Recommended QoS Configuration Settings for Rosewill RNX-AC750RT Wireless Router

RingCentral®

Contents

Introduction

RingCentral has taken the guesswork out of router selection. Because we know that Quality of Service (QoS) is paramount to your business, we have carefully selected and tested a set of dependable routers suitable for supporting high-quality VoIP conversations.

This document provides recommended configuration settings to ensure the highest possible QoS for voice calls on the Rosewill® RNX-AC750RT wireless router.

Additional routers that have been tested and recommended are shown on the Recommended Routers page of the RingCentral Customer Care website.

Supported Browsers for Test

- Internet Explorer® 11 or higher (Windows® XP, 7, 8 or higher)
- Firefox® version 36 or higher (Windows and Mac®)
- Safari version 6.2 or higher (Mac)

Note:

The routers recommended here are quality hardware that we have tested internally and work reliably with our services. However, given the constantly updated firmware and physical changes made by manufacturers and the nature of cloud-based services, RingCentral cannot control the final configuration of the hardware or your computer systems/networks, or promise that any given router will work with your system, or guarantee that our information is 100% up to date.

Quality of Service

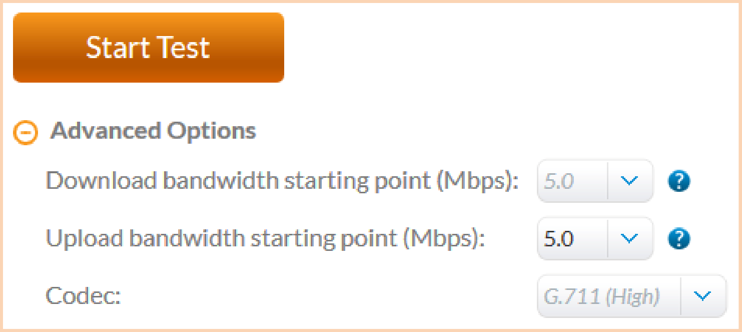
RingCentral provides reliable, high-quality voice service. Your local network, internet connection, and your router all contribute to overall call quality, with sufficient dedicated bandwidth to voice calls being the biggest factor. To help you manage your call quality, RingCentral offers tools to check your internet connection speed, and instructions to configure the Quality of Service (QoS) settings of your routers.

The QoS settings on your router enable it to give priority to real-time voice traffic over lower-priority data traffic, such as large downloads. This document provides recommended configuration settings to ensure the highest-possible QoS experience on the RNX-AC750RT wireless router. Please reference the relevant TCP/UDP settings on the Ports and Firewalls table to complete the recommended setup.

Test Your Connection Capacity

The RingCentral Connection Capacity test will help determine the maximum number of simultaneous RingCentral calls that can be supported on your broadband connection. Run this test during normal business hours when the connection is in use by other applications, including large file downloads.

The capacity test should be run using the maximum number of simultaneous call connections needed, and should use the G.711 codec selection.



Download bandwidth starting point (Mbps): 5.0

Upload bandwidth starting point (Mbps): 5.0

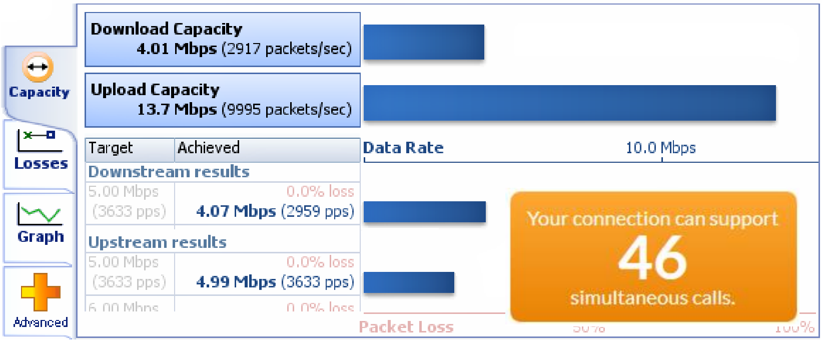
Codec: G.711 (High)

Specific requirements for QoS:

- Bandwidth—100 Kbps up and down per call
- Latency (one-way)—less than 150 ms
- Jitter—not to exceed 100 ms
- Packet loss—less than 3%

These requirements are the foundation for ensuring your local network can support satisfactory VoIP. Failure to meet these requirements will result in poor voice quality.

When the test completes, you will see the recommended number of simultaneous calls your connection can support while maintaining good quality voice calls.



Download Capacity **4.01 Mbps** (2917 packets/sec)

Upload Capacity **13.7 Mbps** (9995 packets/sec)

Target	Achieved
Downstream results	
5.00 Mbps (3633 pps)	0.0% loss **4.07 Mbps** (2959 pps)
Upstream results	
5.00 Mbps (3633 pps)	0.0% loss **4.99 Mbps** (3633 pps)
6.00 Mbps	0.0% loss

Your connection can support 46 simultaneous calls.

Test Your Connection Quality

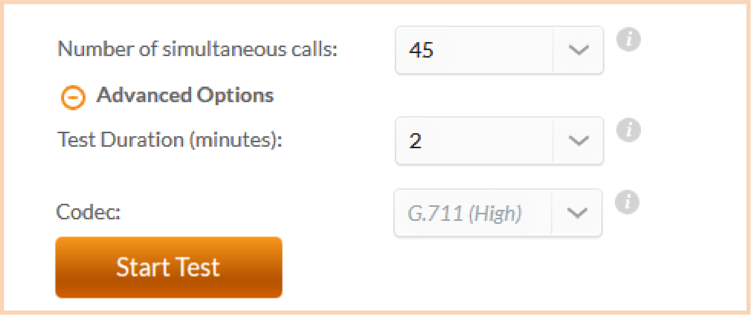
RingCentral provides a VoIP Quality test that will simulate VoIP calls between your computer and RingCentral, and provide an estimate of the voice quality you should expect when using our service. For the most accurate results, run this test *at least* three different times throughout a business day, and *during peak usage times*, while connected to the network that you plan to use for RingCentral.

A two-minute test is typically sufficient, while longer tests are useful to find intermittent problems or to simultaneously test VoIP performance along with other traffic, such as file transfers or remote access.

Select the maximum number of simultaneous users you expect to support, and set the test duration between 1 and 5 minutes; 2 minutes is considered sufficient in most instances.

Click jitter and packet loss on the RESULTS SUMMARY panel to view the overall quality of your expected VoIP connection.

MOS score (Mean Opinion Score) refers to a test that has been used for decades in telephony networks to obtain the human user's view of the quality of the network. The MOS is the arithmetic mean of all the individual scores, and can range from 1 (worst) to 5 (best). A MOS score of 4 is good.

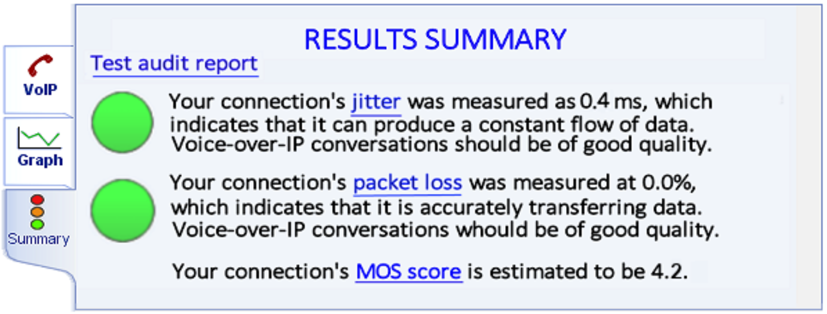


Number of simultaneous calls: 45

⊖ Advanced Options

Test Duration (minutes): 2

Codec: G.711 (High)



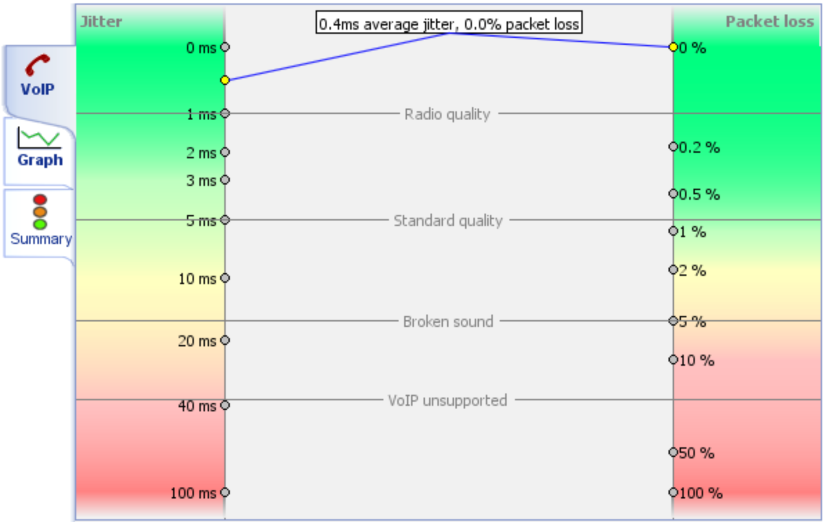
RESULTS SUMMARY

Test audit report

● Your connection's jitter was measured as 0.4 ms, which indicates that it can produce a constant flow of data. Voice-over-IP conversations should be of good quality.

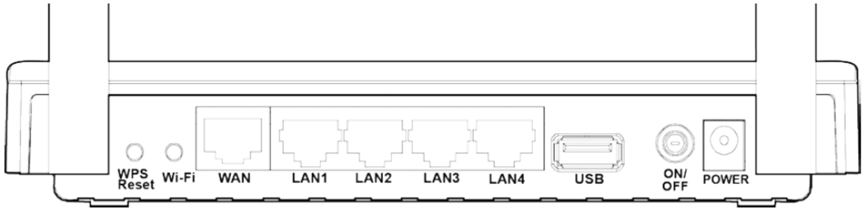
● Your connection's packet loss was measured at 0.0%, which indicates that it is accurately transferring data. Voice-over-IP conversations whould be of good quality.

Your connection's MOS score is estimated to be 4.2.



Configure Your Router

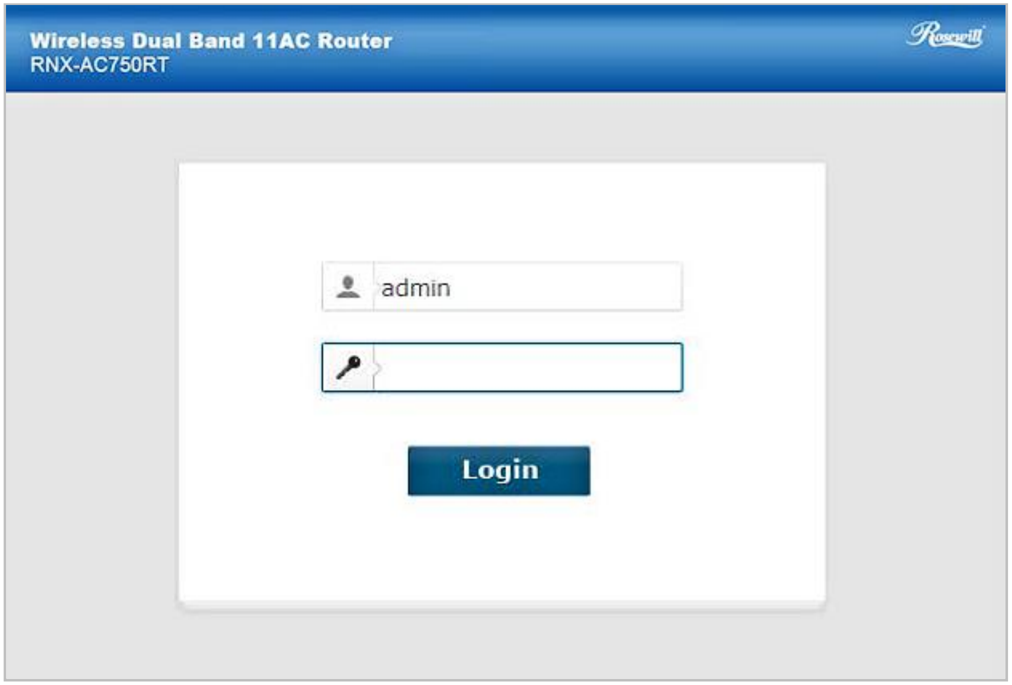
RNX-AC750RT Router QoS Configuration



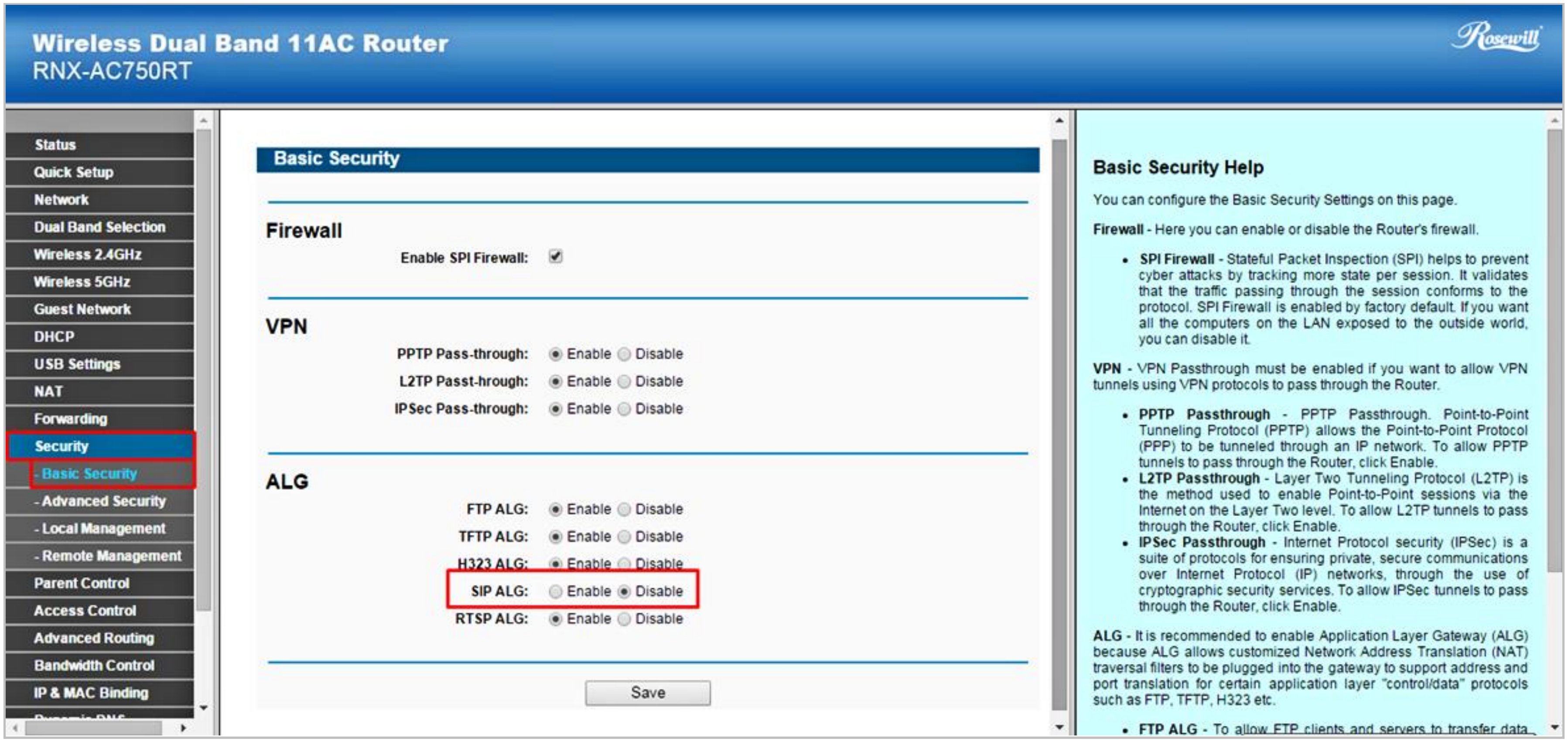
Brand:	Rosewill
Model:	AC750 (RNX-AC750RT)
Hardware version:	RNX-AC750RT v1 00000000
Firmware version:	0.9.10.9 v0032.0 Build 150624 Rel.62513n

To review the User Guide for the Rosewill RNX-AC750RT click here.

1. Browse to the default router IP address (normally 192.168.1.1). User name is **admin** and the default password is **admin**. Click **Login**.



2. Click **Security**; then click **Basic Security**. Under **AGL** find an option for **SIP ALG**. Set **SIP ALG** to **Disable**. Click **Save**.



Basic Security

Firewall

Enable SPI Firewall: ☑

VPN

PPTP Pass-through: ● Enable ○ Disable
L2TP Passt-hrough: ● Enable ○ Disable
IPSec Pass-through: ● Enable ○ Disable

ALG

FTP ALG: ● Enable ○ Disable
TFTP ALG: ● Enable ○ Disable
H323 ALG: ● Enable ○ Disable
SIP ALG: ○ Enable ● Disable
RTSP ALG: ● Enable ○ Disable

Basic Security Help

You can configure the Basic Security Settings on this page.

Firewall - Here you can enable or disable the Router's firewall.

- **SPI Firewall** - Stateful Packet Inspection (SPI) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol. SPI Firewall is enabled by factory default. If you want all the computers on the LAN exposed to the outside world, you can disable it.

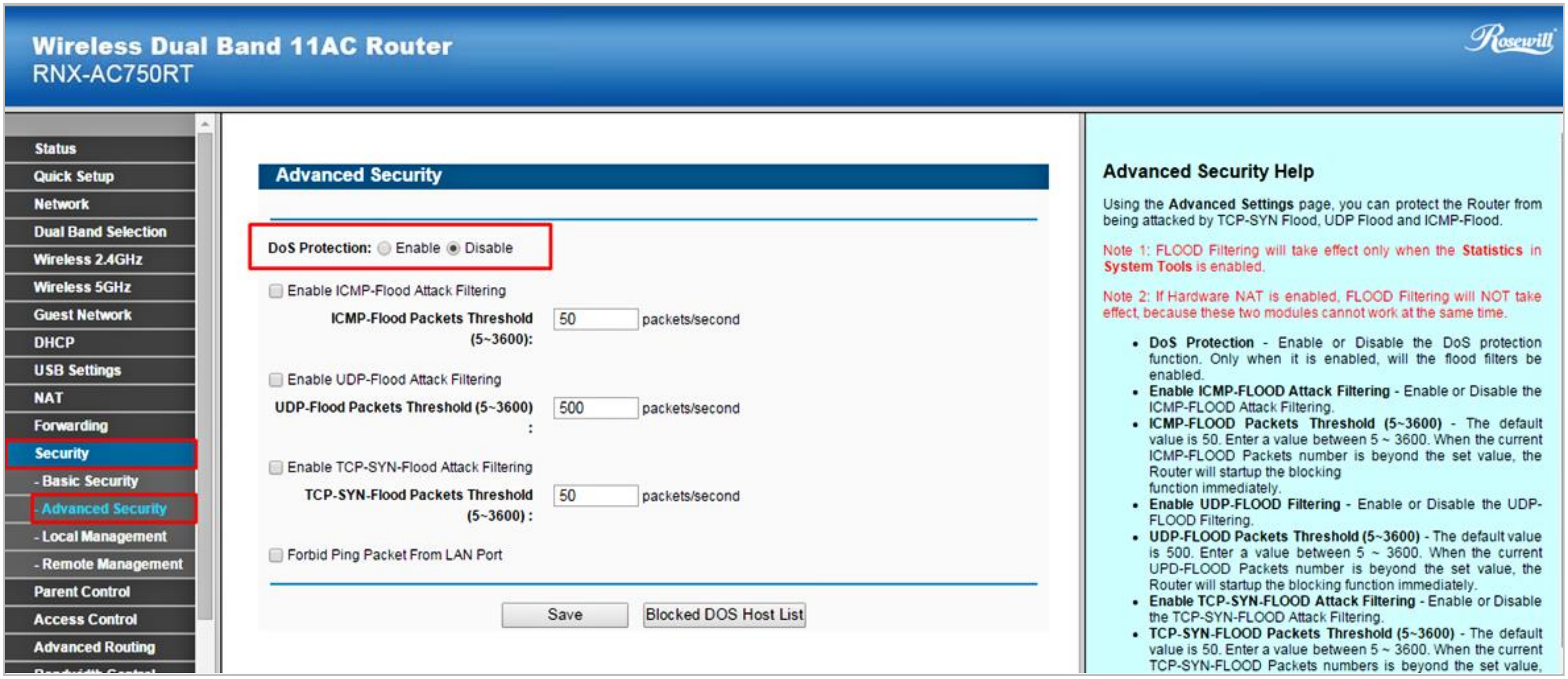
VPN - VPN Passthrough must be enabled if you want to allow VPN tunnels using VPN protocols to pass through the Router.

- **PPTP Passthrough** - PPTP Passthrough. Point-to-Point Tunneling Protocol (PPTP) allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. To allow PPTP tunnels to pass through the Router, click Enable.
- **L2TP Passthrough** - Layer Two Tunneling Protocol (L2TP) is the method used to enable Point-to-Point sessions via the Internet on the Layer Two level. To allow L2TP tunnels to pass through the Router, click Enable.
- **IPSec Passthrough** - Internet Protocol security (IPSec) is a suite of protocols for ensuring private, secure communications over Internet Protocol (IP) networks, through the use of cryptographic security services. To allow IPSec tunnels to pass through the Router, click Enable.

ALG - It is recommended to enable Application Layer Gateway (ALG) because ALG allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, TFTP, H323 etc.

- **FTP ALG** - To allow FTP clients and servers to transfer data

3. Under the same **Security** tab, click **Advanced Security**. On this menu change **DoS Protection** to **Disable**. Click **Save**.



Advanced Security

DoS Protection: ○ Enable ● Disable

□ Enable ICMP-Flood Attack Filtering

ICMP-Flood Packets Threshold (5~3600): 50 packets/second

□ Enable UDP-Flood Attack Filtering

UDP-Flood Packets Threshold (5~3600) : 500 packets/second

□ Enable TCP-SYN-Flood Attack Filtering

TCP-SYN-Flood Packets Threshold (5~3600) : 50 packets/second

□ Forbid Ping Packet From LAN Port

Advanced Security Help

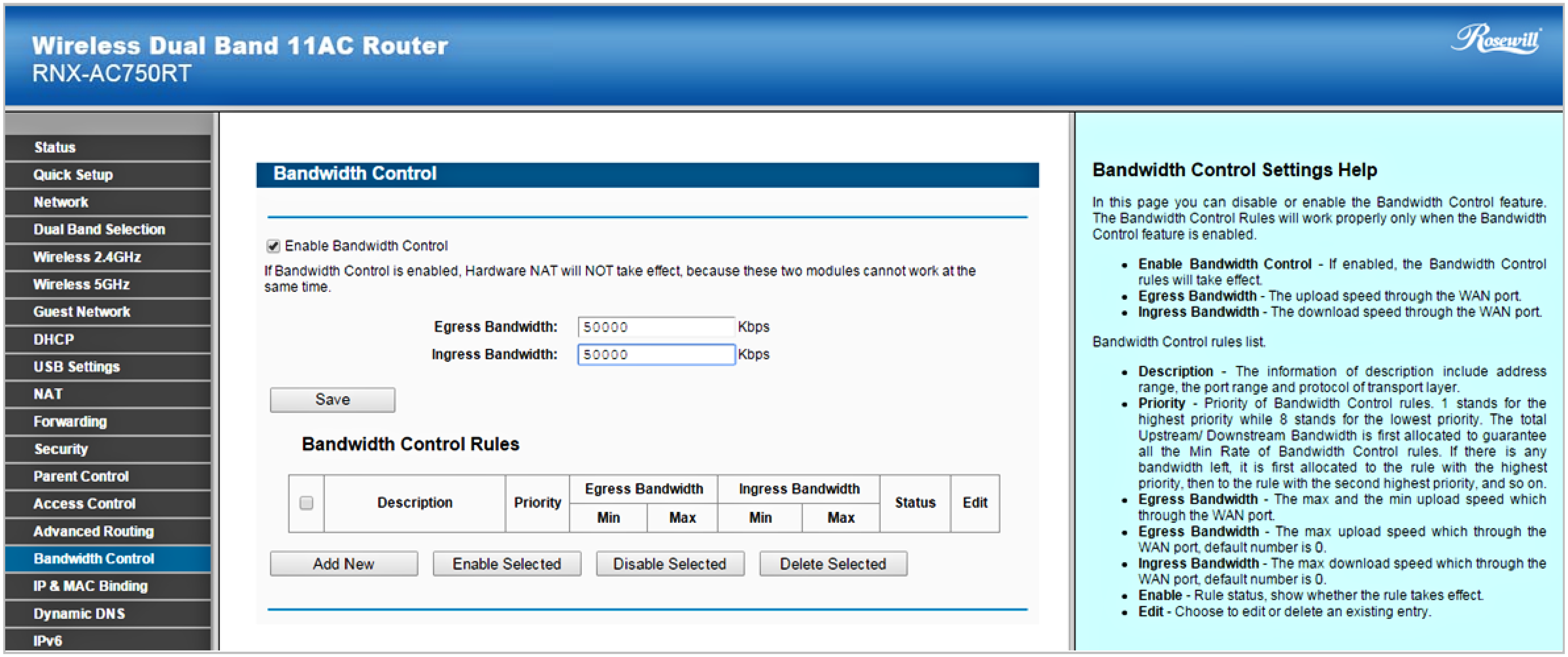
Using the **Advanced Settings** page, you can protect the Router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood.

Note 1: FLOOD Filtering will take effect only when the **Statistics** in **System Tools** is enabled.

Note 2: If Hardware NAT is enabled, FLOOD Filtering will NOT take effect, because these two modules cannot work at the same time.

- **DoS Protection** - Enable or Disable the DoS protection function. Only when it is enabled, will the flood filters be enabled.
- **Enable ICMP-FLOOD Attack Filtering** - Enable or Disable the ICMP-FLOOD Attack Filtering.
- **ICMP-FLOOD Packets Threshold (5~3600)** - The default value is 50. Enter a value between 5 ~ 3600. When the current ICMP-FLOOD Packets number is beyond the set value, the Router will startup the blocking function immediately.
- **Enable UDP-FLOOD Filtering** - Enable or Disable the UDP-FLOOD Filtering.
- **UDP-FLOOD Packets Threshold (5~3600)** - The default value is 500. Enter a value between 5 ~ 3600. When the current UPD-FLOOD Packets number is beyond the set value, the Router will startup the blocking function immediately.
- **Enable TCP-SYN-FLOOD Attack Filtering** - Enable or Disable the TCP-SYN-FLOOD Attack Filtering.
- **TCP-SYN-FLOOD Packets Threshold (5~3600)** - The default value is 50. Enter a value between 5 ~ 3600. When the current TCP-SYN-FLOOD Packets numbers is beyond the set value,

4. Click the **Bandwidth Control** tab. Check **Enable Bandwidth Control** and enter in your network's upload and download speed in Kbps. *This can be obtained using your ISP's speed-test feature, via their website. Example: Search (via Google) "Comcast speed test", or "AT&T speed test"; then click on the link to your ISP's website.*



Bandwidth Control

☑ Enable Bandwidth Control

If Bandwidth Control is enabled, Hardware NAT will NOT take effect, because these two modules cannot work at the same time.

Egress Bandwidth: 50000 Kbps

Ingress Bandwidth: 50000 Kbps

Bandwidth Control Rules

			Egress Bandwidth		Ingress Bandwidth			
☐	Description	Priority	Min	Max	Min	Max	Status	Edit

Bandwidth Control Settings Help

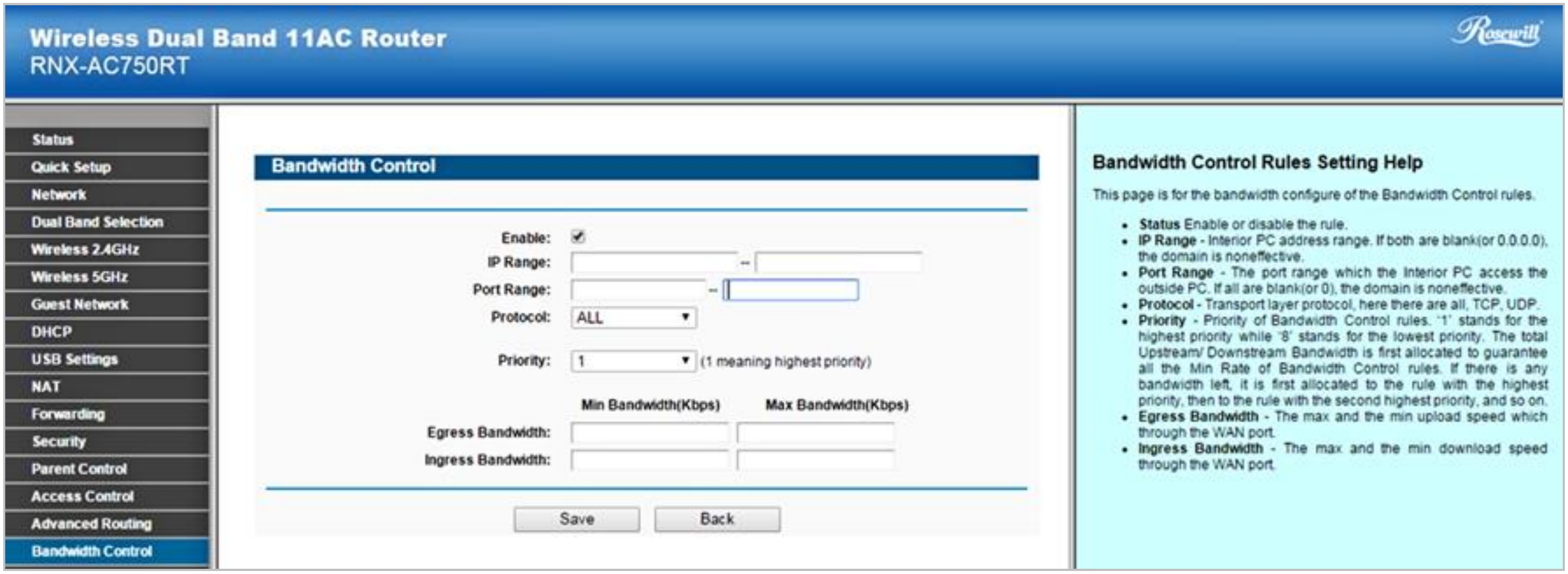
In this page you can disable or enable the Bandwidth Control feature. The Bandwidth Control Rules will work properly only when the Bandwidth Control feature is enabled.

- **Enable Bandwidth Control** - If enabled, the Bandwidth Control rules will take effect.
- **Egress Bandwidth** - The upload speed through the WAN port.
- **Ingress Bandwidth** - The download speed through the WAN port.

Bandwidth Control rules list.

- **Description** - The information of description include address range, the port range and protocol of transport layer.
- **Priority** - Priority of Bandwidth Control rules. 1 stands for the highest priority while 8 stands for the lowest priority. The total Upstream/ Downstream Bandwidth is first allocated to guarantee all the Min Rate of Bandwidth Control rules. If there is any bandwidth left, it is first allocated to the rule with the highest priority, then to the rule with the second highest priority, and so on.
- **Egress Bandwidth** - The max and the min upload speed which through the WAN port.
- **Egress Bandwidth** - The max upload speed which through the WAN port, default number is 0.
- **Ingress Bandwidth** - The max download speed which through the WAN port, default number is 0.
- **Enable** - Rule status, show whether the rule takes effect.
- **Edit** - Choose to edit or delete an existing entry.

5. Under the **Bandwidth Control Rules**, click **Add New**. Set a new rule for each Port Range found on our required port page.
   a. **Port Range**—Port protocol (e.g., 5060 – 6000)
   b. **Protocol**—either UDP, TCP, or ALL
   c. **Priority** —1
   d. **Egress Bandwidth** —The max and the min upload speed through the WAN port
   e. **Ingress Bandwidth** —The max and the min download speed through the WAN port
   f. Click **Save** after all required fields are entered.



Bandwidth Control

Enable: ☑

IP Range: ____ – ____

Port Range: ____ – ____

Protocol: ALL ▾

Priority: 1 ▾ (1 meaning highest priority)

	Min Bandwidth(Kbps)	Max Bandwidth(Kbps)
Egress Bandwidth:		
Ingress Bandwidth:		

Bandwidth Control Rules Setting Help

This page is for the bandwidth configure of the Bandwidth Control rules.

- **Status** Enable or disable the rule.
- **IP Range** - Interior PC address range. If both are blank(or 0.0.0.0), the domain is noneffective.
- **Port Range** - The port range which the Interior PC access the outside PC. If all are blank(or 0), the domain is noneffective.
- **Protocol** - Transport layer protocol, here there are all, TCP, UDP.
- **Priority** - Priority of Bandwidth Control rules. '1' stands for the highest priority while '8' stands for the lowest priority. The total Upstream/ Downstream Bandwidth is first allocated to guarantee all the Min Rate of Bandwidth Control rules. If there is any bandwidth left, it is first allocated to the rule with the highest priority, then to the rule with the second highest priority, and so on.
- **Egress Bandwidth** - The max and the min upload speed which through the WAN port.
- **Ingress Bandwidth** - The max and the min download speed through the WAN port.

Ports and Firewalls Settings for RingCentral VoIP Service

Please see RingCentral Ports and Firewalls reference link for the required TCP/UDP ports that need to be opened for RingCentral devices to work. Categories are:

- Device Type
- Protocol
- Source Port—Customer Side
- Destination Port—RingCentral Side

Also see information on **Port Triggering** on the referenced page.