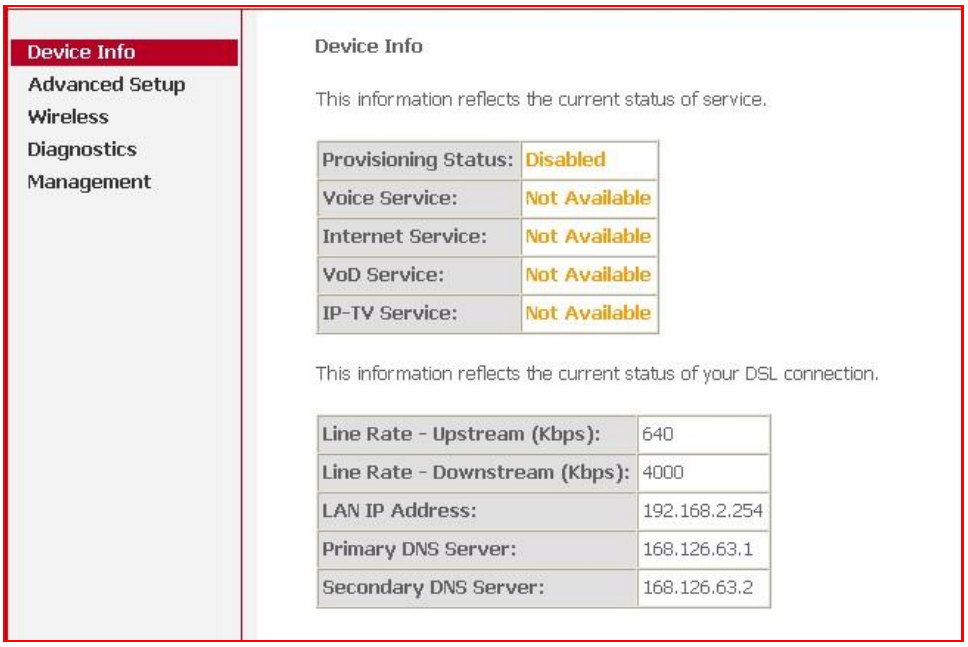
User can change this default password using management menu on the WEB UI (User Interface)



You can change the LAN IP address of IAD. IAD is enabled DHCP server by default to give IP addresses to its Host network devices from the next IP address you set on LAN interface.
User can not disable DHCP server function for STB.
The leased IP address from DHCP server will be refreshed after the leased time.
Click on the Next button to setup Wireless LAN.

1.2.1 Device information

After rebooting, below Device information will be come up. This page displays information about the current state of the DV-2010. If DV-2010 is connected to ADSL line properly, it shows current Line Rate (Upstream and Downstream) and the LAN IP address and DNS IP address for Internet. If the Downstream line rate is below than 14000 Kbps, you should contact DV-2010 service center.



2 Advanced Setup

There are many advanced router features and Internet Telephony features supported by the DV-2010. These features are documented in this section, and include:

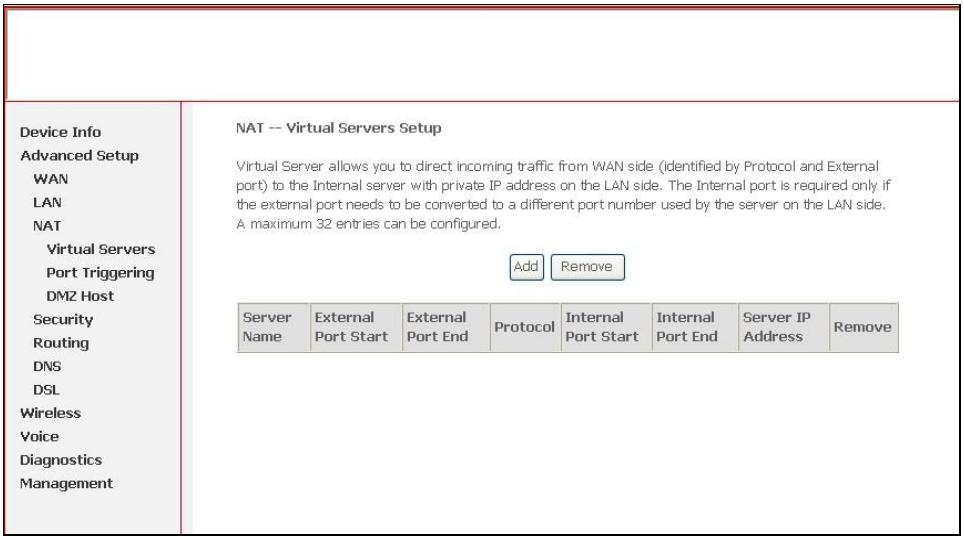
1. Various NAT Function(Virtual Servers, Port Triggering, DMZ Host)
2. Security(LAN IP address, port number filtering, Parental Control)

2.1 NAT (Network Address Translation)

The DV-2010 is capable of operating in several modes that adjust how the device routes IP traffic. These features are accessible from the Advanced Menu on the left Main menu.

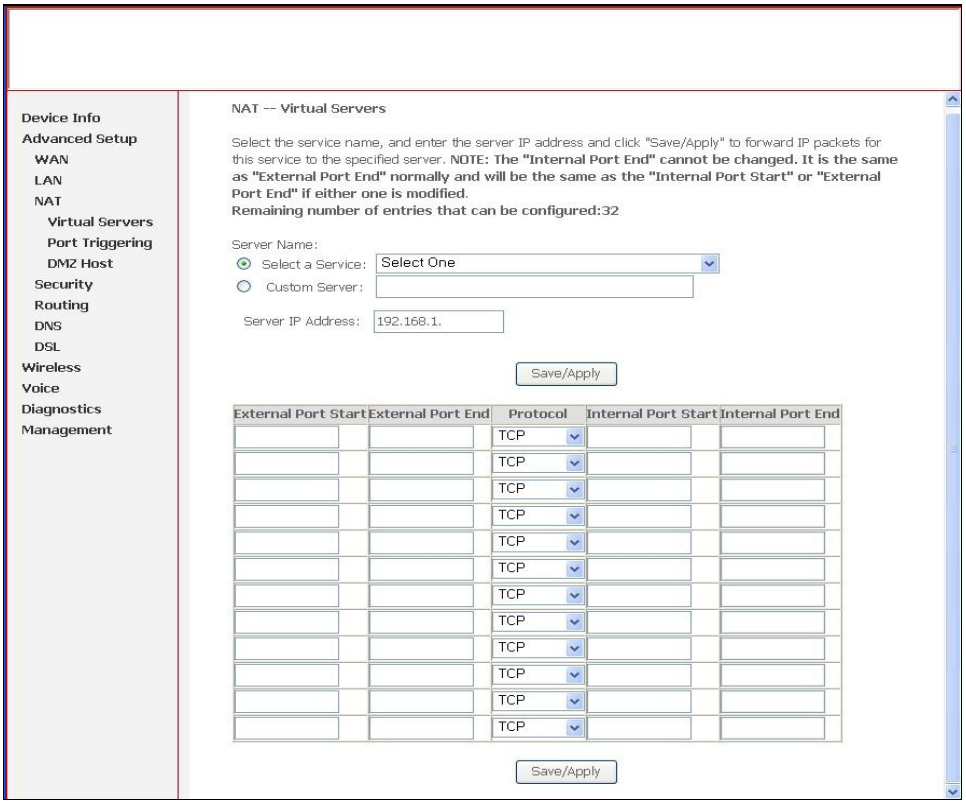
2.1.1 Virtual Servers

Virtual server setup page will be come up when you click NAT sub menu of the Advanced Setup menu.



Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to internal server which has a private IP address on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

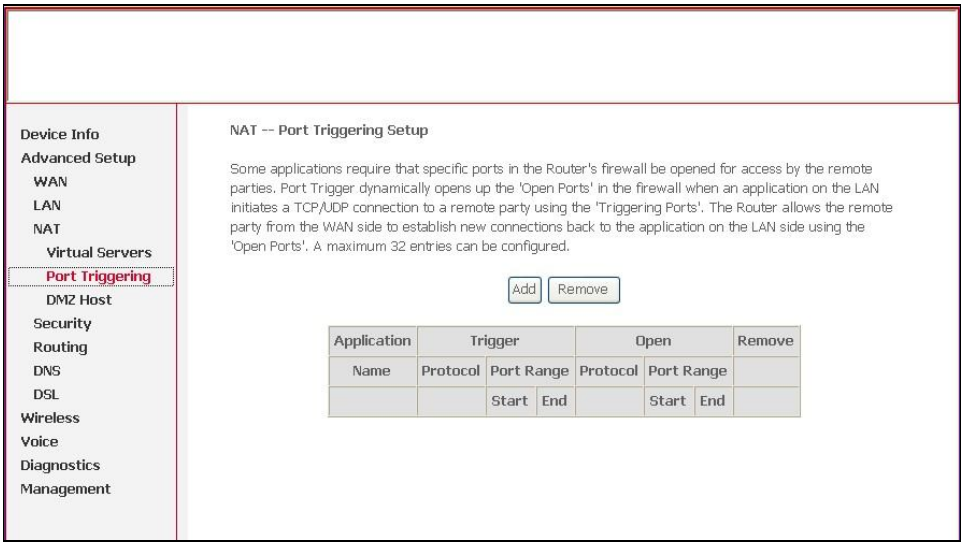
Click on the Add button to configure virtual server.



There are many famous service names on the Service list. Select a service name, and enter the local IP address and click "Save/Apply" to forward IP packets for this service to the specified server. If there is no matched service name on the list, set service name at the custom server and put the service specific port number at the below column. After clicking on the save/apply button, the virtual server list will be come up.

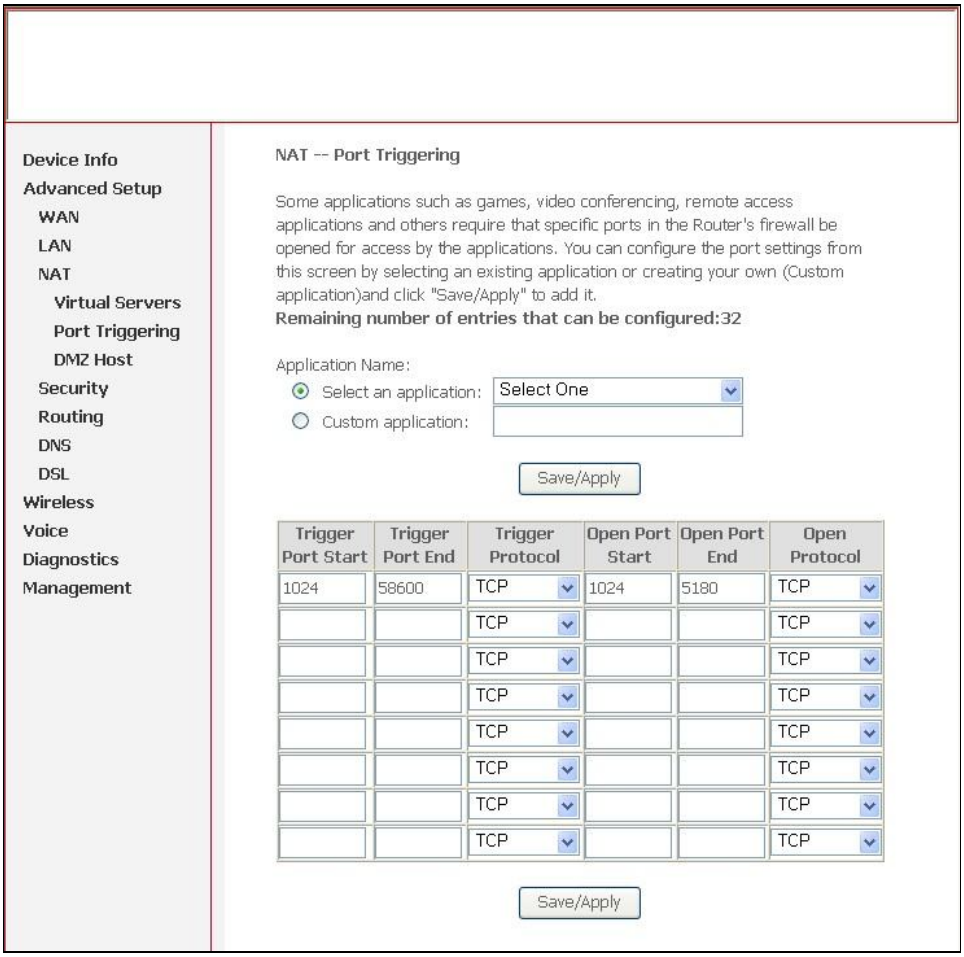
2.1.2 Port Triggering

Port Triggering is similar to Port Forwarding except that they are not static ports held open all the time. When the DV-2010 detects outgoing data on a specific IP port number set in the ¡Trigger Range¡, the resulting ports set in the ¡Target Range¡ are opened for incoming (or sometimes referred to as bi-directional ports) data. If no outgoing traffic is detected on the ¡Trigger Range¡ ports for 10 minutes, the ¡Target Range¡ ports will close. This is a safer method for opening specific ports for special applications (e.g. video conferencing programs, interactive gaming, file transfer in chat programs, etc.) because they are dynamically triggered and not held open constantly or erroneously left open via the router administrator and exposed for potential hackers to discover.



Click on the Add button to set up port triggering. A maximum 32 entries can be configured. Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application)and click "Save/Apply" to add it.

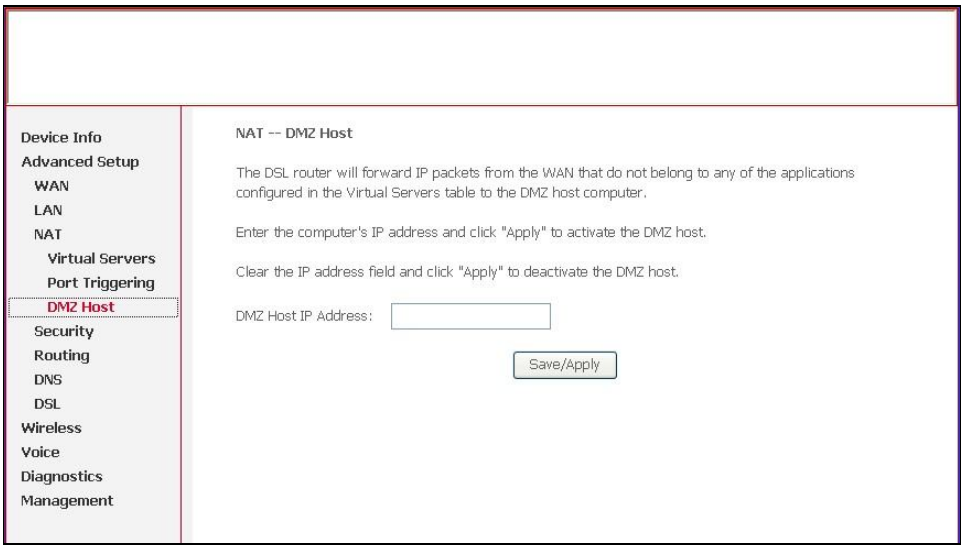
Port Triggering should be set up for commonly used special applications requiring bi-directional communications on specific port numbers in order to operate correctly. One of the most common applications that require this is video conferencing applications that require separate IP ports for video and audio transmissions to management servers in the public (WAN) network.



Above is an example setup that allows a special application to communicate with any PC on the Private LAN that tries to first connect with outgoing port numbers in the range of 1024 through 5180 and consequently triggers an opening of ports 1024 through 58,600 for bi-directional traffic for both TCP and UDP. This operation can only be effective for a single PC at a time, but can be used for any PC at a later time after the trigger ¡times out¡. This is a very effective method for allowing various user¡s on the Private LAN to use a common application at different times without the security risk of leaving IP ports open all the time and the directed PC¡s unprotected.

2.1.3 DMZ Hosting

DMZ (De-militarized Zone) hosting (also commonly referred to as ¡Exposed Host¡) allows you to specify the ¡default¡ recipient of WAN traffic that NAT is unable to translate to a known local PC. This can also be described as a computer or small sub-network that sits between the trusted internal private LAN and un-trusted public Internet. The DMZ Host page is shown below.

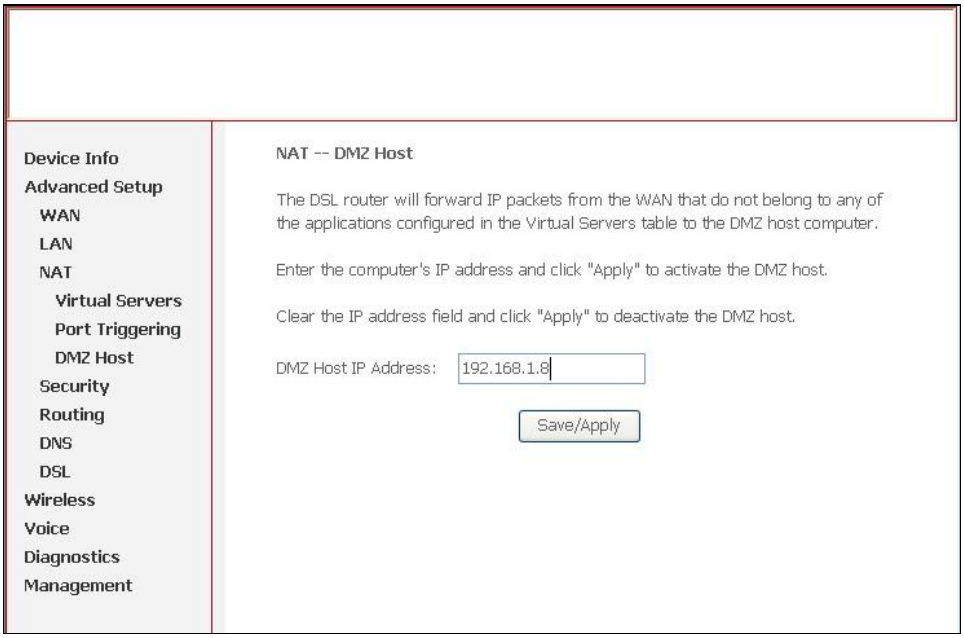


You may configure one PC to be the DMZ host. This setting is generally used for PC¡s using ¡problem¡ applications that use random port numbers and do not function correctly with specific port triggers or port forwarding setups mentioned earlier.

If a specific PC is set as a DMZ Host, remember to set this back to ¡0¡ when finished with the needed application, since this PC will be effectively exposed to the public Internet, though still protected from Denial of Service (DoS) attacks via the Firewall.

Enter the computer's IP address and click "Apply" to activate the DMZ host.
Clear the IP address field and click "Apply" to deactivate the DMZ host.

With some problem applications (using random port numbers that may be undefined), the user may have to DMZ the Specific Host PC in order to get the application to work correctly. This allows a guarantee that any application can work behind the firewall/NAT application in the DV-2010.



In the example above, the PC with the IP address 192.168.1.8 has all of its IP Ports exposed to the WAN just as a PC on a bridging data mode would. However, the firewall is still activated here for specific DoS attacks, etc.

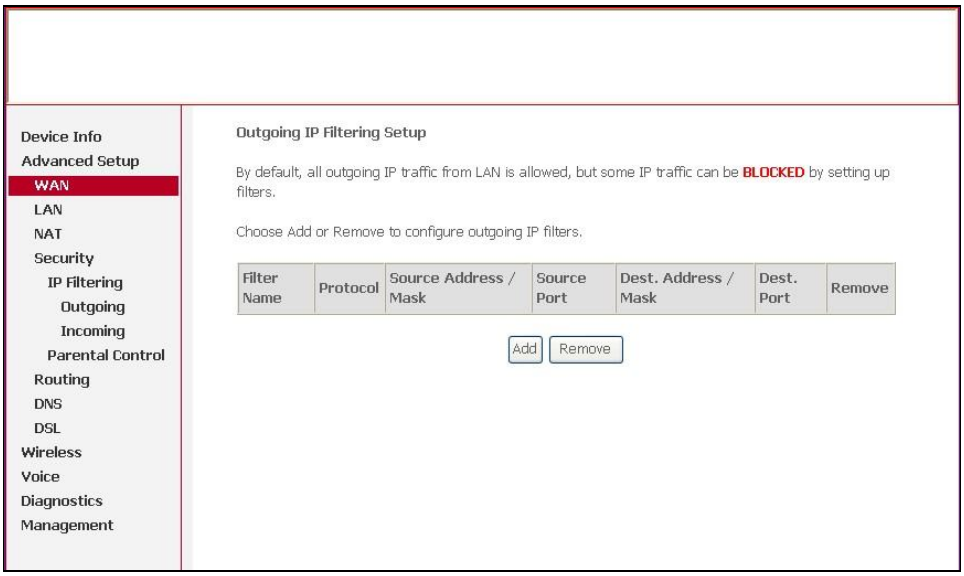
2.2 Security

The Web Filter page has various settings related to blocking or exclusively allowing different

types of data through the DV-2010 from the WAN to the LAN.

2.2.1 IP Filtering

The DV-2010 can be configured to prevent local PCs from getting access the WAN by specifying those IP addresses that should be filtered. It is also possible to control outgoing IP traffic from LAN. This can be done from the IP Filtering page in the Advanced Security Menu. The IP Filtering page shows below.



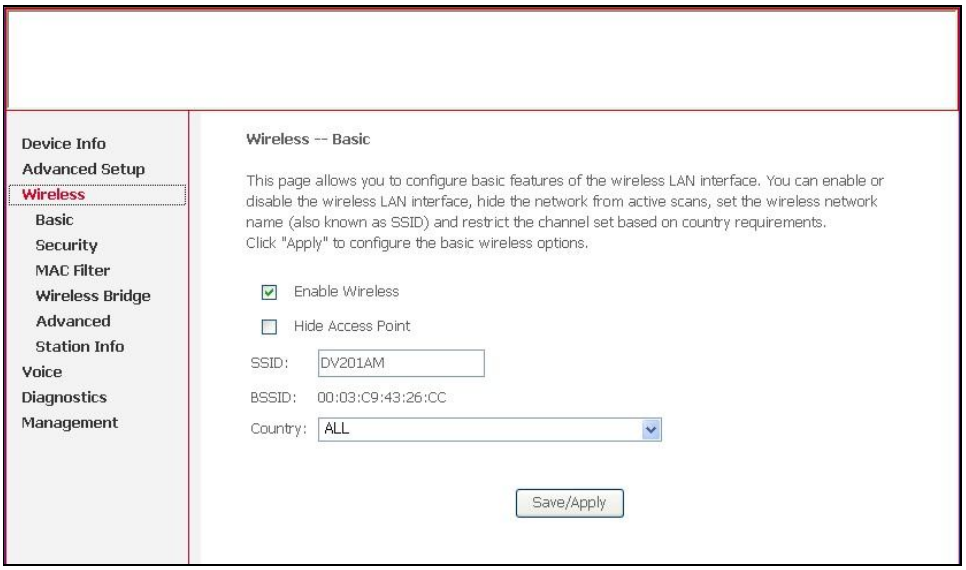
By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters. You can configure which local PCs are denied access to the WAN. By default, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be ACCEPTED by setting up filters. Note that you only need to enter the LSB (Least-significant byte) of the IP address; the upper bytes of the IP address are set automatically from the DV-2010 IP address. To activate the IP address filter, you must also click on the Save/Apply button. The new filter rule will be applied without system reboot.

3 Wireless Configuration

The DV-2010 also serves as an 802.11b/g access point (AP). If DV-2010 has an 802.11 interface card installed, it can be configured using the web interface. If the wireless card is not installed, the Wireless menu on the left column of the web interface will not be present.

3.1 Wireless Basic

Click on the Wireless menu to bring up the Wireless 802.11b/g Basic configuration page is shown below.



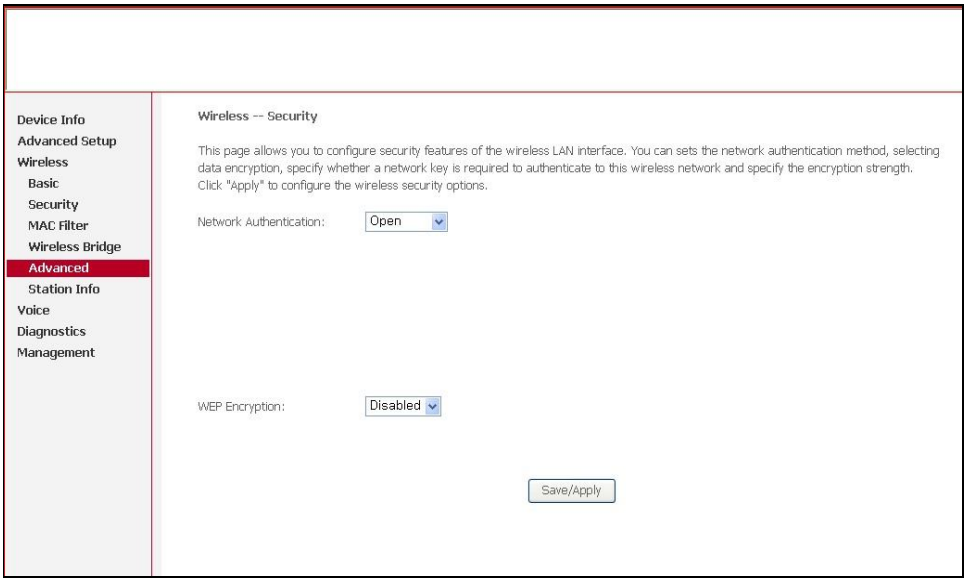
This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID). The 802.11 radio can also be shut down to disable the wireless network if desired. This is the safest way to prevent unwanted wireless network intrusion when wireless access is not needed. The Service Set Identifier (SSID) is a text description of the Access Point and is entered as a string of ASCII characters. The Network Type can be selected and Opened or Hided. In an open network, the AP broadcasts its SSID in each periodic beacon packet so all clients can anonymously discover its SSID. If you choose Hide Access Point, the SSID broadcast is silenced and a client that wished to connect to the AP must already have knowledge of the SSID in order to gain access. This provides an additional layer of security to gaining access to the wireless network. The country selection is used to properly alter the 802.11 network transmissions to match the operating frequency bands allowed in each area.

Setting	Description	Value List or Range	Default
Network Name (SSID)	Sets the Network Name (also known as SSID) of this network.	up to 32 character string containing ASCII characters any keyboard character	DV201AM
Network Type	Selecting hides the network from active scans. Selecting Hide to reveals the network from active scans.	Check or Leave	Leave (open)
Country	Restricts the channel set based on country requirements.	Worldwide, Thailand, Israel, Jordan, China, Japan, USA, Europe, All channels	ALL

<Table 7 : Basic Settings Definitions >

3.2 Security

Click on the Security sub menu to bring up the 802.11 Encryption page shown below. Table 12 describes the settings on this page.



This page allows you to configure security features of the wireless LAN interface. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

Setting	Description	Value List or Range	Default
Network Authentication	Sets the network authentication method. 802.1X and WPA require that valid RADIUS parameters be set. WPA-PSK requires a valid WPA Pre-Shared Key to be set.	Disabled, shared, 802.1x, WPA, WPA-PSK, etc.	Open
Open	Null authentication algorithm	Grant any request for authentication	802.11
Shared	Require static encryption key	64bit or 128bit strength	802.11
802.1X	Provides the link layer with extensible authentication	RADIUS server	802.11 MAC layer security
WPA	Wi-Fi Protected Access	TKIP, AES or both	TKIP
WPA2	Using counter mode with CCMP	TKIP, AES or both	AES
WPA-PSK	Sets the WPA Pre-Shared Key (PSK).	Depends on Network Authentication setting. See <.	<NULL>

<Table 8> Security Settings Definitions

Network Auth / Parameter	Shared	802.1x	WPA	WPA-PSK
WPA Pre-Shared Key	Disabled	Disabled	Disabled	Either a 64-digit hexadecimal number *or* a 8 to 63 character ASCII string.
WPA Group Rekey nterval	Disabled	Disabled	0 to 232-1	0 to 232-1
RADIUS Server	Disabled	IP v.4 address	IP v.4 address	Disabled
RADIUS Port	Disabled	0 to 65535	0 to 65535	Disabled
RADIUS Key	Disabled	0 to 255 character ASCII string	0 to 255 character ASCII string	Disabled
Data Encryption	Off, WEP (64-bit), WEP (128-bit)	WEP (128-bit)	TKIP, AES	TKIP, AES
Network Key 1 thru Network Key	4	2	Disabled	Disabled

<Table 9> Parameter Value List/Range depends on Network Authentication Setting

Data / Enc / Setting	Off	WEP	TKIP, AES, or TKIP + AES
PassPhrase	Disabled	up to 32 character string containing ASCII characters with codes between 0x20 and 0x7e	Disabled
Network Key 1 thru Network Key 4	Disabled	5 or 13 ASCII characters or 10 or 26 hexadecimal digits	Disabled
Current Network Key	Disabled	1 to 4	Disabled

<Table 10> Parameter Value List/Range depend on Network Authentication Settings

Setting	Description	Value List or Range	Default
Network Authentication	Sets the network authentication method. 802.1X and WPA require that valid RADIUS parameters be set. WPA-PSK requires a valid WPA Pre-Shared Key to be set.	Disabled, 802.1x, WPA, WPA-PSK	Disabled
WPA Pre-Shared Key	Sets the WPA Pre-Shared Key (PSK).	Depends on Network Authentication setting. See <.	<NULL>
WPA Group Rekey Interval	Sets the WPA Group Rekey Interval in seconds. Set to zero to disable periodic rekeying.	Depends on Network Authentication setting. See <.	0
RADIUS Server	Sets the IP address of the RADIUS server to use for authentication and dynamic key derivation.	Depends on Network Authentication setting. See <.	<NULL>
RADIUS Port	Sets the UDP port number of the RADIUS server. The port number is usually 1812 or 1645 and depends upon the server.	Depends on Network Authentication setting. See <.	1812
RADIUS Key	Sets the shared secret for the RADIUS connection.	Depends on Network Authentication setting. See <.	<NULL>
Data Encryption	Selecting Off disables data encryption. Selecting WEP enables WEP data encryption and requires that a valid network key be set and selected unless 802.1X is enabled.	Depends on Network Authentication setting. See <.	Off (Disabled, 802.1x); TKIP (WPA, WPA-PSK)

Shared Key Authentication	Sets whether shared key authentication is required to associate. A valid network key must be set and selected if required.	Depends on Network Authentication setting. See <.	Optional
PassPhrase	Sets the text to use for WEP keys generation.	Depends on Data Encryption setting..	<NULL>
Network Key 1 thru Network Key 4	Enter 5 ASCII characters or 10 hexadecimal digits for a 64-bit key. Enter 13 ASCII characters or 26 hexadecimal digits for a 128-bit key.	Depends on Data Encryption setting..	<NULL>
Current Network Key	Selects which network key is used for encrypting outbound data and/or authenticating clients.	Depends on Data Encryption setting..	1

<Table 11> Security Setting Definitions

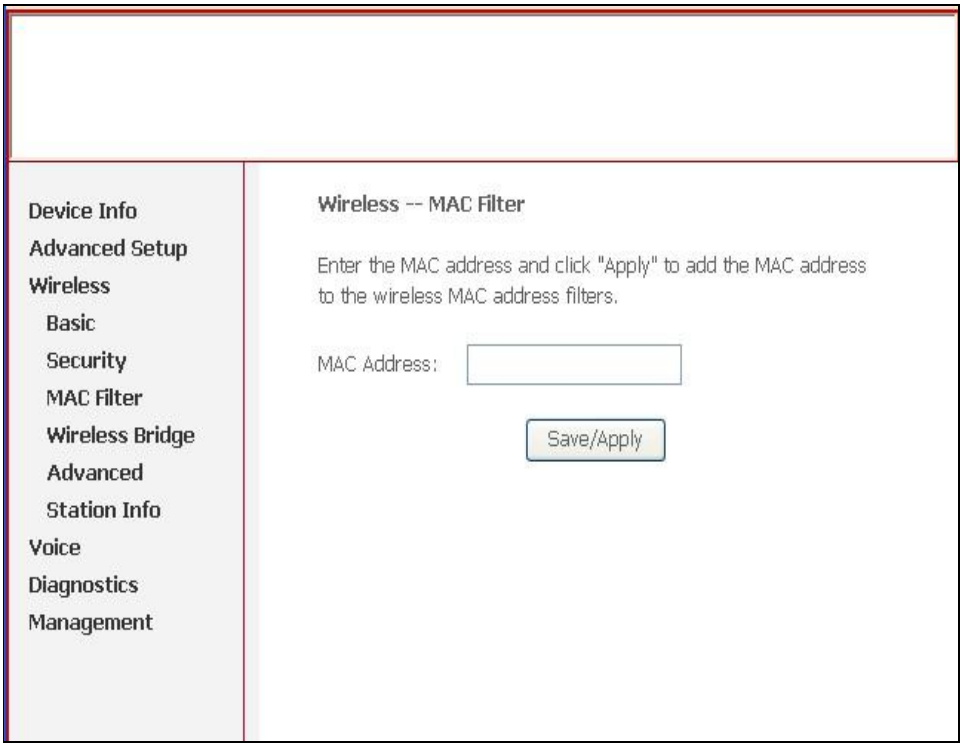
3.3 Access Control using MAC Filter

The Access Control page allows the user to store MAC addresses of specific wireless clients and allow or deny them access to the network. To add MAC addresses to the list, simply type each address in one MAC address blank and click Save/Apply to store it. To do nothing with the addresses entered, just leave the MAC Restrict Mode set to Disabled. To allow WAN and private LAN network access to all of the MAC addresses entered, exclusively, click on the Allow sphere. To deny network access to all of the MAC addresses entered, click on the Deny sphere to Deny.

This Deny setting will block all of the listed wireless clients from gaining access to the WAN as well as the private LAN. A list of connected clients is shown at the bottom of the page.

Setting	Description	Value List or Range	Default
MAC Restrict Mode	Selects whether clients with the specified MAC address are allowed or denied wireless access.	Disabled, Allow, Deny	Disabled
MAC Addresses	Allows or denies wireless access to clients with the specified MAC addresses. Accepted input MAC address formats are XX:XX:XX:XX:XX:XX and XX-XX-XX-XX-XX-XX. The display format shall be XX:XX:XX:XX:XX:XX.	GUI: 16 addresses; Non-Vol: 32 addresses. Customers can display more in GUI, if desired.	<NULL>

<Table 12> Access Control Settings Definitions



3.4 Wireless Advanced

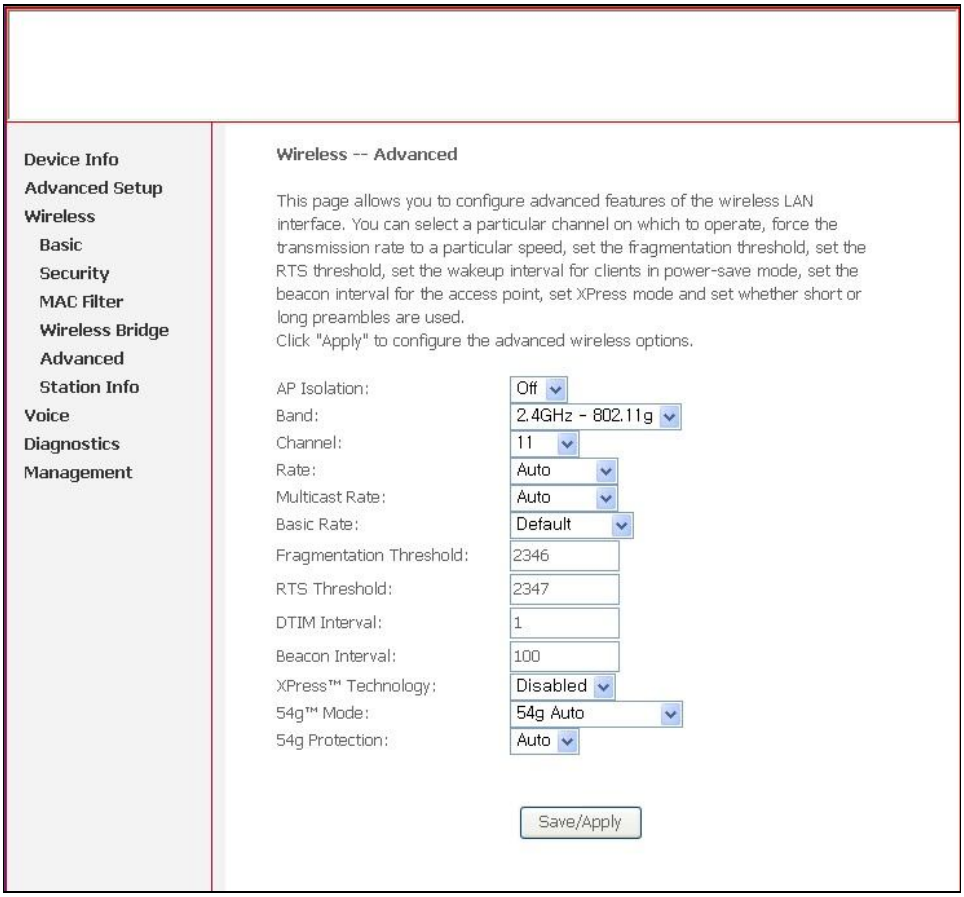
This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.

Click "Apply" to configure the advanced wireless options.

For maximum reliable link speed, it is recommended that Auto Rate is selected and the client and AP negotiate the best operating combination.

The settings shown in the image below are the default settings for 802.11g operation

The channel number is the 802.11 channel number used for transmitting and receiving data. When any of the above settings are changed, the Save/Apply button must be clicked in order to activate them.



The Beacon and DTIM Intervals should be left at 100 ms and 1 ms respectfully for successful operation with most client cards and WiFi¢ operation compliance. The Beacon Interval specifies how often packets are sent by the Access Point (AP) to synchronize a wireless network and its clients. The DTIM (Delivery Traffic Indication Message) Interval is a countdown informing the wireless clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. AP clients hear the beacons and awaken to receive the broadcast and multicast messages.

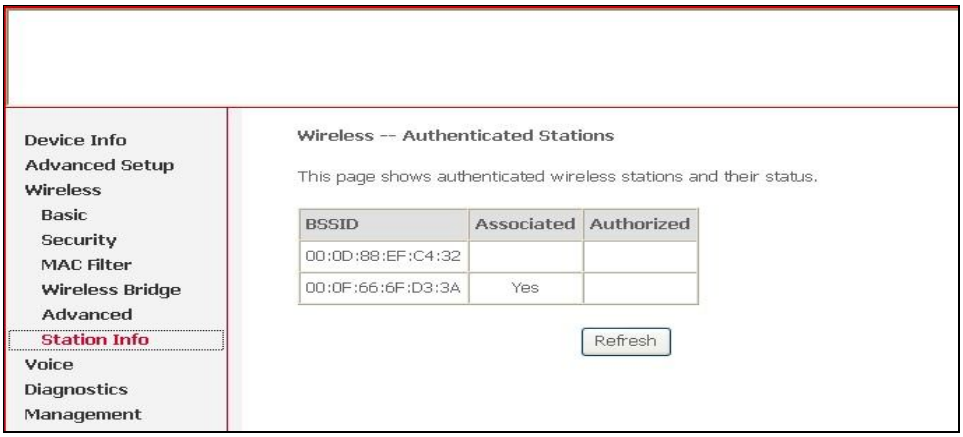
Fragmentation and RTS Thresholds should be set to 2346 bytes and 2347 bytes respectfully. Lesser settings can hurt data throughput as large frames could be fragmented or collisions could occur, especially when set below 1536 bytes, which could cause fragmentation of maximum size Ethernet frames.

Setting	Description	Value List or Range	Default

54g¢ Network Mode	Sets the network mode. Max Compatibility interoperates with the widest variety of 54g and 802.11b clients. 54g Only accepts only 54g clients. Max performance provides the highest throughout and accepts only 54g clients; nearby 802.11b networks may have degraded performance.	Max Compatibility, 54g Only, Max Performance	Max Compatibility
54g¢ Protection	In Auto mode the AP will use RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection Off to maximize 802.11g throughput under most conditions.	Off, Auto	Auto
Rate	Forces the transmission rate for the AP to a particular speed.	Auto, 1 Mbps, 2 Mbps, 5.5 Mbps, 6 Mbps, 9 Mbps, 11 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54 Mbps	Auto
Beacon Interval	Sets the beacon interval for the AP.	1..65535	100
DTIM Interval	Sets the wakeup interval for clients in power-save mode.	1..255	1
Fragmentation	Sets the fragmentation threshold.	256..2346	2346
RTS	Sets the RTS threshold.	1..2347	2347

<Table 13> Advanced Settings Definitions

3.5 Station Info



3.6 Wireless environment

This page recommends you where IAD should be located for Wireless efficiency.

► Should be away from Micro wave at least 5M.
If there is no way to avoid from microwave, set channel 1,2,12,13

► When IAD is located at the same place with Plasma lamp, set channel 11~13
Should be away from Bluetooth at least 5M

► If there is a walkie-talkie near IAD, should set the channel which is not covered the same Frequency.
- Channel 1 : 2410HHz
- Channel 2 : 2430HHz
- Channel 3 : 2450HHz
- Channel 4 : 2470HHz

► If more than 2 AP are used at the same location, add channel interval like below to avoid channel duplication. 1,6,11 or 1,5,9,13

This page intentionally left blank

DV-2010 User Manual

Visit us at
htDV-2010://www.davolink.com