DRAFT - 6/25/2010

User Guide

Wireless-N Broadband Home Router

Model: RMN302

DRAFT - 6/25/2010

Notice to Installers

The servicing instructions in this notice are for use by qualified service personnel only. To reduce the risk of electric shock, do not perform any servicing other than that contained in the operating instructions, unless you are qualified to do so.

Note to System Installer

For this apparatus, the cable shield/screen shall be grounded as close as practical to the point of entry of the cable into the building.For products sold in the US and Canada, this reminder is provided to call the system installer's attention to Article 820-93 and Article 820-100 of the NEC (or Canadian Electrical Code Part 1), which provides guidelines for proper grounding of the coaxial cable shield.

⚡ This symbol is intended to alert you that uninsulated voltage within this product may have sufficient magnitude to cause electric shock.Therefore, it is dangerous to make any kind of contact with any inside part of this product.

⚠ This symbol is intended to alert you of the presence of important operating and maintenance (servicing) instructions in the literature accompanying this product.

⚡ **CAUTION** ⚠

RISK OF ELECTRIC SHOCK
DO NOT OPEN

AVIS

RISQUE DE CHOC ÉLECTRIQUE
NE PAS OUVRIR

CAUTION: To reduce the risk of electric shock, do not remove cover (or back). No user-serviceable parts inside. Refer servicing to qualified service personnel.

WARNING

TO PREVENT FIRE OR ELECTRIC SHOCK, DO NOT EXPOSE THIS UNIT TO RAIN OR MOISTURE.

Notice à l'attention des installateurs de réseaux câblés

Les instructions relatives aux interventions d'entretien, fournies dans la présente notice, s'adressent exclusivement au personnel technique qualifié. Pour réduire les risques de chocs électriques, n'effectuer aucune intervention autre que celles décrites dans le mode d'emploi et les instructions relatives au fonctionnement, à moins que vous ne soyez qualifié pour ce faire.

Remarque à l'attention de l'installateur du système

Avec cet appareil, le blindage/écran du câble doit être mis à la terre aussi près que possible du point d'entrée du câble dans le bâtiment. En ce qui concerne les produits vendus aux États-Unis et au Canada, ce rappel est fourni pour attirer l'attention de l'installateur sur les articles 820-93 et 820-100 du Code national de l'électricité (ou Code de l'électricité canadien, Partie 1) qui fournissent des lignes directrices concernant la mise à la terre correcte du blindage (écran) du câble. coaxial

⚡ Ce symbole a pour but de vous prévenir que des tensions électriques non isolées existent à l'intérieur de ce produit, pouvant être d'une intensité suffisante pour causer des chocs électriques. Il est donc dangereux d'établir un contact quelconque avec l'une des pièces comprises à l'intérieur de ce produit.

⚠ Ce symbole a pour but de vous prévenir de la présence d'instructions importantes relatives au fonctionnement ou à l'entretien (et aux réparations) dans la documentation accompagnant ce produit.

⚡ **CAUTION** ⚠

RISK OF ELECTRIC SHOCK
DO NOT OPEN

ATTENTION

DANGER ÉLECTRIQUE
NE PAS OUVRIR

ATTENTION : Pour réduire les risques de chocs électriques, ne pas enlever le couvercle (ou le panneau arrière). Ne contient aucune pièce réparable par l'utilisateur. Confier les interventions aux techniciens d'entretien qualifiés.

AVERTISSEMENT

POUR ÉVITER LES INCENDIES OU LES CHOCS ÉLECTRIQUES, NE PAS EXPOSER L'APPAREIL À LA PLUIE OU À L'HUMIDITÉ.

Mitteilung für CATV-Techniker

Die in dieser Mitteilung aufgeführten Wartungsanweisungen sind ausschließlich für qualifiziertes Fachpersonal bestimmt. Um die Gefahr eines elektrischen Schlags zu reduzieren, sollten Sie keine Wartungsarbeiten durchführen, die nicht ausdrücklich in der Bedienungsanleitung aufgeführt sind, außer Sie sind zur Durchführung solcher Arbeiten qualifiziert.

Mitteilung an den Systemtechniker

Für dieses Gerät muss der Kabelschutz/Schirm so nahe wie möglich am Eintrittspunkt des Kabels in das Gebäude geerdet werden. Dieser Erinnerungshinweis liegt den in den USA oder Kanada verkauften Produkten bei.Er soll den Systemtechniker auf Paragraph 820-93 und Paragraph 820-100 der US- Elektrovorschrift NEC (oder der kanadischen Elektrovorschrift Canadian Electrical Code Teil 1) aufmerksam machen, in denen die Richtlinien für die ordnungsgemäße Erdung des Koaxialkabelschirms festgehalten sind.

⚡ Dieses Symbol weist den Benutzer auf das Vorhandensein von nicht isolierten gefährlichen Spannungen im Gerät hin, die Stromschläge verursachen können. Ein Kontakt mit den internen Teilen dieses Produktes ist mit Gefahren verbunden.

⚠ Dieses Symbol weist den Benutzer darauf hin, dass die mit diesem Produkt gelieferte Dokumentation wichtige Betriebs- und Wartungsanweisungen für das Gerät enthält.

⚡ **CAUTION** ⚠

RISK OF ELECTRIC SHOCK
DO NOT OPEN

ACHTUNG

STROMSCHLAGGEFAHR,
NICHT ÖFFNEN

ACHTUNG: Zur Vermeidung eines Stromschlags darf die Abdeckung (bzw. die Geräterückwand) nicht entfernt werden. Das Gerät enthält keine vom Benutzer wartbaren Teile. Wartungsarbeiten dürfen nur von qualifiziertem Fachpersonal durchgeführt werden.

AVERTISSEMENT

DAS GERÄT NICHT REGEN ODER FEUCHTIGKEIT AUSSETZEN, UM STROMSCHLAG ODER DURCH EINEN KURZSCHLUSS VERURSACHTEN BRAND ZU VERMEIDEN

Aviso a los instaladores de sistemas CATV

Las instrucciones de reparación contenidas en el presente aviso son para uso exclusivo por parte de personal de mantenimiento cualificado. Con el fin de reducir el riesgo de descarga eléctrica, no realice ninguna otra operación de reparación distinta a las contenidas en las instrucciones de funcionamiento, a menos que posea la cualificación necesaria para hacerlo.

Nota para el instalador del sistema

En lo que se refiere a este aparato, el blindaje del cable debe conectarse a tierra lo más cerca posible al punto por el cual el cable entra en el edificio. En el caso de los productos vendidos en los EE. UU. y Canadá, el presente aviso se suministra para llamar la atención del instalador del sistema sobre los Artículos 820-93 y 820-100 del NEC (o Código Eléctrico de Canadá, Parte 1), que proporcionan directrices para una correcta conexión a tierra del blindaje del cable coaxial.

⚡ Este símbolo tiene como fin advertirle de que una tensión sin aislamiento en el interior de este producto podría ser de una magnitud suficiente como para provocar una descarga eléctrica. Por consiguiente, resulta peligroso realizar cualquier tipo de contacto con alguno de los componentes internos de este producto.

⚠ Este símbolo tiene como fin alertarle de la presencia de importantes instrucciones de operación y mantenimiento (revisión) contenidas en la literatura que acompaña al producto.

⚡ **CAUTION** ⚠

RISK OF ELECTRIC SHOCK
DO NOT OPEN

ATENCIÓN

RIESGO DE DESCARGA
ELÉCTRICA NO ABRIR

ATENCIÓN: con el fin de reducir el riesgo de descarga eléctrica, no retire la tapa (ni la parte posterior). No existen en el interior componentes que puedan ser reparados por el usuario. Encargue su revisión a personal de mantenimiento cualificado.

ADVERTENCIA

PARA EVITAR EL RIESGO DE INCENDIO O DESCARGA ELÉCTRICA, NO EXPONGA LA UNIDAD A LA LLUVIA O A LA HUMEDAD.

IMPORTANT SAFETY INSTRUCTIONS

1) **Read these instructions.**
2) **Keep these instructions.**
3) **Heed all warnings.**
4) **Follow all instructions.**
5) **Do not use this apparatus near water.**
6) **Clean only with dry cloth.**
7) **Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.**
8) **Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.**
9) **Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding-type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.**
10) **Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.**
11) **Only use attachments/accessories specified by the manufacturer.**
12) **Use only with the cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with the apparatus. When a cart is used, use caution when moving the cart/apparatus combination to avoid injury from tip-over.**
13) **Unplug this apparatus during lightning storms or when unused for long periods of time.**
14) **Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as a power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.**

Power Source Warning

A label on this product indicates the correct power source for this product. Operate this product only from an electrical outlet with the voltage and frequency indicated on the product label. If you are uncertain of the type of power supply to your home or business, consult your service provider or your local power company.

The AC inlet on the unit must remain accessible and operable at all times.

Ground the Product

WARNING: Avoid electric shock and fire hazard! If this product connects to coaxial cable wiring, be sure the cable system is grounded (earthed). Grounding provides some protection against voltage surges and built-up static charges.

Protect the Product from Lightning

In addition to disconnecting the AC power from the wall outlet, disconnect the signal inputs.

Verify the Power Source from the On/Off Power Light

When the on/off power light is not illuminated, the apparatus may still be connected to the power source. The light may go out when the apparatus is turned off, regardless of whether it is still plugged into an AC power source.

Eliminate AC Mains Overloads

WARNING: Avoid electric shock and fire hazard! Do not overload AC mains, outlets, extension cords, or integral convenience receptacles. For products that require battery power or other power sources to operate them, refer to the operating instructions for those products.

Provide Ventilation and Select a Location

- Remove all packaging material before applying power to the product.
- Do not place this apparatus on a bed, sofa, rug, or similar surface.
- Do not place this apparatus on an unstable surface.
- Do not install this apparatus in an enclosure, such as a bookcase or rack, unless the installation provides proper ventilation.
- Do not place entertainment devices (such as VCRs or DVDs), lamps, books, vases with liquids, or other objects on top of this product.
- Do not block ventilation openings.

Protect from Exposure to Moisture and Foreign Objects

WARNING: Avoid electric shock and fire hazard! Do not expose this product to dripping or splashing liquids, rain, or moisture. Objects filled with liquids, such as vases, should not be placed on this apparatus.

WARNING: Avoid electric shock and fire hazard! Unplug this product before cleaning. Do not use a liquid cleaner or an aerosol cleaner. Do not use a magnetic/static cleaning device (dust remover) to clean this product.

WARNING: Avoid electric shock and fire hazard! Never push objects through the openings in this product. Foreign objects can cause electrical shorts that can result in electric shock or fire.

Service Warnings

WARNING: Avoid electric shock! Do not open the cover of this product. Opening or removing the cover may expose you to dangerous voltages. If you open the cover, your warranty will be void. This product contains no user-serviceable parts.

Check Product Safety

Upon completion of any service or repairs to this product, the service technician must perform safety checks to determine that this product is in proper operating condition.

Protect the Product When Moving It

Always disconnect the power source when moving the apparatus or connecting or disconnecting cables.

Telephone Equipment Notice

When using your telephone equipment, basic safety precautions should always be followed to reduce the risk of fire, electric stock and injury to persons, including the following:

1. Do not use this product near water, for example, near a bath tub, wash bowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
2. Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
3. Do not use the telephone to report a gas leak in the vicinity of the leak.

SAVE THESE INSTRUCTIONS

20090326_Modem No Battery_Safety

FCC Compliance

United States FCC Compliance

This device 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 such interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instructions, it may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment OFF and ON, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Any changes or modifications not expressly approved by Cisco Systems, Inc., could void the user's authority to operate the equipment.

The information shown in the FCC Declaration of Conformity paragraph below is a requirement of the FCC and is intended to supply you with information regarding the FCC approval of this device. *The phone numbers listed are for FCC-related questions only and not intended for questions regarding the connection or operation for this device. Please contact your service provider for any questions you may have regarding the operation or installation of this device.*

FC Declaration of Conformity

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

Cisco Wireless-N Broadband Home Router

Model: RMN302

Manufactured by:
Cisco Systems, Inc.
5030 Sugarloaf Parkway
Lawrenceville, Georgia 30044 USA
Telephone: 770-236-1077

Canada EMI Regulation

This Class B digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la class B est conforme à la norme NMB-003 du Canada.

FCC Part 68

The Federal Communications Commission (FCC) of the United States restricts specific uses of modems, and places registration responsibilities on both the manufacturer and the individual user.

1. The modem may not be connected to a party line or to a coin-operated telephone.
2. Notification to the telephone company is no longer required prior to connecting registered equipment, but upon request from the telephone company, the user shall tell the telephone company which line the equipment is connected to as well as the registration number and ringer equivalence number of the registered protective circuitry. FCC information is printed on a label on the bottom of the modem.

This equipment complies with Part 68 of FCC Rules and the requirements adopted by the ACTA. On the base unit of this equipment is a label that contains, among other information, a product identifier in the format US: GEMDL01BDDR2201V1. If requested, this number must be provided to the telephone company.

The REN is useful to determine the quantity of devices you may connect to your telephone line and still have those devices ring when your telephone number is called. In most, but not all areas, the sum of the REN of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices you may connect to your line, as determined by the REN, you should contact your local telephone company to determine the maximum REN for your calling area.

If your equipment causes harm to the telephone network, the telephone company may discontinue your service temporarily. If possible, they will notify you in advance. If advance notice is not practical, you will be notified as soon as possible. You will be informed of your right to file a complaint with the FCC. Your telephone company may make changes in its facilities, equipment, operations or procedures that could affect the proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with this telephone equipment, please contact the service provider for information on obtaining service or repairs.

The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.

This equipment may not be used on coin service provided by the telephone company. Connection to party lines is subject to state tariffs.

IC (Industry Canada) Notice

Notice: The Industry Canada (formerly Canadian Department of Communications) label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational, and safety requirements. The department does not guarantee the equipment will operate to the 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 (telephone extension cord). The customer should be aware that 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 may give the telecommunications company cause to request the user to disconnect the equipment. Users should ensure for their own protection 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: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.**

Radiation Exposure Statements

Note: This transmitter must not be co-located or operated in conjunction with any other antenna or transmitter. This equipment should be installed and operated with a minimum distance of 7.9 inches (20 cm) between the radiator and your body.

US

This system has been evaluated for RF exposure for humans in reference to ANSI C 95.1 (American National Standards Institute) limits. The evaluation was based on evaluation per ANI C 95.1 and FCC OET Bulletin 65C rev 01.01. The minimum separation distance from the antenna to general bystander is 7.9 inches (20 cm) to maintain compliance.

Canada

This system has been evaluated for RF exposure for humans in reference to ANSI C 95.1 limits. The evaluation was based on evaluation per RSS-102 Rev 2. The minimum separation distance from the antenna to general bystander is 7.9 inches (20 cm) to maintain compliance.

EU

This system has been evaluated for RF exposure for humans in reference to the ICNIRP (International Commission on Non-Ionizing Radiation Protection) limits. The evaluation was based on the EN 50385 Product Standard to Demonstrate Compliance of Radio Base Stations and Fixed Terminals for Wireless Telecommunications Systems with basic restrictions or reference levels related to Human Exposure to Radio Frequency Electromagnetic Fields from 300 MHz to 40 GHz. The minimum separation distance from the antenna to general bystander is 20 cm (7.9 inches).

Australia

This system has been evaluated for RF exposure for humans as referenced in the Australian Radiation Protection standard and has been evaluated to the ICNIRP (International Commission on Non-Ionizing Radiation Protection) limits. The minimum separation distance from the antenna to general bystander is 20 cm (7.9 inches).

20090317 FCC DSL_Dom and Intl

CE Compliance

Declaration of Conformity with Regard to the EU Directive 1999/5/EC (R&TTE Directive)

This declaration is only valid for configurations (combinations of software, firmware and hardware) supported or provided by Cisco Systems for use within the EU. The use of software or firmware not supported or provided by Cisco Systems may result in the equipment no longer being compliant with the regulatory requirements.

Български [Bulgarian]	Това оборудване отговаря на съществените изисквания и приложими клаузи на Директива 1999/5/ЕС.
Česky [Czech]:	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Eesti [Estonian]:	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
Français [French]:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviski [Latvian]:	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]:	Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.
Nederlands [Dutch]:	Dit apparaat voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-ħtiġiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Magyar [Hungarian]:	Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.
Norsk [Norwegian]:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]:	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC.
Português [Portuguese]:	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
Română [Romanian]	Acest echipament este in conformitate cu cerintele esentiale si cu alte prevederi relevante ale Directivei 1999/5/EC.
Slovensko [Slovenian]:	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC.
Slovensky [Slovak]:	Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC.
Suomi [Finnish]:	Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

Note: The full declaration of conformity for this product can be found in the Declarations of Conformity and Regulatory Information section of the appropriate product hardware installation guide, which is available on Cisco.com.

The following standards were applied during the assessment of the product against the requirements of the Directive 1999/5/EC:

- Radio: EN 300 328
- EMC: EN 301 489-1 and EN 301 489-17
- Safety: EN 60950 and EN 50385

The CE mark and class-2 identifier is affixed to the product and its packaging. This product conforms to the following European directives:

CE (!) -1999/5/EC

National Restrictions

This product is for indoor use only.

France

For 2.4 GHz, the output power is restricted to 10 mW EIRP when the product is used outdoors in the band 2454 - 2483,5 MHz. There are no restrictions when used in other parts of the 2,4 GHz band. Check http://www.arcep.fr/ for more details.

Pour la bande 2,4 GHz, la puissance est limitée à 10 mW en p.i.r.e. pour les équipements utilisés en extérieur dans la bande 2454 - 2483,5 MHz. Il n'y a pas de restrictions pour des utilisations dans d'autres parties de la bande 2,4 GHz. Consultez http://www.arcep.fr/ pour de plus amples détails.

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.comunicazioni.it/it/ for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.comunicazioni.it/it/ per maggiori dettagli.

Latvia

The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.

2,4 GHz frekven?u joslas izmantošanai ?rpus telp?m nepieciešama at?auja no Elektronisko sakaru direkcijas. Vair?k inform?cijas: http://www.esd.lv.

Note: The regulatory limits for maximum output power are specified in EIRP. The EIRP level of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

Antennas

Use only the antenna supplied with the product.

20090312 CE_Gateway

Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this guide. We reserve the right to change this guide at any time without notice.

Documentation Copyright Notice

Information in this document is subject to change without notice. No part of this document may be reproduced in any form without the express written permission of Cisco Systems, Inc.

Software and Firmware Use

The software described in this document is protected by copyright law and furnished to you under a license agreement. You may only use or copy this software in accordance with the terms of your license agreement.

The firmware in this equipment is protected by copyright law. You may only use the firmware in the equipment in which it is provided. Any reproduction or distribution of this firmware, or any portion of it, without our express written consent is prohibited.

U.S. Patents

A patent notice is affixed to this product. In addition, the product may also be covered by one or more of the following patents:

4,498,169, 4,692,919, 4,748,667; 4,829,569; 4,866,770; 4,885,775; 4,888,799; 4,890,319; 4,922,456; 4,922,532; 4,924,498; 4,965,534; 4,991,011; 5,003,384; 5,012,510; 5,029,207; 5,045,816; 5,053,883; 5,054,071; 5,058,160; 5,142,575; 5,142,690; 5,146,526; 5,155,590; 5,214,390; 5,225,902; 5,225,925; 5,235,619; 5,237,610; 5,239,540; 5,241,610; 5,247,364; 5,255,086; 5,257,403; 5,267,071; 5,270,809; 5,271,041; 5,272,752; 5,282,028; 5,285,497; 5,287,351; 5,301,028; 5,309,514; 5,317,391; 5,319,709; 5,341,425; 5,347,388; 5,347,389; 5,357,276; 5,359,601; 5,361,156; 5,367,571; 5,379,141; 5,379,145; 5,381,481; 5,390,337; 5,400,401; 5,406,558; 5,418,782; 5,420,866; 5,420,923; 5,425,101; 5,428,404; 5,430,568; 5,434,610; 5,436,749; 5,438,370; 5,440,632; 5,442,472; 5,455,570; 5,457,701; 5,471,492; 5,477,199; 5,477,262; 5,477,282 5,477,370; 5,481,389; 5,481,542; 5,485,221; 5,493,339; 5,497,187; 5,500,758; 5,502,499; 5,506,904; 5,519,780; 5,539,822; 5,550,825; 5,579,055; 5,579,057; 5,583,562; 5,592,551; 5,596,606; 5,600,378; 5,602,933; 5,640,388; 5,657,414; 5,675,575; 5,684,876; 5,715,515; 5,724,525; 5,734,822; 5,740,300; 5,742,677; 5,754,940; 5,757,416; 5,771,064; 5,774,859; 5,825,829; 5,826,167; 5,850,305; 5,854,703; 5,870,474; 5,892,607; 5,920,626; 5,923,755; 5,930,024; 5,930,515; 5,937,067; 5,963,352; 5,966,163; 5,982,424; 5,991,139; 5,999,207; 6,005,631; 6,005,938; 6,016,163; 6,028,941; 6,029,046; 6,052,384; 6,055,244; 6,072,532; 6,105,134; 6,148,039; 6,157,719; 6,188,729; 6,195,389; 6,212,278; 6,215,530; 6,219,358; 6,240,103; 6,243,145; 6,246,767; 6,252,964; 6,272,226; 6,292,081; 6,292,568; 6,320,131; 6,374,275; 6,405,239; 6,411,602; 6,417,949; 6,424,714; 6,424,717; 6,433,906; 6,438,139; 6,463,586; 6,467,091; 6,476,878; 6,493,876; 6,510,519; 6,516,002; 6,516,412; 6,526,508; 6,538,595; 6,546,013; 6,560,340; 6,567,118; 6,570,888; 6,622,308; 6,629,227; 6,664,984; 6,667,994; 6,671,879; 6,674,967; 6,678,891; 6,714,598; 6,721,352; 6,721,956; 6,725,459; 6,738,982; 6,744,892; 6,744,967; 6,751,271; 6,760,918; 6,795,972; 6,802,077; 6,804,708; 6,811,447; 6,817,028; 6,822,972; 6,823,385; 6,832,386; 6,845,106; 6,868,473; 6,874,075; 6,889,191; 6,909,471; 6,917,622; 6,917,628; 6,922,412; 6,927,806; 6,928,656; 6,931,058; 6,937,729; 6,969,279; 6,971,008; 6,971,121; 6,978,310; 6,986,156; 6,988,900; 6,996,838; 7,010,801; 7,053,960; 7,065,213; 7,069,578; 7,069572; D348065; D354959; D359737; D363932; D390217; D434753; D507240; D507535; D513407; D516518; RE36368; RE36988

20070417 Patents

DRAFT - 6/25/2010

Table of Contents

DRAFT - 6/25/2010

Product Overview

Thank you for choosing the Cisco® Wireless-N Broadband Home Router. The Router lets you access the Internet via a wireless connection or through one of its four (or five) switched ports.

You can also use the Router to share resources such as computers and storage. Various security features help to protect your data and your privacy while you are online. Security features include WPA2 security, a Stateful Packet Inspection (SPI) firewall, and NAT technology. Configuring the Router is easy using the provided browser-based utility.

Front Panel

Power (Green/Red) The Power LED lights up when the Router is powered on. It flashes during the self-test. The LED becomes red during a malfunction.

Internet (Green/Red)The Internet LED lights up when the Router is connected to the Internet. It flashes to indicate network activity over the Internet port. The LED becomes red when the Internet connection fails.

WAN (Green) The WAN LED corresponds with the WAN port and serves two purposes. If the LED is continuously lit, the Router is successfully connected to a device through that port. It flashes to indicate network activity over that port.

WAN MOCA (Green) Text TBD

LAN MOCA (Green)Text TBD

LAN 1-4 (Green) These numbered LEDs, corresponding with the numbered Ethernet ports on the Router's back panel, serve two purposes. If the LED is continuously lit, the Router is connected to a device through that port. It flashes to indicate network activity over that port.

WLAN (Green) The WLAN LED lights up when the wireless feature is enabled. It flashes when the Router is sending or receiving data over the wireless network.

USB 1 and 2 (Green) The USB LED lights up when the Router is connected to a device through the USB port. It flashes to indicate USB activity.

WPS (Green/Red) The WPS LED lights up when wireless security is enabled. It flashes during the Wi-Fi Protected Setup process. The LED becomes red when wireless security is disabled.

DRAFT - 6/25/2010

Top Panel

Wi-Fi Protected Setup If you have a client device, such as a wireless adapter, that supports Wi-Fi Protected Setup, then you can use Wi-Fi Protected Setup to automatically configure wireless security for your wireless network(s).

Note: Wi-Fi Protected Setup can only be used for the default wireless network. (The Router supports up to four wireless networks. The other three can be configured using the Router's web-based utility.)

Follow the appropriate instructions:

Method #1

Use this method if your client device has a Wi-Fi Protected Setup button.

1. Click or press the **Wi-Fi Protected Setup** button on the client device. (If Wi-Fi Protected Setup is an on-screen option, then select it.)
2. Click the **Wi-Fi Protected Setup** button on the top panel of the Router.
3. After the client device has been configured, refer back to your client device or its documentation for further instructions.

Method #2

Use this method if your client device has a Wi-Fi Protected Setup PIN number.

1. Access the Router's web-based utility.
2. Click the **Wireless** tab.
3. Click the **Wi-Fi Protected Setup** tab
4. Enter the client PIN number in the *PIN* field on this screen (the Router's ***Wi-Fi Protected Setup*** screen).
5. Click **Register**.

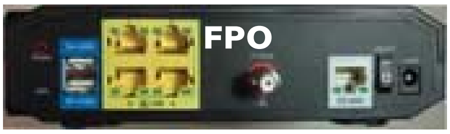
Method #3

Use this method if your client device asks for the Router's PIN number.

1. Enter the PIN number listed on the label on the bottom of the Router.
2. After the client device has been configured, refer back to your client device or its documentation for further instructions.

Note: Wi-Fi Protected Setup configures one client device at a time. Repeat the instructions for each client device that supports Wi-Fi Protected Setup.

Back Panel



Reset There are two ways to reset the Router's settings to factory defaults. Either press and hold the Reset button for approximately ten seconds, or restore the defaults from the Administration > Factory Defaults screen of the Router's web-based utility.

Note: The reset does not restore the voice settings to the factory defaults.

WPS Text TBD

USB The USB port connects to a USB storage device, such as a USB hard drive or flash disk.

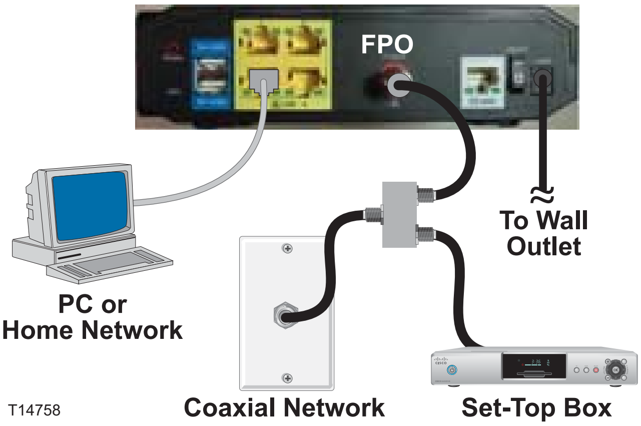
Ethernet LAN 1-4 These Ethernet ports (1, 2, 3, 4) connect the Router to wired computers and other Ethernet network devices.

F Connector Text TBD

Ethernet WAN/LAN5 The WAN/LAN5 port can act as a Wide Area Network (WAN) or Local Area Network (LAN) port. As a WAN port, it connects to a broadband modem. As a LAN port, it connects to a wired computer or other Ethernet network device.

Connecting to the Network

1. Use a coaxial cable to connect the F-Conn port on the RMN302 to the wall connector or to the coaxial network used to distribute IP data.
2. Use an Ethernet cable to connect the LAN port on the RMN302 to your home network or to a PC.
3. Attach the power adapter to the POWER port on the back of the RMN302, and plug it into a wall outlet.
4. Turn on the power switch.



Placement Positions

There are two ways to physically install the Router. The first way is to place the Router horizontally on a surface. The second way is to mount the Router on a wall.

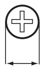
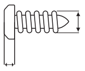
Horizontal Placement

The Router has four rubber feet on its bottom panel. Place the Router on a level surface near an electrical outlet.

Wall-Mounting Placement

The Router has four wall-mount slots on its bottom panel. The distance between two adjacent slots is 54 mm (2.13 inches).

Two screws are needed to mount the Router.

Suggested Mounting Hardware	
 4 to 5 mm	 2.5 to 3.0 mm 1 to 1.5 mm

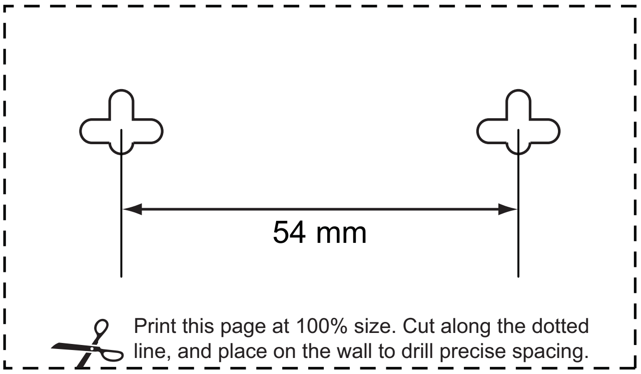
Note: Mounting hardware illustrations are not true to scale.

Note: Cisco is not responsible for damages incurred by insecure wall-mounting hardware.

Follow these instructions:

1. Determine where you want to mount the Router. Make sure that the wall you use is smooth, flat, dry, and sturdy. Also make sure the location is within reach of an electrical outlet.
2. Drill two holes into the wall. Make sure the holes are 54 mm (2.13 inches) apart.
3. Insert a screw into each hole and leave 2 mm (0.8 inches) below the head exposed.
4. Maneuver the Router so two of the wall-mount slots line up with the two screws.
5. Place the wall-mount slots over the screws and slide the Router down until the screws fit snugly into the wall-mount slots.

Note: To safely wall-mount the Router, the side panel with the antenna must face upward.



Print this page at 100% size. Cut along the dotted line, and place on the wall to drill precise spacing.

Wall Mounting Template

Wireless Security Checklist

Wireless networks are convenient and easy to install, so homes with high-speed Internet access are adopting them at a rapid pace. Because wireless networking operates by sending information over radio waves, it can be more vulnerable to intruders than a traditional wired network. Like signals from your cellular or cordless phones, signals from your wireless network can also be intercepted. Since you cannot physically prevent someone from connecting to your wireless network, you need to take some additional steps to keep your network secure.

1. Change the default wireless network name or SSID

Wireless devices have a default wireless network name or Service Set Identifier (SSID) set by the factory. This is the name of your wireless network, and can be up to 32 characters in length. Cisco wireless products use **cisco** as the default wireless network name. You should change the wireless network name to something unique to distinguish your wireless network from other wireless networks that may exist around you, but do not use personal information (such as your Social Security number) because this information may be available for anyone to see when browsing for wireless networks.

2. Change the default password

For wireless products such as access points, routers, and gateways, you will be asked for a password when you want to change their settings. These devices have a default password set by the factory. The Cisco default password is **admin**. Hackers know these defaults and may try to use them to access your wireless device and change your network settings. To thwart any unauthorized changes, customize the device's password so it will be hard to guess.

3. Enable MAC address filtering

Cisco routers and gateways give you the ability to enable Media Access Control (MAC) address filtering. The MAC address is a unique series of numbers and letters assigned to every networking device. With MAC address filtering enabled, wireless network access is provided solely for wireless devices with specific MAC addresses. For example, you can specify the MAC address of each computer in your home so that only those computers can access your wireless network.

4. Enable encryption

Encryption protects data transmitted over a wireless network. Wi-Fi Protected Access (WPA/WPA2) and Wired Equivalency Privacy (WEP) offer different levels of security for wireless communication.

A network encrypted with WPA/WPA2 is more secure than a network encrypted with WEP, because WPA/WPA2 uses dynamic key encryption. To protect the information as it passes over the airwaves, you should enable the highest level of encryption supported by your network equipment.

WEP is an older encryption standard and may be the only option available on some older devices that do not support WPA.

DRAFT - 6/25/2010

General Network Security Guidelines

Wireless network security is useless if the underlying network is not secure.

- Password protect all computers on the network and individually password protect sensitive files.
- Change passwords on a regular basis.
- Install anti-virus software and personal firewall software.
- Disable file sharing (peer-to-peer). Some applications may open file sharing without your consent and/or knowledge.

Additional Security Tips

- Keep wireless routers, access points, or gateways away from exterior walls and windows.
- Turn wireless routers, access points, or gateways off when they are not being used (at night, during vacations).
- Use strong passphrases that are at least eight characters in length. Combine letters and numbers to avoid using standard words that can be found in the dictionary.

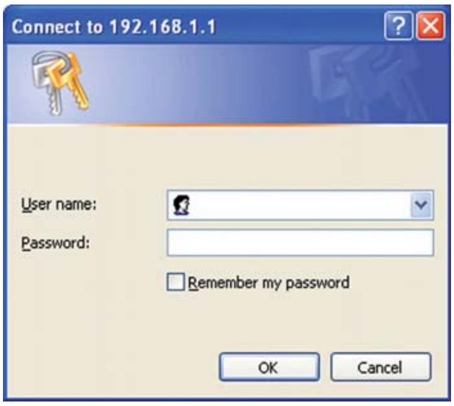
Web: For more information on wireless security, visit **www.linksysbycisco.com/security**

Advanced Configuration

To configure the Router, use its web-based utility. This chapter describes each web page of the utility and each page's key functions. You can access the utility via a web browser on a computer connected to the Router.

Note: If your service provider supplied you with the Router, then it may be pre-configured for you, and you will not need to make any changes. Contact your service provider for more information.

The web-based utility has these main tabs: Setup, Wireless, Storage, Security, Parental Control, Applications & Gaming, Administration, Status, and Advanced. Additional tabs will be available after you click one of the main tabs.



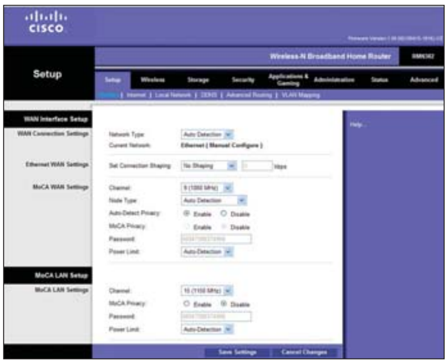
Login Screen

How to Access the Web-Based Utility

To access the web-based utility, launch the web browser on your computer, and enter the Router's default IP address, **192.168.1.1**, in the *Address* field. Then, press **Enter**.

A login screen appears. The first time you open the web-based utility, use the default user name and password, **admin and password**. (You can set a new user name and password from the Administration tab's *Management* screen.) Click **OK** to continue.

Note: If the Router was supplied by your service provider, then it may restrict access to the web-based utility. Contact your service provider for the login information.



Network Type: Auto Detection

Current Network: Ethernet (Manual Configure)

Set Connection Shaping: No Shaping kbps

Channel: 9 (1000 MHz)

Node Type: Auto Detection

Auto-Detect Privacy: ● Enable ○ Disable

MoCA Privacy: ○ Enable ● Disable

Password:

Power Limit: Auto-Detection

Channel: 15 (1150 MHz)

MoCA Privacy: ○ Enable ● Disable

Password:

Power Limit: Auto-Detection

Setup > Interface

Setup > Interface

WAN Interface Setup

WAN Connection Settings

Network Type: Choose your WAN interface type from the dropdown list. Options include Auto-Detection, MoCA, and Ethernet**.**

- **Auto Detection:** The router detects physical interface automatically and determine the connection type. The detect result is displayed in "Current Network" field;
- **MoCA:** You can manually configure MoCA connection as physical interface.
- **Ethernet:** You can manually configure the layer 2 network as Ethernet WAN connection

Current Network: Indicates whether the current WAN connection is MoCA or Ethernet WAN, and whether the connection is manually configured or auto-detected.

Ethernet WAN settings

Set Connection Shaping: Choose whether you want the router to smooth the ethernet bandwidth. Options include No Shaping, Auto(link speed) and Manual.

MoCA WAN settings

Channel: Allow the router to detect an available frequency for your MoCA WAN, or choose a channel frequency.

Node Type: Allow the router to detect your node type, or choose the correct option.

Auto-Detect privacy: Choose this option if you want to enable privacy auto detection.

MoCA Privacy: Choose this option if you want to enable privacy on your MoCA WAN connection.

Password: If you chose to enable privacy on your MoCA WAN, enter your password here.

Power Limit: Allow the router to set the limit for the transmission power on your MoCA WAN, or choose a percentage of power to use as a limit.

MoCA LAN Setup

MoCA LAN Settings

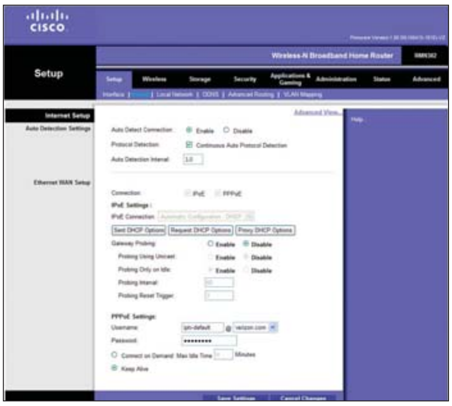
Channel: Allow the router to detect an available frequency for your MoCA LAN, or choose a channel frequency.

MoCA Privacy: Choose this option if you want to enable privacy on your MoCA LAN connection.

Password: If you chose to enable privacy on your MoCA LAN, enter your password here.

Power Limit: Allow the router to set the limit for the transmission power on your MoCA WAN, or choose a percentage of power to use as a limit.

Setup > Internet



Auto Detect Connection: ● Enable ○ Disable

Protocol Detection: ☑ Continuous Auto Protocol Detection

Auto Detection Interval: 1.0

Connection: ○ IPoE ○ PPPoE

IPoE Settings :

IPoE Connection: Automatic Configuration - DHCP [illegible]

Gateway Probing: ○ Enable ● Disable

Probing Using Unicast: ○ Enable ● Disable

Probing Only on Idle: ● Enable ○ Disable

Probing Interval: [illegible]

Probing Reset Trigger: [illegible]

PPPoE Settings:

Username: gm-default @ verizon.com

Password: •••••••••

○ Connect on Demand: Max Idle Time [illegible] Minutes

● Keep Alive

Setup > Internet

WAN Connection Settings

Network Type: Choose your network type. Connection Type

Auto Detection Settings

Auto Detect Connection: Allows you to enable or disable internet connection type auto detection.

Protocol Detection: Select this checkbox if you want the router to detect the internet connection continuously, as defined by the Auto Detection Interval.

Auto Detection Interval: Specify how often the router should detect the internet connection (if you chose Protocol Detection).

Ethernet WAN Setup

Connection Type: Choose whether your WAN uses IPoE (including DHCP and static IP) or PPPoE.

IPoE Settings

IPoE Connection: Need text.

Gateway Probing: Choose whether you want to probe the gateway if the gateway is alive. Select ARP to resolve MAC address by default.

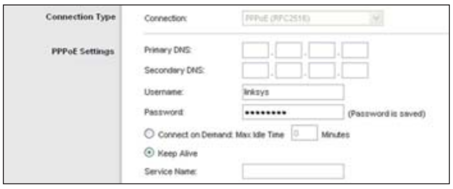
Probing Using Unicast: Choose whether you want to ping the gateway with an ICMP request.

Probing Only on Idle: Choose whether you want to restrict probing if traffic is going through router.

Probing Interval: Specify your probing interval, in seconds.

Probing Reset Trigger: Specify how long the probe should run before resetting the connection

PPPoE Settings for PPPoE (RFC2516)



Connection Type

Connection: PPPoE (RFC2516)

PPPoE Settings

Primary DNS: □.□.□.□

Secondary DNS: □.□.□.□

Username: linksys

Password: •••••••• (Password is saved)

○ Connect on Demand: Max Idle Time 0 Minutes

● Keep Alive

Service Name:

Setup > ADSL (WAN Connection for PVC) > PPPoE (RFC2516)

Primary (Required) and Secondary (Optional) DNS Enter the DNS (Domain Name System) server IP address(es) provided by your service provider. At least one is required.

Username and Password Enter the Username and Password provided by your service provider.

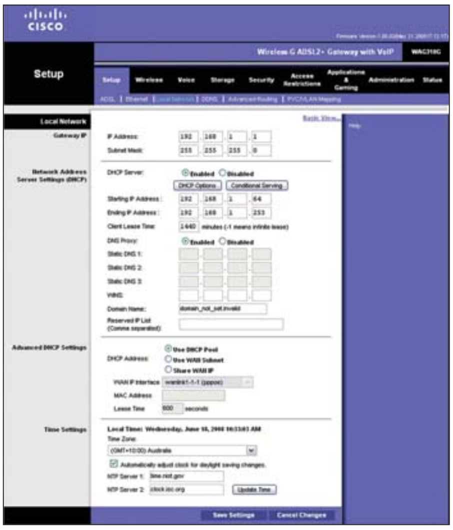
Connect on Demand: Max Idle Time You can configure the Router to cut the Internet connection after it has been inactive for a specified period of time (Max Idle Time). If your Internet connection has been terminated due to inactivity, Connect on Demand enables the Router to automatically re-establish your connection as soon as you attempt to access the Internet again. To use this option, select **Connect on Demand**. In the ***Max Idle Time*** field, enter the number of minutes you want to have elapsed before your Internet connection terminates. The default Max Idle Time is **5** minutes.

Keep Alive If you select this option, the Router will periodically check your Internet connection. If you are disconnected, then the Router will automatically re-establish your connection. To use this option, select **Keep Alive**.

Setup > Local Network

Configure the Router's Local Area Network (LAN) settings on this screen.

There are two views available, Basic and Advanced. The default view is Basic. To display the Advanced View, click **Advanced View**. To return to the Basic View, click **Basic View**.


cisco
Wireless G ADSL2+ Gateway with VoIP
WAG310G
Setup
Setup Wireless Voice Storage Security Access Restrictions Applications & Gaming Administration Status
ADSL | Ethernet | Local Network | DDNS | Advanced Routing | PVC/VLAN Mapping
Basic View...
Help...
Save Settings
Cancel Changes

Local Network

Gateway IP
IP Address: 192 . 168 . 1 . 1
Subnet Mask: 255 . 255 . 255 . 0

Network Address Server Settings (DHCP)
DHCP Server: ● Enabled ○ Disabled
DHCP Options | Conditional Serving
Starting IP Address: 192 . 168 . 1 . 64
Ending IP Address: 192 . 168 . 1 . 253
Client Lease Time: 1440 minutes (-1 means infinite lease)
DNS Proxy: ● Enabled ○ Disabled
Static DNS 1:
Static DNS 2:
Static DNS 3:
WINS:
Domain Name: domain_not_set.invalid
Reserved IP List (Comma separated):

Advanced DHCP Settings
DHCP Address: ● Use DHCP Pool ○ Use WAN Subnet ○ Share WAN IP
WAN IP Interface: wanlink1-1-1 (pppoe)
MAC Address:
Lease Time: 600 seconds

Time Settings
Local Time: Wednesday, June 18, 2008 10:33:03 AM
Time Zone:
(GMT+10:00) Australia
☑ Automatically adjust clock for daylight saving changes.
NTP Server 1: time.nist.gov
NTP Server 2: clock.isc.org
Update Time

Setup > Local Network (Advanced View)

Local Network

The Local Network section changes the settings on the network connected to the Router's Ethernet ports. Wireless setup is performed through the Wireless tab.

Router IP

The values for the Router's local IP Address and Subnet Mask are displayed. In most cases, keeping the default values will work.

IP Address The default value is **192.168.1.1**.

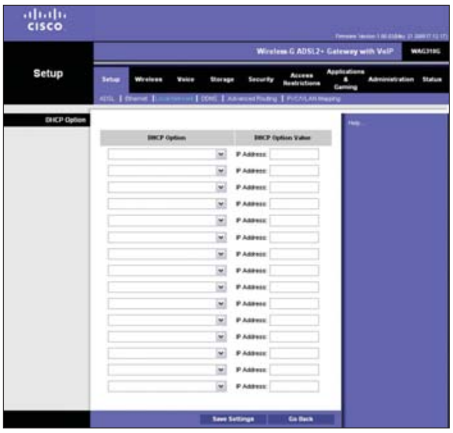
Subnet Mask The default value is **255.255.255.0**.

Network Address Server Settings (DHCP)

The settings allow you to configure the Router's Dynamic Host Configuration Protocol (DHCP) server function. The Router can be used as a DHCP server for your network. A DHCP server automatically assigns an IP address to each computer on your network. If you choose to enable the Router's DHCP server option, make sure there is no other DHCP server on your network.

DHCP Server A Dynamic Host Configuration Protocol (DHCP) server automatically assigns an IP address to each computer on your network for you. Unless you already have one, Cisco recommends that you keep the default, **Enabled**.

DHCP Options To configure DHCP options (available if DHCP is enabled), click this option. A new window appears.


cisco
Wireless G ADSL2+ Gateway with VoIP
WAG310G
Setup
Setup Wireless Voice Storage Security Access Restrictions Applications & Gaming Administration Status
ADSL | Ethernet | Local Network | DDNS | Advanced Routing | PVC/VLAN Mapping
Help...
Save Settings
Go Back

DHCP Option

DHCP Option	DHCP Option Value
	IP Address:
	IP Address:
	IP Address:
	IP Address:
	IP Address:
	IP Address:
	IP Address:
	IP Address:
	IP Address:
	IP Address:
	IP Address:
	IP Address:
	IP Address:
	IP Address:
	IP Address:

Setup > Local Network > DHCP Option

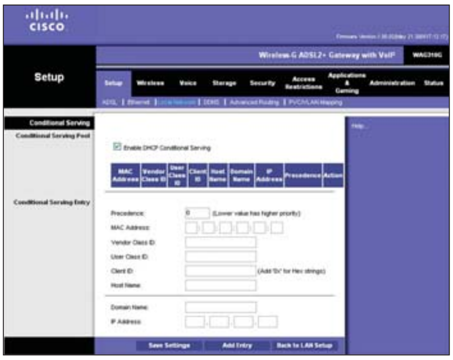
DHCP Option

- **DHCP Option** Select the appropriate setting.
- DHCP Option Value Enter the appropriate IP address, which is stored as a binary string on the Router. (No check is performed on these values.)

Click **Save Settings** to apply your changes, or click **Go Back** to cancel your changes and return to the *Local Network* screen.

Conditional Serving To configure the Conditional Serving Pool settings (available if DHCP is enabled), click this option. A new window appears.

Conditional Serving



☑ Enable DHCP Conditional Serving

Precedence: 0 (Lower value has higher priority)

MAC Address:

Vendor Class ID:

User Class ID:

Client ID: (Add '0x' for Hex strings)

Host Name:

Domain Name:

IP Address:

Setup > Local Network > Conditional Serving

Conditional Serving Pool

Enable DHCP Conditional Serving To enable this option, select the check box. Otherwise, leave the check box blank.

For each entry, the table lists the following: MAC Address, Vendor Class ID, User Class ID, Client ID, Host Name, Domain Name, IP Address, Precedence, and Action. To delete an entry, click **Delete**. To configure the DHCP options for an entry, click **DHCP Option**.

Conditional Serving Entry

Precedence Enter the Precedence value. A lower value indicates higher priority.

MAC Address Enter the MAC Address, if applicable as a filter condition.

Vendor Class ID Enter the Vendor Class ID, if applicable as a filter condition.

User Class ID Enter the User Class ID, if applicable as a filter condition.

Client ID Enter the Client ID, if applicable as a filter condition. This field accepts ASCII or hexadecimal strings. To enter a hexadecimal string, add **Ox** before the string.

Host Name Enter the Host Name, if applicable as a filter condition.

Domain Name If there is a match, the DHCP server will assign this Domain Name to the host.

IP Address If there is a match, the DHCP server will assign this IP Address to the host.

Click **Add Entry** to add a new entry to the table. Click **Save Settings** to apply your changes. Click **Back to LAN Setup** to return to the *Local Network* screen.

Starting IP Address Enter a value for the DHCP server to start with when issuing IP addresses. Because the Router's default IP address is 192.168.1.1, the Starting IP Address must be 192.168.1.2 or greater, but smaller than 192.168.1.253. The default is **192.168.1.64**.

Ending IP Address Specify the final IP address of the range available for assignment. The default is **192.168.1.253**.

Client Lease Time The Client Lease Time is the amount of time a network device will be allowed connection to the Router with its current dynamic IP address. Enter the number of minutes that the device will be "leased" this dynamic IP address. After the time is up, the device will be automatically assigned a new dynamic IP address. The default is **1440** minutes.

DNS Proxy (Advanced View) The Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. To use DNS Proxy, keep the default, **Enable**. Otherwise, select **Disable**.

Static DNS 1-3 (Advanced View) These entries are valid only when the DNS Proxy option is disabled. At least one DNS server IP address is provided by your service provider. You can enter up to three DNS server IP addresses here. The Router will use these for quicker access to functioning DNS servers.

WINS (Advanced View) The Windows Internet Naming Service (WINS) converts NetBIOS names to IP addresses. If you use a WINS server, enter that server's IP address here. Otherwise, leave this field blank.

Domain Name (Advanced View) Enter the Domain Name of your local network.

Reserved IP List (Advanced View) Enter the IP addresses you want to reserve, so they will not be leased to DHCP clients.

Advanced DHCP Settings (Advanced View)

DHCP Address This option defines the DHCP address allocation method. To assign local IP addresses from the DHCP pool you have defined, keep the default, **Use DHCP Pool**.

To have the local network devices share the WAN subnet address, select **Use WAN Subnet**. In this pass-through mode, the local computers get WAN-side IP addresses. They bypass NAT and are visible on the service provider's network. However, these computers can still communicate with other computers that are allocated private IP addresses.

To have a local network device share the WAN IP address, select **Share WAN IP**. In this mode, which is also known as super-DMZ mode, a single computer bypasses NAT. You can specify the computer's MAC address in the *MAC Address* field.

WAN IP Interface If you selected Use WAN Subnet or Share WAN IP, select the appropriate WAN IP connection to use.

MAC Address If you selected Share WAN IP, enter the MAC address of the local network device.

Lease Time Enter the number of seconds you want the local network device to lease the WAN IP address.

Time Settings (Advanced View)

Time Zone Select the time zone in which your network functions.

Automatically adjust clock for daylight saving changes Select this option if you want the Router to automatically adjust for daylight saving time.

NTP Server 1/2 Enter the URL (web address) of the Network Time Protocol (NTP) server you want to use. The default NTP servers are **time.nist.gov** and **clock.isc.org**.

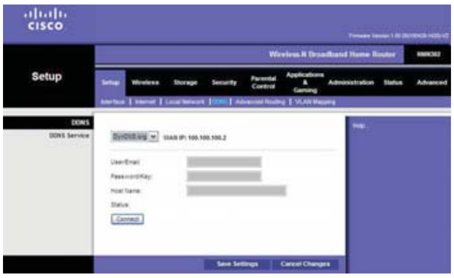
Update Time Click this option to immediately synchronize the Router with the NTP server.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Setup > DDNS

The Router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP address. It is useful when you are hosting your own website, FTP server, or other server behind the Router.

Before you can use this feature, you need to sign up for DDNS service with a DDNS service provider, www.dyndns.org or www.TZO.com. If you do not want to use this feature, keep the default, **Disabled**.



DDNS Service DynDNS.org WAN IP: 100.100.100.2

User/Email:

Password/Key:

Host Name:

Status:

Setup > DDNS

DDNS

DDNS Service

Disabled/DynDNS.org/TZO.com If your DDNS service is provided by DynDNS.org, then select **DynDNS.org** from the drop-down menu. If your DDNS service is provided by TZO, then select **TZO.com**. The features available on the *DDNS* screen will vary, depending on which DDNS service provider you use.

WAN IP The WAN IP address of the Router is displayed.

User/Email Enter the user name or e-mail address for your account.

Password/Key Enter the password or key for your account.

Host Name Enter the DDNS URL assigned by the service.

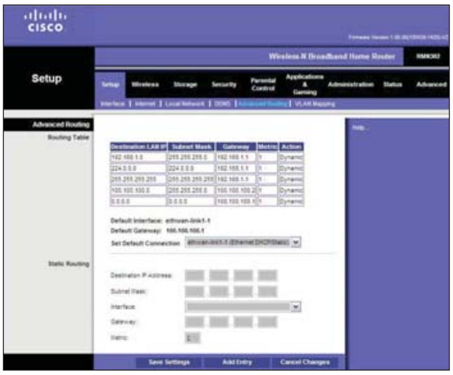
Status The status of the DDNS service connection is displayed.

Connect To manually trigger an update, click this button.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Setup > Advanced Routing

This screen is used to set up the Router's advanced routing functions. Static Routing sets up a fixed route to another network destination.



Destination LAN IP	Subnet Mask	Gateway	Metric	Action
192.168.1.0	255.255.255.0	192.168.1.1	1	Dynamic
224.0.0.0	224.0.0.0	192.168.1.1	1	Dynamic
255.255.255.255	255.255.255.255	192.168.1.1	1	Dynamic
100.100.100.0	255.255.255.0	100.100.100.2	1	Dynamic
0.0.0.0	0.0.0.0	100.100.100.1	1	Dynamic

Default Interface: ethwan-link1-1

Default Gateway: 100.100.100.1

Set Default Connection: ethwan-link1-1 (Ethernet DHCP/Static)

Destination IP Address:

Subnet Mask:

Interface:

Gateway:

Metric: 1

Setup > Advanced Routing

Advanced Routing

Routing Table

For each route, the Destination LAN IP address, Subnet Mask, Router, and Metric are displayed. In the Action column, click **Delete** to delete a static route.

Default Interface The default Layer 3 connection is displayed.

Default Router The default next-hop gateway of the default interface is displayed.

Default Connection This advanced setting usually indicates the default connection since the Router supports multiple WAN connections. If the Router has multiple connections, specify which one is the default.

Static Routing

A static route is a pre-determined pathway that network information must travel to reach a specific host or network. Enter the information described below to set up a new static route.

Note: When you add a static route, certain rules apply. For example, the Router must belong to the subnet of any of the router's interfaces.

Destination IP Address The Destination IP Address is the IP address of the remote network or host to which you want to assign a static route.

Subnet Mask The Subnet Mask determines which portion of a Destination IP Address is the network portion, and which portion is the host portion.

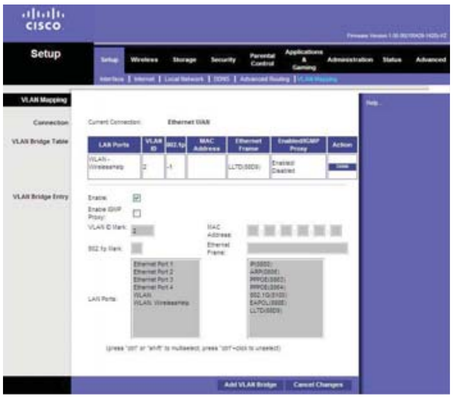
Router This is the IP address of the gateway device that allows for contact between the Router and the remote network or host.

Metric This is the number of hops to each node until the destination is reached (16 hops maximum). Enter the appropriate Metric. The default is **1**.

To save the static route you have configured, click **Add Entry**. Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

DRAFT - 6/25/2010

Setup > PVC/VLAN Mapping



Current Connection: Ethernet WAN

LAN Ports	VLAN ID	802.1p	MAC Address	Ethernet Frame	Enabled/IGMP Proxy	Action
WLAN - Wirelessnetp	2	-1		LLTD(88D9)	Enabled Disabled	Delete

Enable: ☑

Enable IGMP Proxy: □

VLAN ID Mark: 2

802.1p Mark:

MAC Address:

Ethernet Frame:

LAN Ports: Ethernet Port 1
Ethernet Port 2
Ethernet Port 3
Ethernet Port 4
WLAN
WLAN: Wirelessnetp

IP(0800)
ARP(0806)
PPPOE(8863)
PPPOE(8864)
802.1Q(8100)
EAPOL(888E)
LLTD(88D9)

(press "ctrl" or "shift" to multiselect, press "ctrl"+click to unselect)

Setup > PVC/VLAN Mapping

This advanced screen is used to map the PVCs to the Virtual Local Area Networks (VLANs). When you create a mapping, a layer 2 bridge is formed between the Router's LAN port (including WLAN SSID) and WAN port (PVC or Ethernet WAN).

You should configure this screen according to your service provider's instructions. For example, when Ethernet port 1 is connected to a set-top box, a PVC mapping is created for Ethernet port 1 and PVC 1 with VLAN 1002. Traffic is marked with the configured VLAN ID when it travels to the service provider's network.

PVC VLAN Mapping

Select PVC Connection Select the PVC you want to map.

VLAN Bridge Table

For each entry, the table lists the following: LAN Ports, VLAN ID, 802.1p, MAC Address, Ethernet Frame, Enable status, and Action. To delete an existing PVC/VLAN mapping, click **Delete**.

VLAN Bridge Entry

Enabled Select **Enabled** to enable the mapping rule.

VLAN ID Enter the VLAN you want to map. The default is **2**.

MAC Address Enter the packet's source MAC address, if applicable as a filter condition.

802.1p Enter the priority level for each port. These are the mappings to 802.1p:

- 6 High (highest, EF)
- 5 Medium (CS)
- 4 Normal (CS)
- 0 Low (best effort)
- -1 No Change (no change to the original 802.1p value)

Cisco recommends the following:

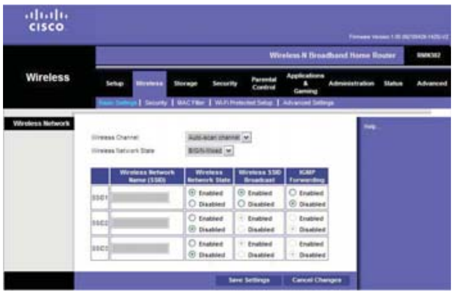
- For voice and video traffic, enter **6**.
- For gaming or mission-critical traffic, enter **5**.
- For normal traffic, enter **4**.
- For low-priority traffic, enter **0**.

LAN Ports Every LAN interface is listed, including the Ethernet ports and Wireless Local Area Network (WLAN) ports. (The WLAN ports are listed with their wireless network names, also known as SSIDs.) Select the appropriate LAN interface. For multiple selection, press the **Ctrl** or **Shift** key. To deselect, use **Ctrl + click** (click the selection).

Ethernet Frame The Ethernet frame types are listed. Select the packet's Ethernet frame type, if applicable as a filter condition. For multiple selection, press the **Ctrl** or **Shift** key. To deselect, use **Ctrl + click** (click the selection).

Click **Add VLAN Bridge** to create a new PVC/VLAN mapping, or click **Cancel Changes** to cancel your changes.

Wireless > Basic Settings



Wireless Channel: Auto-scan channel

Wireless Network State: B/G/N-Mixed

	Wireless Network Name (SSID)	Wireless Network State	Wireless SSID Broadcast	IGMP Forwarding
SSID1		● Enabled ○ Disabled	● Enabled ○ Disabled	○ Enabled ● Disabled
SSID2		○ Enabled ● Disabled	● Enabled ○ Disabled	○ Enabled ● Disabled
SSID3		○ Enabled ● Disabled	● Enabled ○ Disabled	○ Enabled ● Disabled

Wireless > Basic Settings

The basic settings for wireless networking are set on this screen.

There are two ways to configure the Router's wireless settings, manual and Wi-Fi Protected Setup. For manual configuration, use this screen to change the settings.

Wi-Fi Protected Setup is a feature that makes it easy to set up your wireless network. If you have devices that support Wi-Fi Protected Setup, then click the **Wi-Fi Protected Setup** tab, and follow the on-screen instructions (refer to the "Wireless > Wi-Fi Protected Setup" section for more information).

Note: Wi-Fi Protected Setup can only be used for the default wireless network. (The Router supports up to four wireless networks. The other three can be configured using the Router's web-based utility.)

Wireless Network

Wireless Channel Select the channel you want to use. All devices in your wireless network must use the same channel in order to communicate.

Wireless Network State Select the wireless standards running on your network. If you have Wireless-G and Wireless-B devices in your network, keep the default, **Mixed**. If you have only Wireless-G devices, select **G-Only**. If you have only Wireless-B devices, select **B-Only**. If you do not have any wireless devices, select **Disabled**.

The Router supports up to four wireless networks. By default, only the first wireless network is enabled. On the *Wireless Security* and *MAC Filter* screens, you can configure different security settings and MAC filtering rules for each wireless network.

Configure the following settings for each wireless network (SSID1-4):

Wireless Network Name (SSID) The network name is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Cisco recommends that you change the default name of the first network, **linksys1**, to a unique name of your choice.

Wireless Network State If you want to use the wireless network, select **Enabled**. Otherwise, select **Disabled**.

Wireless SSID Broadcast When wireless devices survey the local area for wireless networks to associate with, they will detect the wireless network name or SSID broadcast by the Router. If you want to broadcast the Router's SSID, keep the default, **Enabled**. Otherwise, select **Disabled**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Wireless > Security

The *Security* screen configures the security of your wireless network(s). The Router supports the following wireless security mode options: WPA2-Personal, WPA-Personal, WEP, WPA-Enterprise, and WPA2-Enterprise. (WPA stands for Wi-Fi Protected Access, which is a security standard stronger than WEP encryption, and WEP stands for Wired Equivalent Privacy.) For detailed instructions on configuring wireless security for the Router, refer to "Wireless Security Checklist" on page 7.

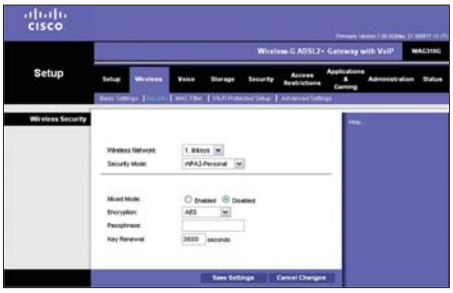
Note: If you used Wi-Fi Protected Setup to configure your wireless network(s), then wireless security has already been set up. Do not make changes to the *Wireless Security* screen.

Wireless Security

Wireless Network Select the wireless network you want to configure.

Security Mode Select the security method for your wireless network. Proceed to the appropriate instructions. If you do not want to use wireless security, keep the default, **Off**.

> **Note:** If you are using wireless security, remember that each device in your wireless network MUST use the same security method and settings, or else the wireless devices cannot communicate.



Wireless Network: 1. linksys
Security Mode: WPA2-Personal
Mixed Mode: ○ Enabled ● Disabled
Encryption: AES
Passphrase:
Key Renewal: 3600 seconds

Security Mode > WPA2-Personal

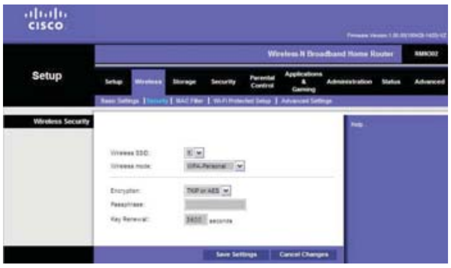
WPA2-Personal

Mixed Mode Select **Enabled** to support both WPA and WPA2 clients. Otherwise, keep the default, **Disabled**.

Encryption Select the appropriate method, **AES** or **TKIP or AES**.

Passphrase Enter a Passphrase (also called a WPA shared key) of 8-63 characters.

Key Renewal Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. The default is **3600** seconds.



Wireless SSID: 5
Wireless mode: WPA-Personal
Encryption: TKIP or AES
Passphrase:
Key Renewal: 3600 seconds

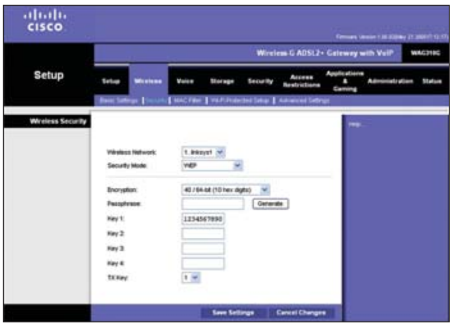
Security Mode > WPA-Personal

WPA-Personal

Encryption TKIP is automatically selected.

Passphrase Enter a Passphrase (also called a WPA shared key) of 8-63 characters.

Key Renewal Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. The default is **3600** seconds.



Wireless Network: 1. linksys1
Security Mode: WEP
Encryption: 40 / 64-bit (10 hex digits)
Passphrase:
Key 1: 1234567890
Key 2:
Key 3:
Key 4:
TX Key: 1

Security Mode > WEP

WEP

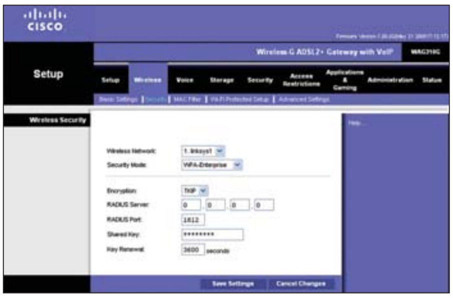
Encryption Select a level of WEP encryption, **40/64-bit (10 hex digits)** or **104/128-bit (26 hex digits)**.

Passphrase Enter a Passphrase to automatically generate WEP keys. Then click **Generate**.

> **Note:** The WEP Passphrase is compatible with Cisco wireless products only. If you are using non-Cisco products, manually enter the appropriate WEP key on those devices.

Key 1-4 If you did not enter a Passphrase, enter the WEP key(s) manually.

TX Key Select which TX (Transmit) Key to use. The default is **1**.



Wireless Network: 1. linksys1
Security Mode: WPA-Enterprise
Encryption: TKIP
RADIUS Server: 0 . 0 . 0 . 0
RADIUS Port: 1812
Shared Key: ********
Key Renewal: 3600 seconds

Security Mode > WPA Enterprise

WPA Enterprise

This option features WPA used in coordination with a RADIUS server. (RADIUS stands for Remote Authentication Dial-In User Service. This option should only be used when a RADIUS server is connected to the Router.)

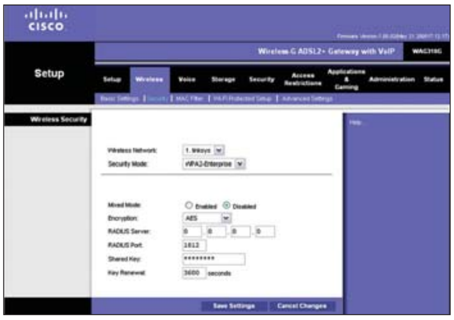
Encryption TKIP is automatically selected.

RADIUS Server Enter the IP address of the RADIUS server.

RADIUS Port Enter the port number of the RADIUS server. The default value is **1812**.

Shared Key Enter the key shared between the Router and the server.

Key Renewal Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. The default is **3600** seconds.



Wireless Network: 1. linksys

Security Mode: WPA2-Enterprise

Mixed Mode: ○ Enabled ● Disabled

Encryption: AES

RADIUS Server: 0 . 0 . 0 . 0

RADIUS Port: 1812

Shared Key: ********

Key Renewal: 3600 seconds

Security Mode > WPA2 Enterprise

WPA2 Enterprise

This option features WPA2 used in coordination with a RADIUS server. (It should only be used when a RADIUS server is connected to the Router.)

Mixed Mode Select **Enabled** to support both WPA and WPA2 clients. Otherwise, keep the default, **Disabled**.

Encryption Select the appropriate method, **AES** or **TKIP** or **AES**.

RADIUS Server Enter the IP address of the RADIUS server.

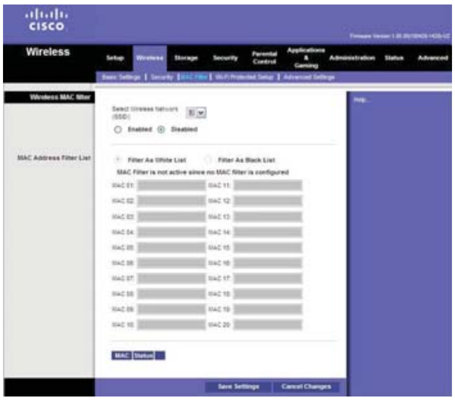
RADIUS Port Enter the port number of the RADIUS server. The default value is **1812**.

Shared Key Enter the key shared between the Router and the server.

Key Renewal Enter a Key Renewal period, which instructs the Router how often it should change the encryption keys. The default is **3600** seconds.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Wireless > MAC Filter



Select Wireless Network (SSID)

○ Enabled ● Disabled

○ Filter As White List ○ Filter As Black List

MAC Filter is not active since no MAC filter is configured

MAC 01: MAC 11:
MAC 02: MAC 12:
MAC 03: MAC 13:
MAC 04: MAC 14:
MAC 05: MAC 15:
MAC 06: MAC 16:
MAC 07: MAC 17:
MAC 08: MAC 18:
MAC 09: MAC 19:
MAC 10: MAC 20:

Wireless > MAC Filter

Wireless access can be filtered by using the MAC addresses of the wireless devices transmitting within your network's radius.

Wireless MAC Filter

Select Wireless Network (SSID) Select the wireless network you want to configure.

Enabled/Disabled To use the wireless MAC filter, select **Enabled**. Otherwise, keep the default, **Disabled**.

MAC Address Filter

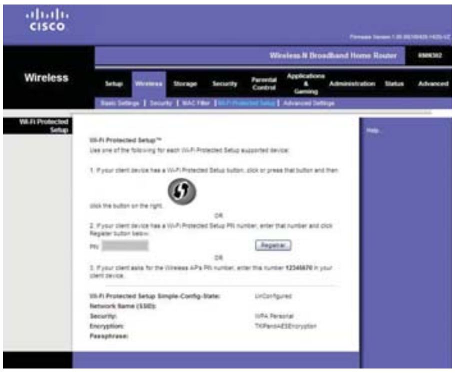
Filter As White List/Filter As Black List To allow access by network devices with the MAC addresses on this list, select **Filter As White List**. To block access by network devices with the MAC addresses on this list, keep the default, **Filter As Black List**.

MAC 01-20 Enter the MAC addresses of the devices whose wireless access you want to block or allow.

For each wireless device, its MAC address and connection status are listed. To copy a MAC address to one of the *MAC 01-20* fields, click **Copy**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Wireless > Wi-Fi Protected Setup



Wi-Fi Protected Setup™

Use one of the following for each Wi-Fi Protected Setup supported device:

1. If your client device has a Wi-Fi Protected Setup button, click or press that button and then click the button on the right.

OR

2. If your client device has a Wi-Fi Protected Setup PIN number, enter that number and click Register button below.

PIN:

OR

3. If your client asks for the Wireless AP's PIN number, enter this number **12345670** in your client device.

Wi-Fi Protected Setup Simple-Config-State: UnConfigured

Network Name (SSID):

Security: WPA Personal

Encryption: TKIPandAESEncryption

Passphrase:

Wireless > Wi-Fi Protected Setup

There are two ways to configure the Router's wireless settings, manual and Wi-Fi Protected Setup. For manual configuration, click the **Basic Settings** tab (refer to the "Wireless > Basic Settings" section for more information).

Wi-Fi Protected Setup is a feature that makes it easy to set up your wireless network. If you have devices that support Wi-Fi Protected Setup, then use the following instructions.

Note: Wi-Fi Protected Setup can only be used for the default wireless network. (The Router supports up to four wireless networks. The other three can be configured using the *Wireless > Basic Settings* screen of the Router's web-based utility.)

Wi-Fi Protected Setup

If you have client devices, such as a wireless adapter, that support Wi-Fi Protected Setup, then you can use Wi-Fi Protected Setup to automatically configure wireless security for your wireless network(s).

There are three methods available. Use the method that applies to the client device you are configuring.

Note: Wi-Fi Protected Setup configures one client device at a time. Repeat the instructions for each client device that supports Wi-Fi Protected Setup.

Method #1

Use this method if your client device has a Wi-Fi Protected Setup button.

1. Click or press the **Wi-Fi Protected Setup** button on the client device. (If Wi-Fi Protected Setup is an on-screen option, then select it.)
2. Click the **Wi-Fi Protected Setup** button on this screen.
3. After the client device has been configured, click **OK**. Then refer back to your client device or its documentation for further instructions.

Method #2

Use this method if your client device has a Wi-Fi Protected Setup PIN number.

1. Enter the client PIN number in the *PIN* field on this screen (the Router's *Wi-Fi Protected Setup* screen).
2. Click **Register**.

Method #3

Use this method if your client device asks for the Router's PIN number.

1. Enter the PIN number listed on this screen. (It is also listed on the label on the bottom of the Router.)
2. After the client device has been configured, click **OK**. Then refer back to your client device or its documentation for further instructions.

At the bottom of the screen, status information for your wireless security is displayed:

Wi-Fi Protected Setup Simple-Config-State The status of the Wi-Fi Protected Setup feature is displayed. The default is **Not configured**. After the Router has been configured, the status changes to "Configured".

Network Name (SSID) The name of the wireless network is displayed.

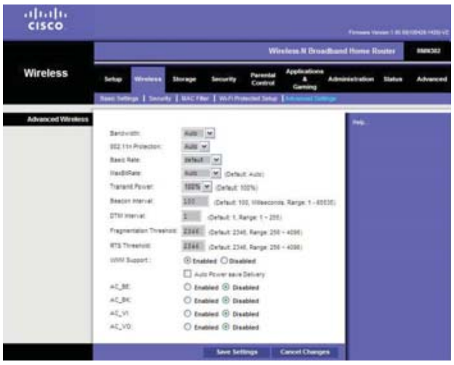
Security The security method of the wireless network is displayed.

Encryption The encryption method, such as TKIP or AES, is displayed.

Passphrase The passphrase for the wireless security method is displayed. It acts like a password for access to the wireless network. (For WPA security methods, the passphrase is also known as a WPA shared key.)

Note: If you have client devices that do not support Wi-Fi Protected Setup, note the wireless settings, and then manually configure those client devices.

Wireless > Advanced Settings



Bandwidth: Auto

802.11n Protection: Auto

Basic Rate: default

MaxBitRate: Auto (Default: Auto)

Transmit Power: 100% (Default: 100%)

Beacon Interval: 100 (Default: 100, Milliseconds, Range: 1 - 65535)

DTIM Interval: 1 (Default: 1, Range: 1 - 255)

Fragmentation Threshold: 2346 (Default: 2346, Range: 256 - 4096)

RTS Threshold: 2346 (Default: 2346, Range: 256 - 4096)

WMM Support: ● Enabled ○ Disabled

□ Auto Power save Delivery

AC_BE: ○ Enabled ● Disabled

AC_BK: ○ Enabled ● Disabled

AC_VI: ○ Enabled ● Disabled

AC_VO: ○ Enabled ● Disabled

Wireless > Advanced Settings

Use this screen to set up the Router's advanced wireless settings, which apply to all of the Router's wireless networks. These settings should only be adjusted by an expert administrator as incorrect settings can reduce wireless performance.

Advanced Wireless

Basic Rate The Basic Rate setting is not actually one rate of transmission but a series of rates at which the Router can transmit. The Router will advertise its Basic Rate to the other wireless devices in your network, so they know which rates will be used. The Router will also advertise that it will automatically select the best rate for transmission. Select the appropriate option: **Default**, for transmission at all standard wireless rates; **1-2Mbps**, for use with older wireless technology; **All**, for transmission at all wireless rates; or **Wi-Fi Alt**. For the Wi-Fi Alt option, basic rates are 1, 2, 5.5, 6, 11, 12, and 24 Mbps; supported rates are 9, 18, 36, 48, and 54 Mbps. If you are not sure which rate to select, keep the default, **Default**.

CTS Protection Mode CTS (Clear-To-Send) Protection Mode's default is **Disabled**. Select **Auto** if you want the device to automatically use CTS Protection Mode when your Wireless-G products are experiencing severe problems and are not able to transmit to the device in an environment with heavy 802.11b traffic. This function boosts the device's ability to catch all Wireless-G transmissions but will severely decrease performance.

Control TX Rate The Control TX Rate should be set depending on the speed of your wireless network. Select from a range of transmission speeds, or keep the default, **Auto**. When the Auto setting is selected, the Router automatically uses the fastest possible data rate and enables the Auto-Fallback feature, which negotiates the best possible connection speed between the Router and a wireless device.

Wireless Afterburner To improve wireless performance when the Router is used with devices that support SpeedBooster, select **Enable**. Otherwise, keep the default, **Disable**.

Beacon Interval Enter a value between 1 and 65,535 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the Router to synchronize the wireless network(s). The default value is **100**.

DTIM Interval This value, between 1 and 255, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is **1**.

Fragmentation Threshold This value specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor reduction of the default value is recommended. In most cases, it should remain at its default value of **2346**.

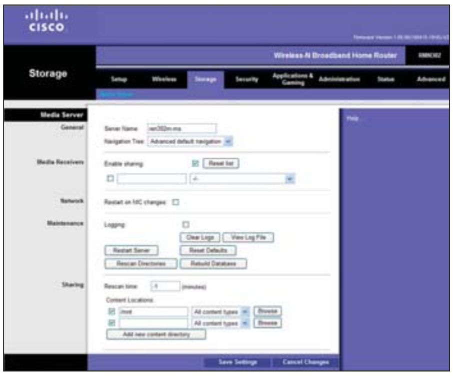
RTS Threshold Should you encounter inconsistent data flow, only minor reduction of the default, **2346**, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The RTS Threshold value should remain at its default value of **2346**.

WMM Support The Router supports Wi-Fi Multimedia (WMM) for Quality of Service (QoS). When WMM Support is enabled, it provides four priority queues for different types of traffic. It automatically maps the incoming packets to the appropriate queues based on QoS settings (in the IP or layer 2 header). WMM provides the capability to prioritize traffic in your environment. If you have other devices on your network that support WMM, select **Enable**. Otherwise, keep the default, **Disable**.

Auto Power Save Delivery Unscheduled Automatic Power Save Delivery (UAPSD) is a special power-saving mode to achieve end-to-end QoS. This option is available if you enabled WMM Support. To use the power save feature, select **Auto Power save Delivery**.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Storage > Media Server



Server Name: ren302m-ms

Navigation Tree: Advanced default navigation

Enable sharing: ☑

☐

Restart on NIC changes: ☐

Logging: ☐

Rescan time: 1 (minutes)

Content Locations

☑ /mnt All content types

☑ All content types

Storage > MediaServer

General

Server Name: Type your Media server name.

Navigation Tree: Choose the way that you want to view the navigation tree, folder structure, and so on.

Media Receivers

Enable Sharing: Choose whether you want to enable media sharing.

Network

Restart on NIC changes: Choose whether you want to restart router when NIC changes are received.

Maintenance

Logging: Choose whether you want to enable media server logging.

Clear logs: Click to clear media server logs.

View Log File: Click to view the media server log.

Restart Server: Click to restart the server.

Reset Defaults: Will remove later

Rescan Directories: Click to scan the content directory manually.

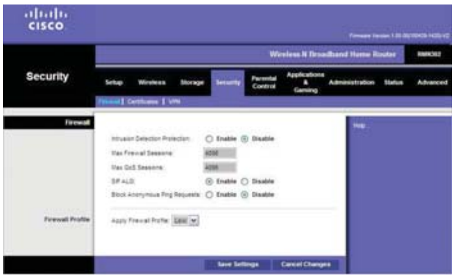
Rebuild Database: Click to delete the database file from the media server and rebuild a new one. This may take 5 seconds.

Sharing

Rescan time: Specify how often the media server may iteratively scan the content directory.

Content Locations: Specify the location of the content directory on the media server. The default location is already configured.

Security > Firewall



Intrusion Detection Protection: ○ Enable ● Disable
Max Firewall Sessions: 4096
Max QoS Sessions: 4096
SIP ALG: ● Enable ○ Disable
Block Anonymous Ping Requests: ○ Enable ● Disable
Apply Firewall Profile: Low

Security > Firewall

The *Firewall* screen is used to configure a firewall that can filter out various types of unwanted traffic on the Router's local network.

Firewall

Intrusion Detection Protection To use Intrusion Detection System (IDS) and Denial of Service (DoS) protection, select **Enabled**. Otherwise, keep the default, **Disabled**.

Web Content Filtering To filter web content, keep the default, **Enabled**. Otherwise, select **Disabled**. (This feature must be enabled to use the Website Blocking options on the *Access Restrictions > Internet Access Policy* screen.)

Max Firewall Sessions Enter the maximum number of firewall sessions that will be processed at any given time.

Max QoS Sessions Enter the maximum number of QoS sessions that will be processed at any given time.

SIP ALG The SIP ALG feature assists VoIP phones behind the Router when NAT problems are encountered. This feature also assists QoS (when enabled) with automatic classification of SIP- and RTP-related traffic. To use the SIP ALG feature, keep the default, **Enabled**. Otherwise, select **Disabled**.

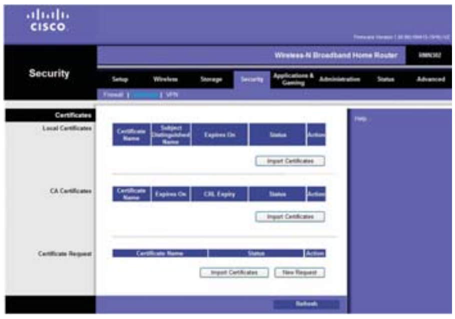
Firewall Profile

Apply Firewall Profile For a low level of firewall protection, keep the default, **Low**. For a high level of firewall protection, select **High**. To disable the firewall, select **Off**.

To configure user-based security rules, click **Access Restrictions**. (Refer to the "Access Restrictions > Internet Access Policy" section for details.)

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Security > Certificates



Local Certificates

Certificate Name	Subject Distinguished Name	Expires On	Status	Action

CA Certificates

Certificate Name	Expires On	CRL Expiry	Status	Action

Certificate Request

Certificate Name	Status	Action

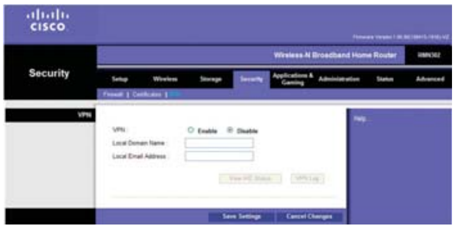
Security > Certificates

Local Certificates: This section shows the certificates associated with the router and allows you to import certificates.

CA Certificates: This section shows the certificates of a certificate authority chain and allows you to import certificates.

Certificate Request: Click here to generate a certificate request, which can be filed to CA.

Security > VPN



VPN : ○ Enable ● Disable
Local Domain Name :
Local Email Address :

Security > VPN

VPN: Choose whether to enable or disable VPN.

Local Domain Name: Type the FQDN (domain name) of the router for IKE phase 1 negotiation.

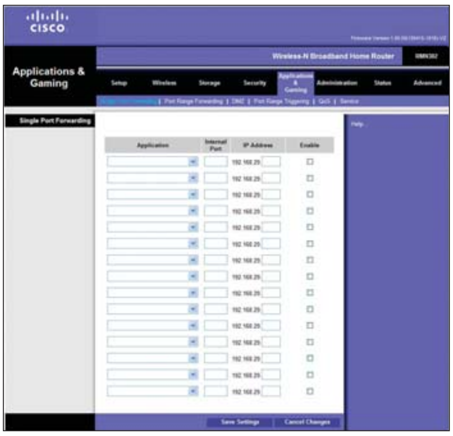
Local Email Address: Type the user-FQDN(email address) of the router for IKE phase 1 negotiation.

View IKE Status: Click to view the IKE negotiation status of the configured endpoints.

VPN Log: Click to view the IKE negotiation log.

IPSec VPN Tunnel: This section shows the IPsec tunnel (endpoint) configuration.

IKE Proposal: This section shows a predefined parameter set for IKE negotiation, which can be associated with a specific IPsec tunnel.



Application	Internal Port	IP Address	Enable
		192.168.29.	☐
		192.168.29.	☐
		192.168.29.	☐
		192.168.29.	☐
		192.168.29.	☐
		192.168.29.	☐
		192.168.29.	☐
		192.168.29.	☐
		192.168.29.	☐
		192.168.29.	☐
		192.168.29.	☐
		192.168.29.	☐
		192.168.29.	☐
		192.168.29.	☐
		192.168.29.	☐

Applications and Gaming > Single Port Forwarding

Applications & Gaming > Single Port Forwarding

The *Single Port Forwarding* screen allows you to customize port services for common applications on this screen.

When users send these types of requests to your network via the Internet, the Router will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers.

Single Port Forwarding

To forward a port, enter the information on each line for the criteria required.

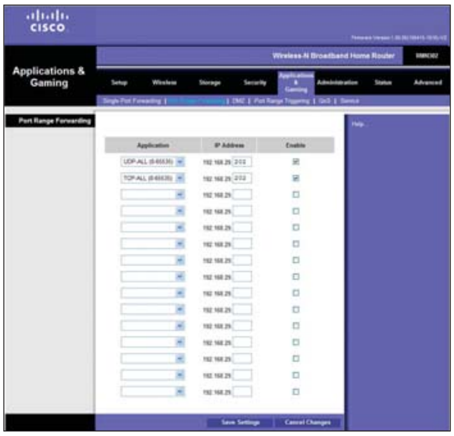
Application Select the appropriate application: **HTTP (80)**, **HTTPS (443)**, **FTP (21)**, **Windows Media Player (1755)**, **DNS (53)**, **POP3 (110)**, **Simple Mail Transfer (25)**, or **TR069 Connection Request (888)**.

Internal Port Enter the internal port number used by the server or Internet application. Check with the Internet application documentation for more information.

IP Address For each application, enter the IP address of the computer that should receive the requests.

Enabled For each application, select **Enabled** to enable port forwarding.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.



Application	IP Address	Enable
UDP-ALL (0-65535)	192.168.29. 202	☑
TCP-ALL (0-65535)	192.168.29. 202	☑
	192.168.29.	☐
	192.168.29.	☐
	192.168.29.	☐
	192.168.29.	☐
	192.168.29.	☐
	192.168.29.	☐
	192.168.29.	☐
	192.168.29.	☐
	192.168.29.	☐
	192.168.29.	☐
	192.168.29.	☐
	192.168.29.	☐
	192.168.29.	☐

Applications and Gaming > Port Range Forwarding

Applications & Gaming > Port Range Forwarding

The *Port Range Forwarding* screen allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. (Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. Some Internet applications may not require any forwarding.)

When users send these types of requests to your network via the Internet, the Router will forward those requests to the appropriate servers (computers). Before using forwarding, you should assign static IP addresses to the designated servers.

If you need to forward all ports to one computer, click the **DMZ** tab.

Port Range Forwarding

To forward a port range, enter the information on each line for the criteria required.

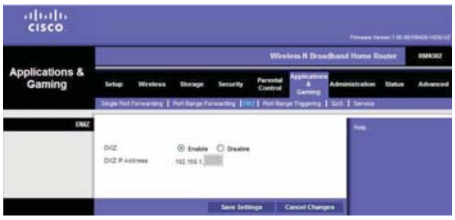
Application Select the appropriate application.

> **Note:** If you do not see the application you want, configure the service on the *Applications & Gaming > Service* screen.

IP Address For each application, enter the IP address of the computer running the specific application.

Enabled Select **Enabled** to enable port forwarding for the applications you have defined.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.



DMZ: ● Enable ○ Disable
DMZ IP Address: 192.168.1.

Applications and Gaming > DMZ

Applications & Gaming > DMZ

The DMZ feature allows one network computer to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Range Forwarding feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer to the Internet.

DMZ

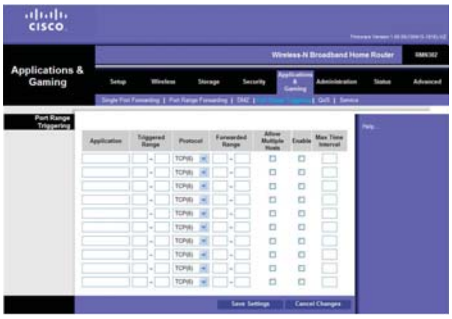
Any computer whose port is being forwarded must have its DHCP client function disabled and should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

DMZ To disable DMZ hosting, keep the default, **Disabled**. To expose one PC, select **Enabled**. Then configure the following setting:

DMZ IP Address Enter the IP address of the computer.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Applications & Gaming > Port Range Triggering



Application	Triggered Range	Protocol	Forwarded Range	Allow Multiple Hosts	Enable	Max Time Interval
	-	TCP(6)	-	□	□	
	-	TCP(6)	-	□	□	
	-	TCP(6)	-	□	□	
	-	TCP(6)	-	□	□	
	-	TCP(6)	-	□	□	
	-	TCP(6)	-	□	□	
	-	TCP(6)	-	□	□	
	-	TCP(6)	-	□	□	
	-	TCP(6)	-	□	□	
	-	TCP(6)	-	□	□	

Applications and Gaming >
Port Range Triggering

The *Port Range Triggering* screen allows the Router to watch outgoing data for specific port numbers. The IP address of the computer that sends the matching data is remembered by the Router, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.

Port Range Triggering

To trigger a port range, enter the information on each line for the criteria required.

Application Name Enter the unique application name of the trigger.

Port Start ~ Port End For each application, enter the starting and ending port numbers of the triggering port number range. These are the ports used by initiating traffic. Check with the Internet application documentation for the port number(s) needed.

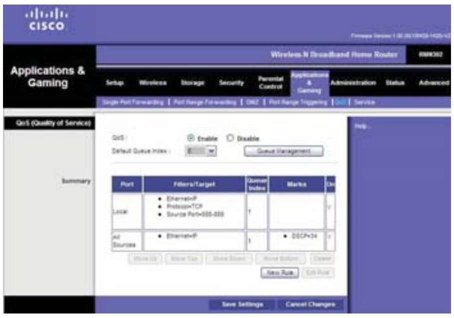
Protocol For each application, select the appropriate protocol, **TCP(6)** or **UDP(17)**.

Forwarded Port Start ~ Forwarded Port End For each application, enter the starting and ending port numbers of the forwarded port number range. These are the ports used by incoming traffic. Check with the Internet application documentation for the port number(s) needed.

Allow Multiple Hosts Select this option to allow multiple hosts in returned traffic.

Enabled Select **Enabled** to enable port triggering for the applications you have defined.

Click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.



QoS: ● Enable ○ Disable
Default Queue Index:

Port	Filters/Target	Queue Index	Marks	On
Local	• Ethernet=IP • Protocol=TCP • Source Port=[illegible]	1		Y
All Sources	• Ethernet=IP	1	• DSCP=34	Y

Applications and Gaming > QoS

Applications & Gaming > QoS

Quality of Service (QoS) ensures better service to high-priority types of network traffic, which may involve demanding, real-time applications, such as videoconferencing.

> **Note:** The Router's QoS is for upstream traffic regulation only. Downstream QoS is usually enforced by the service provider's headend equipment.

QoS (Quality of Service)

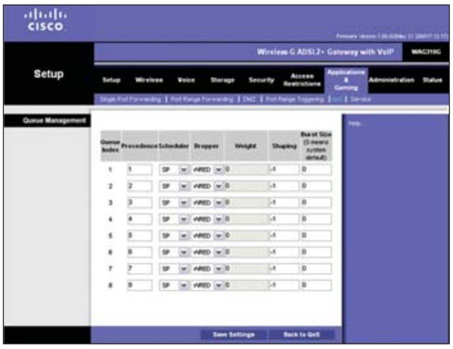
Application-based QoS manages information as it is transmitted and received.

QoS To use QoS, select **Enabled**. Otherwise, keep the default, **Disabled**.

Default Queue Index Select the default queue (and priority) for applications not specified below: **1-8**. (A lower value has higher priority.)

Queue Management A new window appears.

Queue Management



Queue Index	Precedence	Scheduler	Dropper	Weight	Shaping	Burst Size (0 means system default)
1	1	SP	WRED	0	-1	0
2	2	SP	WRED	0	-1	0
3	3	SP	WRED	0	-1	0
4	4	SP	WRED	0	-1	0
5	5	SP	WRED	0	-1	0
6	6	SP	WRED	0	-1	0
7	7	SP	WRED	0	-1	0
8	8	SP	WRED	0	-1	0

Applications and Gaming > QoS > Queue Management

- **Queue Index** There are eight queues for each interface. You can configure the parameters but cannot add or delete queues.

  Higher index queues generally represent higher-priority queues. Queues 1-3 are Strict Priority (WP) queues, and Queues 4-8 are priority-based Weighted Fair Queues (WFQ).

- **Precedence** Enter the Precedence value of this queue relative to the others. A lower value indicates higher precedence.
- Scheduler Select the scheduling algorithm: **SP**, **WFQ**, or **WRR** (Weighted Round Robin). The default is **SP**.
- Dropper Select the dropping algorithm used if there is congestion: **RED** (Random Early Detection), **DT** (Drop Tail), or **WRED** (Weighted RED). The default is **WRED**.
- **Weight** When WFQ or WRR is used, this option is available and used only for queues of equal precedence. Queues 4-6 have equal precedence, and Queues 7-8 have equal precedence. Queues 1-3 have higher precedence than Queues 4-6, while Queues 4-6 have higher precedence than Queues 7-8.
- **Shaping** If the Shaping rate is greater than or equal to 100, then it is the percentage of physical bandwidth. If the Shaping rate is less than 100, then it is the rate in bits per second. A value of -1 indicates no shaping. The default is **-1**.
- Burst Size Enter the Burst Size in bytes (1 to 10485760). For both leaky bucket (constant rate shaping) and token bucket (variable rate shaping) algorithms, the Burst Size value is the bucket size and the maximum burst size. If you set this value to zero, then the Router will use the system default Burst Size, which is the current Shaping rate divided by eight. The default is **0**.

Click **Save Settings** to apply your changes, or click **Back to QoS** to cancel your changes and return to the ***QoS*** screen.

Summary

The QoS rules are displayed with the following information: Port, Filters/Target, Queue Index, Marks and On (status).

To move, edit, or delete a rule, select the entry (its color will change).

Move Up To move a QoS rule up in precedence, click this option.

Move Top To move a QoS rule to highest in precedence, click this option.

Move Down To move a QoS rule down in precedence, click this option.

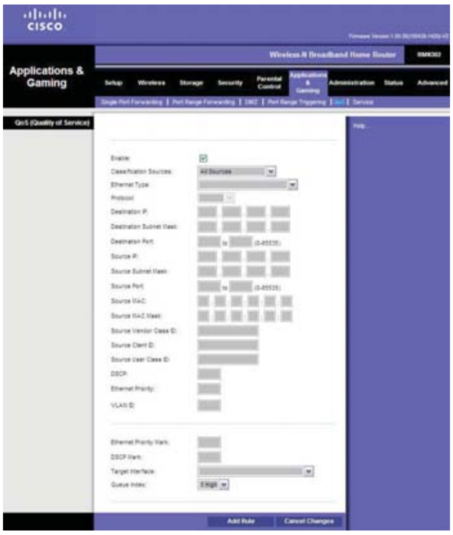
Move Bottom To move a QoS rule lowest in precedence, click this option.

Delete To delete a QoS rule, click this option.

Edit Rule To change a QoS rule, click this option.

New Rule To create a new QoS rule, click this option.

If you click Edit Rule or New Rule, a different screen appears.



Enable: ☑
Classification Sources: All Sources
Ethernet Type:
Protocol:
Destination IP:
Destination Subnet Mask:
Destination Port: to (0-65535)
Source IP:
Source Subnet Mask:
Source Port: to (0-65535)
Source MAC:
Source MAC Mask:
Source Vendor Class ID:
Source Client ID:
Source User Class ID:
DSCP:
Ethernet Priority:
VLAN ID:
Ethernet Priority Mark:
DSCP Mark:
Target Interface:
Queue Index: [illegible] High

QoS > Add New Rule

QoS (Quality of Service)

- **Enable** To enable this QoS rule, select the check box. Otherwise, leave the check box blank.
- Classification Sources Select **All Sources**, **Local Router**, **All LAN Ports** that traffic will come from, or a specific LAN port: Ethernet Ports 1-5 or WLAN SSID networks. The default is **All Sources**.
- Ethernet Type Select **None**, **IP (0x0800)**, **ARP (0x0806)**, **PPPoE Discovery Stage (0x8863)**, **PPPoE Session State (0x8864)**, or **EAPOL (0x888e)**.
- **Protocol** If you selected IP (0x0800) for the Ethernet Type setting, then select the appropriate Protocol: **None**, **ICMP (1)**, **IGMP (2)**, **TCP (6)**, or **UDP (17)**.

Depending on the Protocol you selected, the following settings may be available:

- **Destination IP** Enter the Destination IP address, if applicable as a filter condition.
- Destination Subnet Mask Enter the Destination subnet mask, if applicable as a filter condition.
- Destination Port If you selected TCP or UDP for the Protocol setting, enter the Destination port range, if applicable as a filter condition.
- Source IP Enter the Source IP address of the local computer, if applicable as a filter condition.
- Source Subnet Mask Enter the Source subnet mask, if applicable as a filter condition.
- **Source Port** If you selected TCP or UDP for the Protocol setting, enter the Source port range, if applicable as a filter condition.
- Source MAC Enter the Source MAC address of the local computer, if applicable as a filter condition.
- Source MAC Mask Enter the Source MAC Mask, if applicable as a filter condition. If you leave this setting blank, then this mask will be ignored.
- Source Vendor Class ID If applicable as a filter condition, enter the Source Vendor Class ID in the host's DHCP request.
- Source Client ID If applicable as a filter condition, enter the Source Client ID in the host's DHCP request.
- Source User Class ID If applicable as a filter condition, enter the Source User Class ID in the host's DHCP request.
- DSCP If applicable as a filter condition, enter the DSCP value of the LAN's incoming packet.
- Ethernet Priority If applicable as a filter condition, enter the Ethernet Priority of the LAN's incoming packet.
- **VLAN ID** If applicable as a filter condition, enter the VLAN ID of the LAN's incoming packet.
- Ethernet Priority Mark (optional) To mark outgoing packets with a specific 802.1p value, enter the value in the field provided.
- DSCP Mark (optional) To mark outgoing packets with a specific DSCP value, enter the value in the field provided.
- Target Interface (optional) All WAN connections and PVC/VLAN bridges are listed. Select the appropriate interface. The Router will direct matching packets to this outgoing interface.

- Queue Index Traffic priority applies to LAN-to-WAN traffic only. Higher priority traffic is guaranteed available bandwidth. This is useful for simultaneous activities that put a heavy load on the network (for example, a VoIP phone call during large file downloads). Select the appropriate Queue Index (and priority): **1 High-8** (a lower value means higher priority).

> **Note:** Traffic from the Router's voice lines are automatically assigned highest priority. You can update parameters, such as the Ethernet Priority Mark setting, according to your service provider's request.

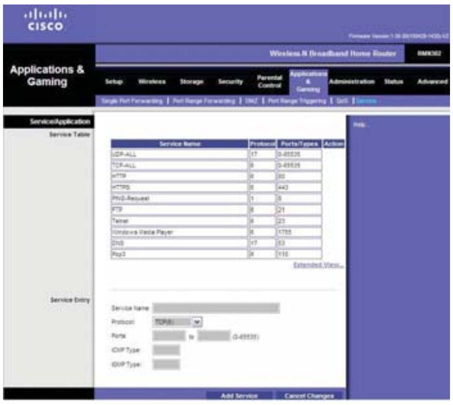
Click **Add Rule** or **Save Rule** to save your changes, or click **Cancel Changes** to cancel your changes and return to the original *QoS* screen.

On the original *QoS* screen, click **Save Settings** to apply your changes, or click **Cancel Changes** to cancel your changes.

Applications & Gaming > Service

The *Service* screen allows you to add services.

Service/Application



Service Name	Protocol	Ports/Types	Action
UDP-ALL	17	0-65535	
TCP-ALL	6	0-65535	
HTTP	6	80	
HTTPS	6	443	
PING-Request	1	8	
FTP	6	21	
Telnet	6	23	
Windows Media Player	6	1755	
DNS	17	53	
Pop3	6	110	

Service Name:
Protocol: TCP(6)
Ports: to (0-65535)
ICMP Type:
IGMP Type:

Applications and Gaming > Service

Service Table

The services are displayed with the following information: Service Name, Protocol, Ports/Types, and Action. To delete a user-defined service, click **Delete**. (Default services cannot be deleted.)

To view additional services, click **Extended View**. To return to the Basic View, click **Basic View**.

Service Entry

Service Name Enter a name for the new service.

Protocol Select the appropriate protocol: **TCP(6)**, **UDP(17)**, **ICMP**, **ESP(50)**, **AH(51)**, **GRE(47)**, **IGMP(2)**, **PIM-DM(103)**, or **IPCOMP(108)**.

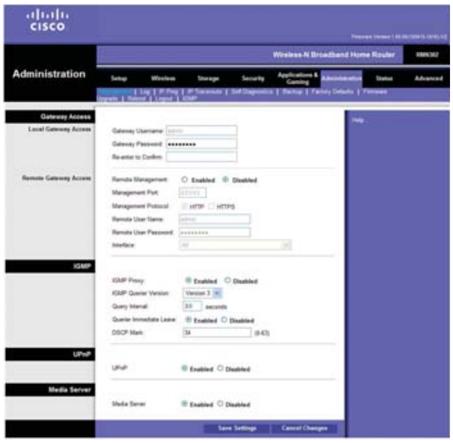
Ports Enter the starting and ending port numbers.

ICMP Type Enter the appropriate number, 1-255, which is valid only for ICMP.

IGMP Type Enter the appropriate number, 1-255, which is valid only for IGMP.
Click **Add Service** to add a new service, or click **Cancel Changes** to cancel your changes.

Administration > Management

The *Administration > Management* screen allows the network's administrator to manage specific Router functions for access and security.



Local Gateway Access
Gateway Username: admin
Gateway Password: •••••••••
Re-enter to Confirm:

Remote Gateway Access
Remote Management: ○ Enabled ● Disabled
Management Port:
Management Protocol: ☐ HTTP ☐ HTTPS
Remote User Name: admin
Remote User Password: ••••••••
Interface:

IGMP Proxy: ● Enabled ○ Disabled
IGMP Querier Version: Version 3
Query Interval: 30 seconds
Querier Immediate Leave: ● Enabled ○ Disabled
DSCP Mark: 34 (0-63)

UPnP: ● Enabled ○ Disabled

Media Server: ● Enabled ○ Disabled

Administration > Management

Gateway Access

Local Gateway Access

To ensure the Router's security, you will be asked for your username and password when you access the Router's web-based utility. The default username and password are **admin**.

Router Username Enter the default Router Username, **admin**.

Router Password Cisco recommends that you change the default Router Password, **admin**, to one of your choice.

Re-enter to Confirm Enter the Router Password again to confirm.

Remote Gateway Access

Remote Management To permit remote access of the Router, from outside the local network, select **Enabled**. Otherwise, keep the default, **Disabled**.

Management Port Enter the port number that will be open to outside access.

Management Protocol Select the appropriate protocol, **HTTP** or **HTTPS**.

> **Note:** When you are in a remote location and wish to manage the Router, enter **https://<Internet_IP_address>:port** or **http://<Internet_IP_address>:port**. Enter the Router's specific Internet IP address in place of <Internet_IP_address>, and enter the Management Port number in place of the word port.

Remote User Name Enter the login user name for remote management.

Remote User Password Enter the login password for remote management.

IGMP

Internet Group Multicast Protocol (IGMP) is used to establish membership in a multicast group and is commonly used for multicast streaming applications. For example, you may have Internet Protocol Television (IPTV) with multiple set-top boxes on the same local network. These set-top boxes have different video streams running simultaneously, so you should use the IGMP feature of the Router.

IGMP Proxy IGMP forwarding (proxying) is a system that improves multicasting for LAN-side clients. If the clients support this option, keep the default, **Enabled**. Otherwise, select **Disabled**.

IGMP Querier Version Select: **Version 1**, **Version 2**, or **Version 3**. The default is **Version 2**.

Query Interval This option is valid when IGMP Proxy is enabled. Enter the number of seconds between queries. The default is **125** seconds.

Querier Immediate Leave Select **Enabled**, if you use IPTV applications and want to allow immediate channel swapping or flipping without lag or delays. Otherwise, keep the default, **Disabled**.

UPnP

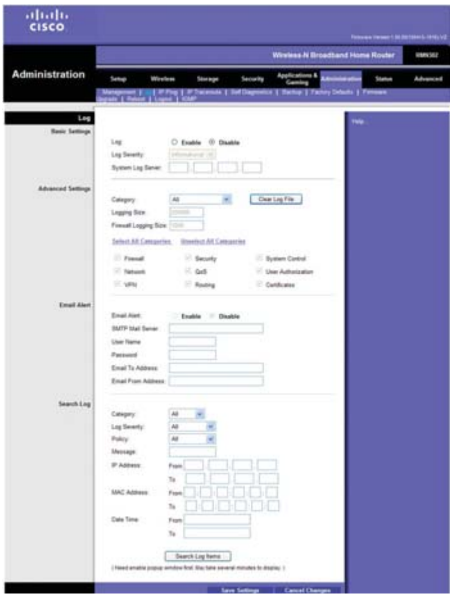
Universal Plug and Play (UPnP) allows Windows XP and Vista to automatically configure the Router for various Internet applications, such as gaming and videoconferencing.

UPnP If you want to use UPnP, keep the default, **Enabled**. Otherwise, select **Disabled**.

> **Note:** IGMPv2 is enabled by default, and v3 is supported. IGMP Snooping is enabled by default for all bridges.

Administration > Log

The Router can keep logs of traffic and events for your Internet connection.



Log: ○ Enable ● Disable

Log Severity:

System Log Server:

Category: All

Logging Size:

Firewall Logging Size:

Firewall, Security, System Control, Network, QoS, User Authorization, VPN, Routing, Certificates

Email Alert: Enable Disable

SMTP Mail Server:

User Name:

Password:

Email To Address:

Email From Address:

Category: All

Log Severity: All

Policy: All

Message:

IP Address: From To

MAC Address: From To

Date Time: From To

(Need enable popup window first. May take several minutes to display.)

Administration > Log

Basic Settings

Log To disable the Log function, select **Disabled**. To monitor traffic between the network and the Internet, keep the default, **Enabled**. With logging enabled, you can choose to view temporary logs.

Log Severity Select the severity level of the log events you want to view: **Informational**, **Warning** (default), or **Critical**.

System Log Server To enable system log server support, enter the IP address of the system log server. To disable system log server support, leave this setting blank.

Advanced Settings

Category: Choose the category of logs that you want to view (firewall, security, system control, network, QoS, user authorization, VPN, routing, or certification).

Logging Size: Type the file size that you want to use for logging files here. The default value is 256 KB.

Firewall Logging size: Type the maximum number of rows to include in a firewall log here. The default value is 1000 rows.

Email Alert

Email Alerts (For Warning Events) To enable E-Mail Alerts for Warning-level events, select **Enabled**. Otherwise, keep the default, **Disabled**.

SMTP Mail Server Enter the address (domain name) or IP address of the Simple Mail Transport Protocol (SMTP) server for outgoing e-mail.

User Name Enter the User Name for SMTP authentication.

Password Enter the Password for SMTP authentication.

Email to Address Enter the e-mail address that will receive alert logs.

Email From Address Enter the return address for the e-mail alerts. (This can be a dummy address.)

Search Log

Category: Choose the category of logs that you want to view (firewall, security, system control, network, QoS, user authorization, VPN, routing, certification).

Log Severity: Choose the severity of messages that you want to include in the logs here..

Policy: TBD.

Message: If you want to see only messages that contain a certain keyword, type that keyword here.

IP Address: Use these fields to restrict the logs so that you only see messages to or from certain IP addresses.

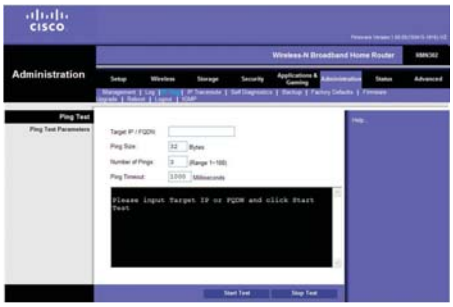
MAC address: Use these fields to restrict the logs so that you only see messages to or from certain MAC addresses.

DateTime: Use the fields to restrict the logs so that you only see messages that happened during a certain date range.

Click **Save Settings** to apply your changes. Click **Clear Event Log** to clear all of the events. Click **Refresh** to update the on-screen information.

Administration > IPPing

The ping test allows you to check the connections of your network devices, including connection to the Internet.


cisco
Administration
Wireless-N Broadband Home Router
Setup
Wireless
Storage
Security
Applications & Gaming
Administration
Status
Advanced
Management | Log | IP Ping | IP Traceroute | Self Diagnostics | Backup | Factory Defaults | Firmware Upgrade | Reboot | Logout | ICMP
Ping Test
Ping Test Parameters
Help...
Start Test
Stop Test

Target IP / FQDN:

Ping Size: 32 Bytes

Number of Pings: 3 (Range 1~100)

Ping Timeout: 1000 Milliseconds

```
Please input Target IP or FQDN and click Start
Test
```

Administration >IPPing

Ping Test

Ping Test Parameters

The ping test checks the status of a connection.

Target IP/FQDN Enter the IP address or Fully Qualified Domain Name (FQDN) that you want to ping. This can be either a local (LAN) or Internet (WAN) IP address.

Ping Size Enter the packet size you want to use. The default is **32** bytes.

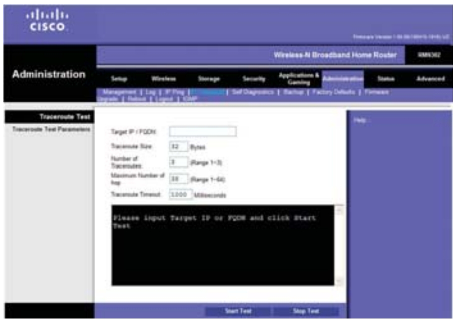
Number of Pings Enter how many times you want to ping. The default is **3**.

Ping Timeout Enter the number of milliseconds before the ping test will time out. The default is **5000** milliseconds.

Ping Result The results of the ping test are displayed.

To run the test, click **Start Test**. Click **Refresh** to update the on-screen information.

Administration > IP Traceroute


cisco
Administration
Wireless-N Broadband Home Router
Setup
Wireless
Storage
Security
Applications & Gaming
Administration
Status
Advanced
Management | Log | IP Ping | IP Traceroute | Self Diagnostics | Backup | Factory Defaults | Firmware Upgrade | Reboot | Logout | ICMP
Traceroute Test
Traceroute Test Parameters
Help...
Start Test
Stop Test

Target IP / FQDN:

Traceroute Size: 32 Bytes

Number of Traceroutes: 3 (Range 1~3)

Maximum Number of hop: 30 (Range 1~64)

Traceroute Timeout: 1000 Milliseconds

```
Please input Target IP or FQDN and click Start
Test
```

Administration > IPTracert

Traceroute test parameters

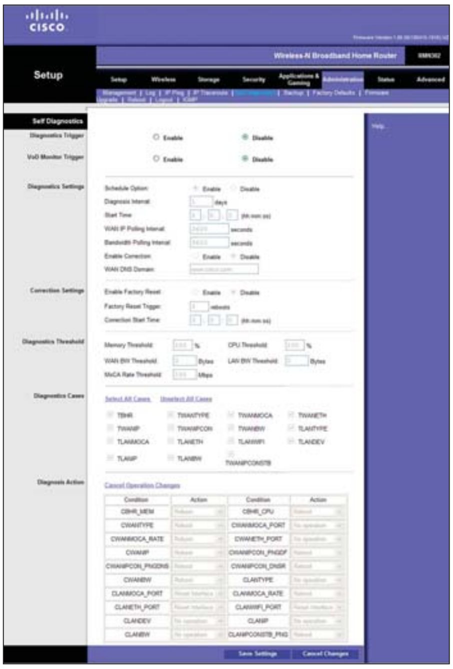
Target IP/FQDN: Type the destination of the traceroute, as an IP address or a domain name.

Traceroute Size: Type the ICMP packet size, in bytes. If the MTU is lower than this value and fragments are not allowed, an ICMP error message appears.

Number of Traceroutes: For each hop, the traceroute application may send multiple packets. Specify the number of traceroutes here.

Max Number of hop: Type the maximum number of hops allowed here. If the number of hops is greater than this value, an ICMP error message appears.

Traceroute Timeout: Type the maximum waiting time between the ICMP request and the ICMP response.



Setup
Setup | Wireless | Storage | Security | Applications & Gaming | Administration | Status | Advanced
Management | Log | IP Ping | IP Traceroute | Self Diagnostics | Backup | Factory Defaults | Firmware Upgrade | Reboot | Logout | IGMP
Wireless-N Broadband Home Router
Help...
Save Settings
Cancel Changes

Self Diagnostics

Diagnostics Trigger: ○ Enable ● Disable

VoD Monitor Trigger: ○ Enable ● Disable

Diagnostics Settings

- Schedule Option: ● Enable ○ Disable
- Diagnosis Interval: 1 days
- Start Time: 0 : 0 : 0 (hh:mm:ss)
- WAN IP Polling Interval: 3600 seconds
- Bandwidth Polling Interval: 3600 seconds
- Enable Correction: ○ Enable ● Disable
- WAN DNS Domain: www.cisco.com

Correction Settings

- Enable Factory Reset: ○ Enable ● Disable
- Factory Reset Trigger: 3 reboots
- Correction Start Time: 0 : 0 : 0 (hh:mm:ss)

Diagnostics Threshold

- Memory Threshold: 100 %
- CPU Threshold: 100 %
- WAN BW Threshold: 0 Bytes
- LAN BW Threshold: 0 Bytes
- MoCA Rate Threshold: 180 Mbps

Diagnostics Cases

Select All Cases Unselect All Cases

☐ TBHR ☐ TWANTYPE ☑ TWANMOCA ☑ TWANETH
☐ TWANIP ☐ TWANIPCON ☐ TWANBW ☑ TLANTYPE
☐ TLANMOCA ☐ TLANETH ☐ TLANWIFI ☑ TLANDEV
☐ TLANIP ☐ TLANBW ☐ TWANIPCONSTB

Diagnosis Action

Cancel Operation Changes

Condition	Action	Condition	Action
CBHR_MEM	Reboot	CBHR_CPU	Reboot
CWANTYPE	Reboot	CWANMOCA_PORT	No operation
CWANMOCA_RATE	Reboot	CWANETH_PORT	No operation
CWANIP	Reboot	CWANIPCON_PINGDF	Reboot
CWANIPCON_PINGDNS	Reboot	CWANIPCON_DNSR	Reboot
CWANBW	Reboot	CLANTYPE	No operation
CLANMOCA_PORT	Reset Interface	CLANMOCA_RATE	Reboot
CLANETH_PORT	Reset Interface	CLANWIFI_PORT	Reset Interface
CLANDEV	No operation	CLANIP	No operation
CLANBW	No operation	CLANIPCONSTB_PING	Reboot

Administration > Self Diagnosis

Administration > Self Diagnostics

Diagnostics Trigger:

Choose whether you want to enable the diagnostics trigger.

VoD Monitor Trigger:

Choose whether you want the MoCA network performance to be recorded in the router persistence log along with a TR-069 parameter for troubleshooting analysis when necessary.

Diagnostics Settings

Schedule option: Choose Enable if you want self-diagnostics to occur periodically, or choose Disable to perform the self-diagnostics immediately, followed by the correction procedure if enabled.

Diagnosis interval: Choose how often the diagnostics tests should occur. The minimum interval is one day.

Start time: Enter the time that the diagnostics tests should start here, in 24-hour format.

WAN IP Polling Interval: Enter the time interval that should pass before the next WAN IP check, in seconds.The default value is 1 hour (3600 seconds).

Bandwidth Polling Interval: Enter the time interval that should pass before the next bandwidth polling test.

Enable Correction: Choose Enable if the router should attempt to recover from any errors that it encounters, or choose Disable if you router should only log the error without attempting to recover.

WAN DNS Domain: Type the domain that is used to test DNS.

Correction Settings

Enable Factory Reset: Choose whether or not to allow self diagnostics to reset the router to the factory default. Choosing Enable will delete the user's configuration.

Factory Reset Trigger: Errors that are detected by self diagnistics may trigger the router to reboot. Specify how many reboots can take place before the router resets itself.

Correction Start Time: Self diagnostics corrections do not take place immediately after the error is detected. Specify when a self diagnostics correct should take place.

Diagnostics Threshold

Memory Threshold: Specify the memory utilization that can be reached before corrective action is taken.

WAN BW Threshold: Specify the bandwidth utilization that can be reached before corrective action is taken.

MoCA Rate Threshold: Specify the MoCA rate utilization that can be reached before corrective action is taken.

Diagnostics Cases

TBHR: This test ensures that there are sufficient internal resources for the router to operate optimally. The CPU and memory utilization snapshot should be taken during the self-diagnostics operation or using a polling interval (BANDWIDTH_POLLING _INTERVAL).

TWANIP: This test ensures that the router has a WAN IP assigned.

TLANMOCA: This test only applies if the MoCA interface is enabled and active. It ensures that the transmission rate for both Tx and Rx should be greater than 180Mbps.

TLANIP: This test ensures that all LAN devices which are currently attached and active have an IP assigned correctly. One method to determine if the LAN device is active or inactive is by sending an ARP request from the router.

TWANTYPE: This test ensures that only one WAN interface is be enabled and active at any time it is in a Connected state. Both WAN interfaces can be enabled, if they are in a Disconnected state.

TWANIPCON: This test ensures that the router has WAN IP connectivity. The IP connectivity is validated via ping tests to both the default gateway (the first hop network router) and the VZ DNS server.

TLANETH: This test ensures that all the Ethernet ports with devices attached are operating optimally, for example, no hardware port failures, excessive framing or CRC errors, and so on. This test only applies if the LAN Ethernet interface is enabled.

TLANBW: This test ensures that at least one of the enabled LAN interfaces can send or receive network traffic based on the delta bytes count. The delta bytes count is the difference between the current value and the last recorded poll value. The default poll interval is every hour.

TWANMOCA: This test ensures that the transmission rate for both Tx and Rx is greater than MoCA threshold level for expected performance. This test only applies if the MoCA interface is enabled.

TWANBW: This test ensures that the WAN interface can send and receive network traffic based on the delta bytes count. The delta bytes count is the difference between the current value and the last recorded polled value. The poll interval is cinfigurable through CMS; the default interval is every hour.

TLANWIFI: This test ensures that the WiFi signal level (RSSI) is acceptable for each WiFi device that is visible in this interface.

TLANIPCONSTB: This test ensures that all set-top boxes that are attached and active on this WAN interface respond successfully to the PING test operation.

TWANETH: This test ensures that the WAN Ethernet port is operating optimally, for exampl, no hardware issue, excessive framing errors, CRC errors, and so on.

TLANTYPE: This test ensures that at least one of the LAN interfaces is enabled and active.

TLANDEV: This test determines how many LAN devices are currently attached and active on the various LAN interfaces (for example, LAN Ethernet, LAN MoCA, and LAN WiFi) of the BHR. The device count determination should be done at the physical medium level and NOT at the IP level. A LAN device must be included in the count if it has been attached and active for more than 30 minutes. (This is due to the BHR implementation of record updates.)

Diagnostics Action

Use this area to specify the action that should take if any of the following conditions occur. For example, for CBHR_MEM, if the memory utilization is less than the memory threshold, then the router will perform the associated action.

The conditions are:

CBHR_MEM: The memory utilization is less than the memory threshold.

CWANTYPE: Only one WAN interface is enabled, or both WAN interfaces are enabled but disconnected.

CWANMOCA_RATE: The transmission rate (Tx and Rx) is greater than the MoCA rate threshold.

CWANIP: The WAN IP address is assigned.

CLANMOCA_PORT: The physical port is operational with no hardware failure.

CLANETH_PORT: All the LAN Ethernet ports which have devices attached are operating optimally, with no failures.

DRAFT - 6/25/2010

CLANDEV: One or more LAN devices are attached and active.

CLANBW: Both the delta number of bytes sent and the number of bytes received are greater than the LAN bandwidth threshold.

CBHR_CPU: The CPU utilization is less than the CPU threshold.

CWANMOCA_PORT: The physical MoCA port is operational with no hardware failure.

CWANETH_PORT: The Ethernet port is operational, with no hardware failure.

CWANIPCON_PNGDF: The default gateway responds to to the ICMP PING.

CWANIPCON_DNSR: The DNS server responds to ICMP PING.

CLANTYPE: One or more of the LAN interface are enabled (LAN MoCA, LAN Ethernet, and LAN WiFi).

CLANMOCA_RATE: Both transmission rates (Tx and Rx) are greater than the MoCA rate threshold.

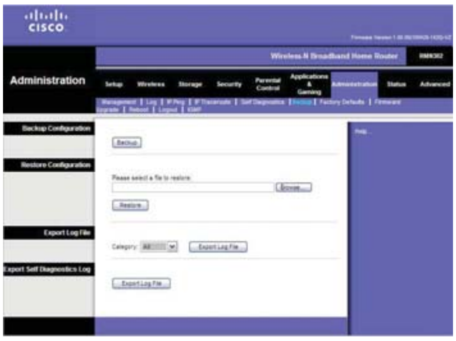
CLANWIFI_PORT: The WiFi interface is operating optimally, with no hardware issues or errors.

CLANIP: All LAN devices have an IP address assigned.

CLANIPCONSTB_PNG: All attached and active set-top boxes respond to the ICMP PING.

Administration > Backup

The *Backup* screen allows you to back up or restore the Router's settings using a configuration file.



Administration > Backup

Backup Configuration

Backup To save the Router's settings in a configuration file, click this button and follow the on-screen instructions.

> **Note:** The voice settings will not be saved in the configuration file.

Restore Configuration

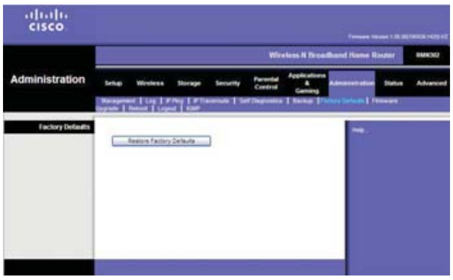
To use this option, you must have previously backed up its configuration settings.

Please select a file to restore Click **Browse** and select the Router's configuration file.

Restore To restore the Router's configuration settings, click this button and follow the on-screen instructions.

Administration > Factory Defaults

The *Factory Defaults* screen allows you to restore the Router's configuration to its factory default settings, except for the voice settings. (An alternative method is to press and hold the Reset button on the Router's back panel for approximately ten seconds.)

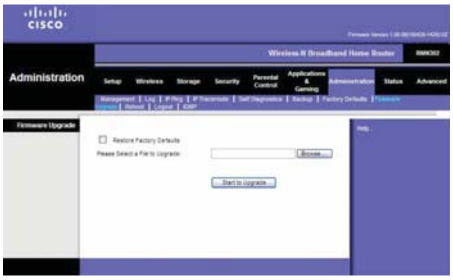

cisco
Wireless-N Broadband Home Router
Administration
Setup
Wireless
Storage
Security
Parental Control
Applications & Gaming
Administration
Status
Advanced
Management | Log | IP Ping | IP Traceroute | Self Diagnostics | Backup | Factory Defaults | Firmware Upgrade | Reboot | Logout | IGMP
Factory Defaults
Restore Factory Defaults
Help...

Administration > Factory Defaults

> **Note:** Restoring factory defaults deletes custom settings except for the voice settings. Note your custom settings before clicking the Restore Factory Defaults button.

Factory Defaults

Restore Factory Defaults To reset settings to the default values, click this button and follow the on-screen instructions. Any custom Router settings you have saved (except for the voice settings) will be lost when the default settings are restored.


cisco
Wireless-N Broadband Home Router
Administration
Setup
Wireless
Storage
Security
Parental Control
Applications & Gaming
Administration
Status
Advanced
Management | Log | IP Ping | IP Traceroute | Self Diagnostics | Backup | Factory Defaults | Firmware Upgrade | Reboot | Logout | IGMP
Firmware Upgrade
□ Restore Factory Defaults
Please Select a File to Upgrade:
Browse...
Start to Upgrade
Help...

Administration > Upgrade

Administration > Upgrade

The *Upgrade* screen allows you to upgrade the Router's firmware. Do not upgrade the firmware unless you are experiencing problems with the Router or the new firmware has a feature you want to use.

Note: The Router may lose the settings you have customized. Before you upgrade its firmware, write down all of your custom settings. After you upgrade its firmware, you will have to re-enter all of your configuration settings.

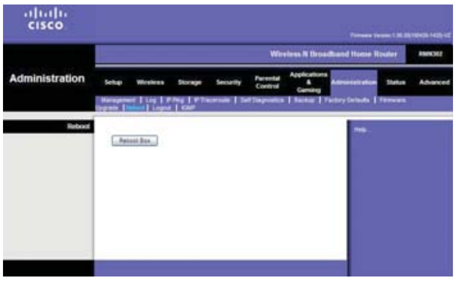
Firmware Upgrade

Before upgrading the firmware, download the Router's firmware upgrade file from the Cisco website, **www.linksysbycisco.com/international**. Then extract the file.

Please Select a File to Upgrade Click Browse and select the extracted firmware upgrade file.

Start to Upgrade After you have selected the appropriate file, click this button, and follow the on-screen instructions.

Note: In rare cases (such as a power failure), the firmware upgrade may fail. If that happens, the Router will enter recovery mode and automatically download firmware from your service provider's provisioning server.



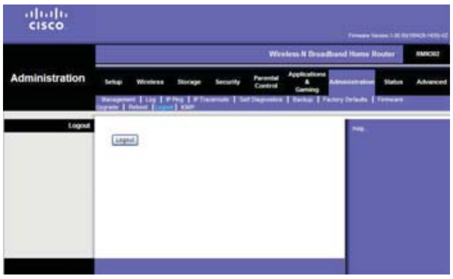
Administration > Reboot

Administration > Reboot

The *Reboot* screen allows you to restart the Router through the web-based utility.

Reboot

Click **Reboot Box** to restart the Router. The restart will terminate the Internet connection.



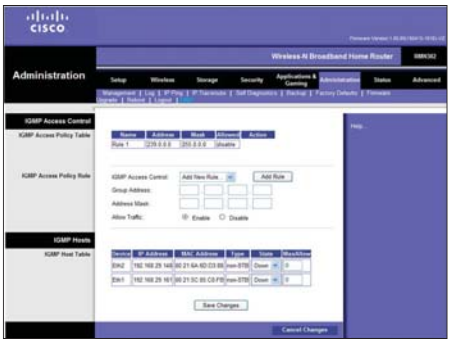
Administration > Logout

Administration > Logout

The *Logout* screen allows you to properly exit the web-based utility.

Logout

Click **Logout** to exit the web-based utility.


Administration
Setup
Wireless
Storage
Security
Applications & Gaming
Administration
Status
Advanced
Wireless-N Broadband Home Router
Management | Log | IP Ping | IP Traceroute | Self Diagnostics | Backup | Factory Defaults | Firmware Upgrade | Reboot | Logout | IGMP
Help...
Add Rule
Save Changes
Cancel Changes

IGMP Access Control

IGMP Access Policy Table

Name	Address	Mask	Allowed	Action
Rule 1	239.0.0.0	255.0.0.0	disable	

IGMP Access Policy Rule

IGMP Access Control: Add New Rule ...

Group Address:

Address Mask:

Allow Traffic: ● Enable ○ Disable

IGMP Hosts

IGMP Host Table

Device	IP Address	MAC Address	Type	State	MaxAllow
Eth2	192.168.25.146	00:21:6A:6D:C3:88	non-STB	Down	0
Eth1	192.168.25.161	00:21:5C:85:C8:FB	non-STB	Down	0

Administration > IGMP

Administration > IGMP

IGMP Access Policy Control

IGMP Access Policy Table:

Needs text.

IGMP Access Policy Rule

IGMP Access control: Choose whether to allow multicast traffic of a specific multicast group.

Group Address: Type the IP address of multicast traffic which is affected the rule.

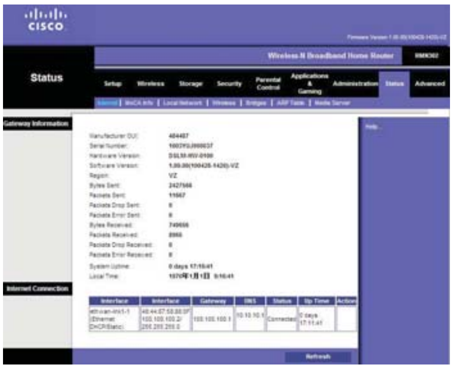
Address Mask: Type the network mask of the IP address specified in the Group Address.

Allow Traffic: Choose whether to allow multicast traffic. This rule defines how the router will respond to a multicast route from outside.

IGMP Hosts

IGMP Host Table

Needs text.


Status
Setup
Wireless
Storage
Security
Parental Control
Applications & Gaming
Administration
Status
Advanced
Wireless-N Broadband Home Router
Internet | MoCA Info | Local Network | Wireless | Bridges | ARP Table | Media Server
Help...
Refresh

Gateway Information

Manufacturer OUI: 404487

Serial Number: 1007YSJ000037

Hardware Version: DSL30-WV-0100

Software Version: 1.00.00(100426-1420)-VZ

Region: VZ

Bytes Sent: 2427566

Packets Sent: 11667

Packets Drop Sent: 0

Packets Error Sent: 0

Bytes Received: 749656

Packets Received: 8966

Packets Drop Received: 0

Packets Error Received: 0

System Uptime: 0 days 17:15:41

Local Time: 1970年1月1日 9:16:41

Internet Connection

Interface	Interface	Gateway	DNS	Status	Up Time	Action
eth-wan-link1-1 (Ethernet DHCP/Static)	40:44:07:58:00:0F 100.100.100.2/ 255.255.255.0	100.100.100.1	10.10.10.1	Connected	0 days 17:11:41	

Status > Internet

Status > Internet

The *Internet* screen displays information about the Router and its current settings.

Router Information

Manufacturer OUI The manufacturer ID number is displayed.

Serial Number The serial number of the Router is displayed.

Hardware Version The version number of the Router's hardware is displayed.

Software Version The version number of the Router's software is displayed.

System Uptime The length of time the Router has been active is displayed.

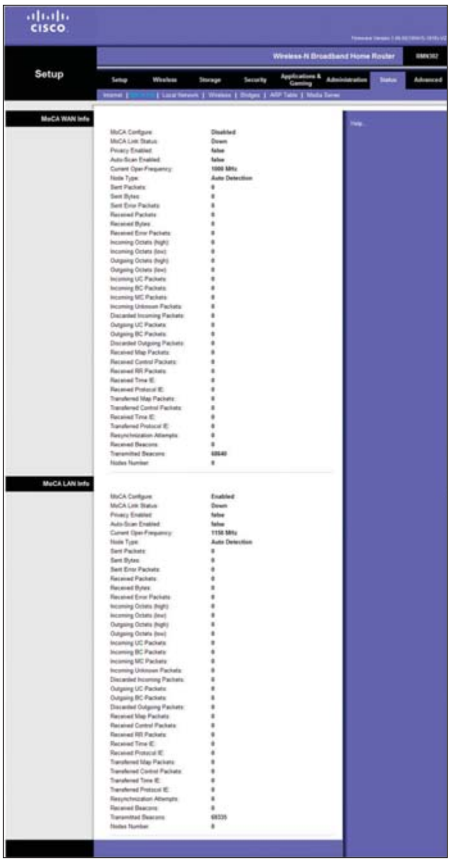
Local Time The date and time of the Router are displayed.

Internet Connection

This section shows the current information for enabled connections. The table lists the following information about each connection: Interface, MAC/IP/Subnet, Router, DNS, and Status.

For DHCP connections, you can manually renew or release them. For PPP-type connections, you can manually connect or disconnect them.

Click **Refresh** to update the on-screen information.


Setup
Wireless-N Broadband Home Router
Setup
Wireless
Storage
Security
Applications & Gaming
Administration
Status
Advanced
Internet | MoCA Info | Local Network | Wireless | Bridges | ARP Table | Media Server
Help...

MoCA WAN Info

MoCA Configure:	Disabled
MoCA Link Status:	Down
Privacy Enabled:	false
Auto-Scan Enabled:	false
Current Oper-Frequency:	1000 MHz
Node Type:	Auto Detection
Sent Packets:	0
Sent Bytes:	0
Sent Error Packets:	0
Received Packets:	0
Received Bytes:	0
Received Error Packets:	0
Incoming Octets (high):	0
Incoming Octets (low):	0
Outgoing Octets (high):	0
Outgoing Octets (low):	0
Incoming UC Packets:	0
Incoming BC Packets:	0
Incoming MC Packets:	0
Incoming Unknown Packets:	0
Discarded Incoming Packets:	0
Outgoing UC Packets:	0
Outgoing BC Packets:	0
Discarded Outgoing Packets:	0
Received Map Packets:	0
Received Control Packets:	0
Received RR Packets:	0
Received Time IE:	0
Received Protocol IE:	0
Transfered Map Packets:	0
Transfered Control Packets:	0
Received Time IE:	0
Transfered Protocol IE:	0
Resynchronization Attempts:	0
Received Beacons:	0
Transmitted Beacons:	68640
Nodes Number:	0

MoCA LAN Info

MoCA Configure:	Enabled
MoCA Link Status:	Down
Privacy Enabled:	false
Auto-Scan Enabled:	false
Current Oper-Frequency:	1150 MHz
Node Type:	Auto Detection
Sent Packets:	0
Sent Bytes:	0
Sent Error Packets:	0
Received Packets:	0
Received Bytes:	0
Received Error Packets:	0
Incoming Octets (high):	0
Incoming Octets (low):	0
Outgoing Octets (high):	0
Outgoing Octets (low):	0
Incoming UC Packets:	0
Incoming BC Packets:	0
Incoming MC Packets:	0
Incoming Unknown Packets:	0
Discarded Incoming Packets:	0
Outgoing UC Packets:	0
Outgoing BC Packets:	0
Discarded Outgoing Packets:	0
Received Map Packets:	0
Received Control Packets:	0
Received RR Packets:	0
Received Time IE:	0
Received Protocol IE:	0
Transfered Map Packets:	0
Transfered Control Packets:	0
Transfered Time IE:	0
Transfered Protocol IE:	0
Resynchronization Attempts:	0
Received Beacons:	0
Transmitted Beacons:	68335
Nodes Number:	0

Status > MoCAInfo

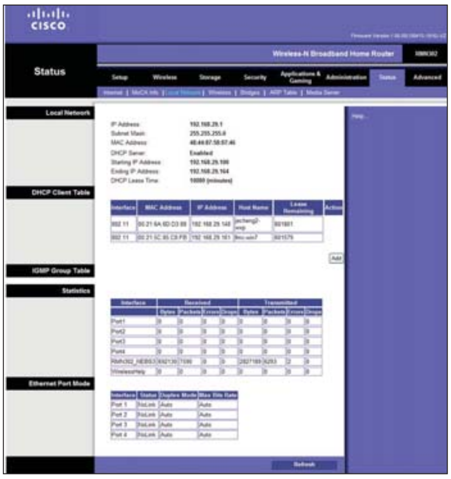
Status > MoCA

MoCA WAN Info

This section p rovides information about the MoCA WAN connection.

MoCA LAN Info

This section provides information about the MoCA LAN connection.


Status
Wireless-N Broadband Home Router
Setup
Wireless
Storage
Security
Applications & Gaming
Administration
Status
Advanced
Internet | MoCA Info | Local Network | Wireless | Bridges | ARP Table | Media Server
Help...
Add
Refresh

Local Network

IP Address:	192.168.29.1
Subnet Mask:	255.255.255.0
MAC Address:	48:44:87:58:87:46
DHCP Server:	Enabled
Starting IP Address:	192.168.29.100
Ending IP Address:	192.168.29.164
DHCP Lease Time:	10080 (minutes)

DHCP Client Table

Interface	MAC Address	IP Address	Host Name	Lease Remaining	Action
802.11	00:21:6A:6D:D3:88	192.168.29.148	jecheng2-wxp	001801	
802.11	00:21:5C:85:C8:FB	192.168.29.161	lmc-win7	001575	

IGMP Group Table

Statistics

Interface	Received				Transmitted			
	Bytes	Packets	Errors	Drops	Bytes	Packets	Errors	Drops
Port1	0	0	0	0	0	0	0	0
Port2	0	0	0	0	0	0	0	0
Port3	0	0	0	0	0	0	0	0
Port4	0	0	0	0	0	0	0	0
RMN302_HEBS3	692130	7190	0	0	2827189	8293	2	0
WirelessHelp	0	0	0	0	0	0	0	0

Ethernet Port Mode

Interface	Status	Duplex Mode	Max Bits Rate
Port 1	NoLink	Auto	Auto
Port 2	NoLink	Auto	Auto
Port 3	NoLink	Auto	Auto
Port 4	NoLink	Auto	Auto

Status > Local Network

Status > Local Network

The *Local Network* screen displays information about the local network.

Local Network

IP Address The Router's IP address, as it appears on your local network, is displayed.

Subnet Mask The Subnet Mask of the Router is displayed.

DHCP Server The status of the Router's DHCP server function is displayed.

Starting IP Address For the range of IP addresses used by devices on your local network, the starting IP address is displayed.

Ending IP Address For the range of IP addresses used by devices on your local network, the ending IP address is displayed.

DHCP Lease Time The length of time for the DHCP lease setting is displayed.

DHCP Client Table

The table displays DHCP, static, and dynamic (found by ARP) types of clients. It describes the devices that have been assigned IP addresses by the Router. For each device, the table lists the following information: Interface, MAC Address, IP Address, Host Name, and Lease Remaining (how much time is left for the current IP address).

IGMP Group Table

The table describes the IGMP configuration of the Router (if configured).

Click **Refresh** to update the on-screen information.

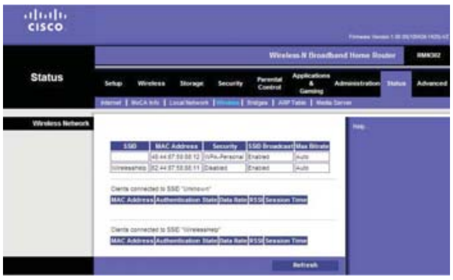
Statistics

This section provides information about transmitted and received data.

Ethernet Port Mode

This section shows the configuration of the LAN interface status, duplex mode and rate.

Status > Wireless



SSID	MAC Address	Security	SSID Broadcast	Max Bitrate
	[illegible]	WPA-Personal	Enabled	Auto
[illegible]	[illegible]	Disabled	Enabled	Auto

Clients connected to SSID "Unknown"

MAC Address	Authentication State	Data Rate	RSSI	Session Time

Clients connected to SSID "[illegible]"

MAC Address	Authentication State	Data Rate	RSSI	Session Time

Status > Wireless

The *Wireless* screen displays information about your wireless network(s).

Wireless Network

For each wireless network, the following is displayed:

SSID The name of the wireless network is displayed.

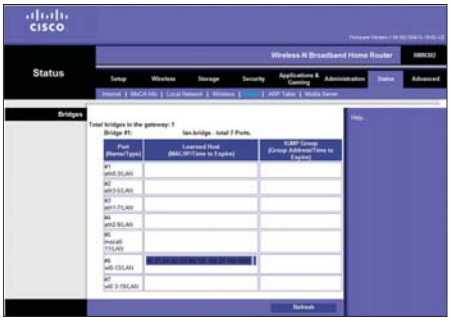
MAC Address The MAC address of the Router's local, wireless interface is displayed.

Security The wireless security method is displayed (if used).

SSID Broadcast The SSID broadcast setting is displayed.

Click **Refresh** to update the on-screen information.

Status > Bridges



Status > Bridge

The *Bridges* screen displays information about the PVC/VLAN and default LAN bridges of the Router

Bridges

The total number of bridges and their descriptions are displayed.

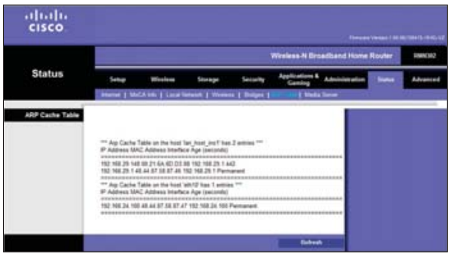
Port (Name/Type) The port name or type is displayed.

Learned Host (MAC/IP/Time to Expire) The MAC address, IP address, or Time to Expire duration is displayed.

IGMP (Group Address/Time to Expire) The IGMP Group Information of this port is displayed.

Click **Refresh** to update the on-screen information.

Status > ARP Table



Status > ARP Table

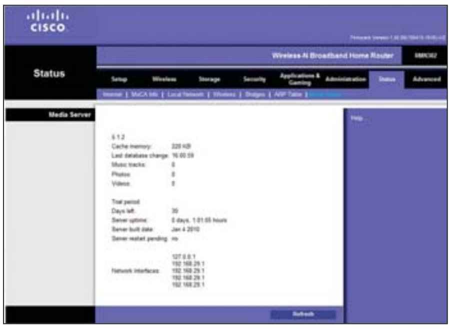
ARP Cache Table

This section displays ARP entries for the listed interface. It includes IP address, corresponding MAC address and length of time active.

Status > Media Server

Media Server

This section provides information about the status of the media server.



Status > MediaServer

Troubleshooting

Your computer cannot connect to the Internet.

Follow the instructions until your computer can connect to the Internet:

- Make sure that the Router is powered on. The Power LED should be green and not flashing.
- If the Power LED is flashing, then power off all of your network devices, including the Router and computers. Then power on each device in the following order:
  1. Router
  2. Computer
- Check the LEDs on the front panel of the Router. Make sure the Power, DSL, and at least one of the numbered LEDs are lit. If they are not, then check the cable connections. The computer should be connected to one of the ports numbered 1-4 on the Router, and the Line port of the Router must be connected to the ADSL line.

When you double-click the web browser, you are prompted for a user name and password. If you want to get rid of the prompt, follow these instructions.

Launch the web browser and perform the following steps (these steps are specific to Internet Explorer but are similar for other browsers):

1. Select **Tools > Internet Options**.
2. Click the **Connections** tab.
3. Select **Never dial a connection**.
4. Click **OK**.

The computer cannot connect wirelessly to the network.

Make sure the wireless network name or SSID is the same on both the computer and the Router. If you have enabled wireless security, then make sure the same security method and key are used by both the computer and the Router.

You need to modify the advanced settings on the Router.

Open the web browser (for example, Internet Explorer or Firefox), and enter the Router's IP address in the address field (the default IP address is **192.168.1.1**). When prompted, complete the User name and Password fields (the default user name and password is **admin**). Click the appropriate tab to change the settings.

Web: Refer to the Cisco website, **www.linksysbycisco.com/international**, if your questions are not addressed here.

Specifications

Model RMN302

Interfaces

COAX	MoCA LAN; MoCA WAN
WAN	Ethernet WAN Interface RJ-45 Port
LAN	Ports (RJ-45); Ethernet 10/100/1000 BASE-T with Auto-Crossover
USB	2 USB 2.0 (host) Ports
Wi-Fi	IEEE 802.11b/g/n 802.1x Authentication External RADIUS Authentication WPA2 and WPA Access WEP, AES & TKIP Encryption WPA/WEP Mixed Mode Wi-Fi Multimedia Support (WMM) Multiple SSIDs MAC Address Filtering Integrated WPS (Push button & PIN entry) Regional Channel Setting
LEDs	Power, Internet ,WAN, WAN MoCA, LAN MoCA, LAN1~4, WLAN, USB1&2, WPS
Buttons	On/Off, Reset, WPS
Mounting	Desktop and Wall Mount

Environmental

Dimensions	220 mm x 42 mm x 175 mm (8.66 in. x 1.65 in. x 6.89 in.)
Weight	400 g (14.11 oz)
Power	110-240 VAC 50/60 Hz Switching Power Supply; 12 VDC, 2 A Output
Certification	FCC Part 68, Part 15, Class B, UL1950, CSA, European EMC & Immunity, CE Mark, Industry-Canada
Operating Temp.	0° to 40°C (32° to 104°F)
Storage Temp.	0° to 70°C (32° to 158°F)
Humidity	20 to 80% Noncondensing

Specifications are subject to change without notice.

Software License Agreement

Software in Cisco Products

This product from Cisco-Cisco LLC or from one of its affiliates Cisco Systems-Cisco (Asia) Pte Ltd. or Cisco-Cisco K.K. ("Cisco") contains software (including firmware) originating from Cisco and its suppliers and may also contain software from the open source community. Any software originating from Cisco and its suppliers is licensed under the Cisco Software License Agreement contained at Schedule 1 below. You may also be prompted to review and accept that Cisco Software License Agreement upon installation of the software

Any software from the open source community is licensed under the specific license terms applicable to that software made available by Cisco at **www.linksysbycisco.com/gpl** or as provided for in Schedules 2, 3 and 4 below.

Where such specific license terms entitle you to the source code of such software, that source code is upon request available at cost from Cisco for at least three years from the purchase date of this product and may also be available for download from **www.linksysbycisco.com/gpl**. For detailed license terms and additional information on open source software in Cisco products please look at the Cisco public web site at: **www.linksysbycisco.com/gpl/** or Schedules 2, 3 or 4 below as applicable.

BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE PRODUCT CONTAINING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THE SOFTWARE LICENSE AGREEMENTS BELOW. IF YOU DO NOT AGREE TO ALL OF THESE TERMS, THEN YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE. YOU MAY RETURN UNUSED SOFTWARE (OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, THE UNUSED PRODUCT) FOR A FULL REFUND UP TO 30 DAYS AFTER ORIGINAL PURCHASE, SUBJECT TO THE RETURN PROCESS AND POLICIES OF THE PARTY FROM WHICH YOU PURCHASED SUCH PRODUCT OR SOFTWARE.

Software Licenses

The software Licenses applicable to software from Cisco are made available at the Cisco public web site at: **www.linksysbycisco.com**. For your convenience of reference, a copy of the Cisco Software License Agreement and the main open source code licenses used by Cisco in its products are contained in the Schedules below.

Schedule 1 - Cisco Software License Agreement

THIS LICENSE AGREEMENT IS BETWEEN YOU AND CISCO-LINKSYS LLC OR ONE OF ITS AFFILIATES CISCO SYSTEMS-LINKSYS (ASIA) PTE LTD. OR CISCO-LINKSYS K.K. ("CISCO") LICENSING THE SOFTWARE INSTEAD OF CISCO-LINKSYS LLC. BY DOWNLOADING OR INSTALLING THE SOFTWARE, OR USING THE PRODUCT CONTAINING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THESE TERMS, THEN YOU MAY NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE. YOU MAY RETURN UNUSED SOFTWARE (OR, IF THE SOFTWARE IS SUPPLIED AS PART OF ANOTHER PRODUCT, THE UNUSED PRODUCT) FOR A FULL REFUND UP TO 30 DAYS AFTER ORIGINAL PURCHASE, SUBJECT TO THE RETURN PROCESS AND POLICIES OF THE PARTY FROM WHICH YOU PURCHASED SUCH PRODUCT OR SOFTWARE.

License. *Subject to the terms and conditions of this Agreement, Cisco grants the original end user purchaser of the Cisco product containing the Software ("You") a nonexclusive license to use the Software solely as embedded in or (where authorized in the applicable documentation) for communication with such product. This license may not be sublicensed, and is not transferable except to a person or entity to which you transfer ownership of the complete Cisco product containing the Software, provided you permanently transfer all rights under this Agreement and do not retain any full or partial copies of the Software, and the recipient agrees to the terms of this Agreement.*

"Software" includes, and this Agreement will apply to (a) the software of Cisco or its suppliers provided in or with the applicable Cisco product, excluding technology from the open source community, and (b) any upgrades, updates, bug fixes or modified versions ("Upgrades") or backup copies of the Software supplied to You by Cisco or an authorized reseller, provided you already hold a valid license to the original software and have paid any applicable fee for the Upgrade.

Protection of Information. The Software and documentation contain trade secrets and/or copyrighted materials of Cisco or its suppliers. You will not copy or modify the Software or decompile, decrypt, reverse engineer or disassemble the Software (except to the extent expressly permitted by law notwithstanding this provision), and You will not disclose or make available such trade secrets or copyrighted material in any form to any third party. Title to and ownership of the Software and documentation and any portion thereof, will remain solely with Cisco or its suppliers.

Collection and Processing of Information. You agree that Cisco and/or its affiliates may, from time to time, collect and process information about your Cisco product and/or the Software and/or your use of either in order (i) to enable Cisco to offer you Upgrades; (ii) to ensure that your Cisco product and/or the Software is being used in accordance with the terms of this Agreement; (iii) to provide improvements to the way Cisco delivers technology to you and to other Cisco customers; (iv) to enable Cisco to comply with the terms of any agreements it has with any third parties regarding your Cisco product and/or Software and/or (v) to enable Cisco to comply with all applicable laws and/or regulations, or the requirements of any regulatory authority or government agency. Cisco and/ or its affiliates may collect and process this information provided that it does not identify you personally. Your use of your Cisco product and/or the Software constitutes this consent by you to Cisco and/or its affiliates' collection and use of such information and, for EEA customers, to the transfer of such information to a location outside the EEA.

Software Upgrades etc. If the Software enables you to receive Upgrades, you may elect at any time to receive these Upgrades either automatically or manually. If you elect to receive Upgrades manually or you otherwise elect not to receive or be notified of any Upgrades, you may expose your Cisco product and/or the Software to serious security threats and/or some features within your Cisco product and/or Software may become inaccessible. There may be circumstances where we apply an Upgrade automatically in order to comply with changes in legislation, legal or regulatory requirements or as a result of requirements to comply with the terms of any agreements Cisco has with any third parties regarding your Cisco product and/or the Software. You will always be notified of any Upgrades being delivered to you. The terms of this license will apply to any such Upgrade unless the Upgrade in question is accompanied by a separate license, in which event the terms of that license will apply.

Open Source Software. The GPL or other open source code incorporated into the Software and the open source license for such source code are available for free download at **http://www.linksysbycisco.com/gpl**. If You would like a copy of the GPL or other open source code in this Software on a CD, Cisco will mail to You a CD with such code for $9.99 plus the cost of shipping, upon request.

Term and Termination. You may terminate this License at any time by destroying all copies of the Software and documentation. Your rights under this License will terminate immediately without notice from Cisco if You fail to comply with any provision of this Agreement.

Limited Warranty. The warranty terms and period specified in the applicable Cisco Product User Guide shall also apply to the Software.

Disclaimer of Liabilities. IN NO EVENT WILL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY LOST DATA, REVENUE OR PROFIT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, REGARDLESS OF CAUSE (INCLUDING NEGLIGENCE), ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF CISCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL CISCO' LIABILITY EXCEED THE AMOUNT PAID BY YOU FOR THE PRODUCT. The foregoing limitations will apply even if any warranty or remedy under this Agreement fails of its essential purpose. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to You.

Export. Software, including technical data, may be subject to U.S. export control laws and regulations and/or export or import regulations in other countries. You agree to comply strictly with all such laws and regulations.

U.S. Government Users. The Software and documentation qualify as "commercial items" as defined at 48 C.F.R. 2.101 and 48 C.F.R. 12.212. All Government users acquire the Software and documentation with only those rights herein that apply to non-governmental customers.

General Terms. This Agreement will be governed by and construed in accordance with the laws of the State of California, without reference to conflict of laws principles. The United Nations Convention on Contracts for the International Sale of Goods will not apply. If any portion of this Agreement is found to be void or unenforceable, the remaining provisions will remain in full force and effect. This Agreement constitutes the entire agreement between the parties with respect to the Software and supersedes any conflicting or additional terms contained in any purchase order or elsewhere.

END OF SCHEDULE 1

Schedule 2

If this Cisco product contains open source software licensed under Version 2 of the "GNU General Public License" then the license terms below in this Schedule 2 will apply to that open source software. The license terms below in this Schedule 2 are from the public web site at **http://www.gnu.org/copyleft/gpl.html**

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright © 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software– to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.
1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.
2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
   a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
   a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.
   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.
   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs

10. whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

END OF SCHEDULE 2

Schedule 3

If this Cisco product contains open source software licensed under Version 2.1 of the "GNU Lesser General Public License" then the license terms below in this Schedule 3 will apply to that open source software. The license terms below in this Schedule 3 are from the public web site at **http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html**.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages—typically libraries—of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".
   A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

   The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

   "Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.
   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
   a) The modified work must itself be a software library.

   b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

   c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

   d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

   (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

   Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

   In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.
   Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

   This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.
   If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

   However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

1. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.
   You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

   a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

   b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

   c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

   d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

   e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:
   a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

   b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.
10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.
11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.
    If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

    It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.
    Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.
14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

END OF SCHEDULE 3

Schedule 4

If this Cisco product contains open source software licensed under the OpenSSL license:

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (**http://www.openssl.org/**).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

In addition, if this Cisco product contains open source software licensed under the OpenSSL license then the license terms below in this Schedule 3 will apply to that open source software. The license terms below in this Schedule 3 are from the public web site at **http://www.openssl.org/source/license.html**.

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (**http://www.openssl.org/**)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (**http://www.openssl.org/**)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

DRAFT - 6/25/2010

Original SSL License

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com)All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:
   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

END OF SCHEDULE 4

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

© 2009 Cisco Systems, Inc.

Part Number 4022934 Rev A