Routers that customers and partners have recommended:

2talk does not support customer networking equipment and does not endorse or recommend any product listed below. We have simply compiled this list based on feedback from our customers and partners. We recommend each customer research which equipment best fits their own needs.

If you have any feedback on the devices below or have had experience, good or bad, with other routers not listed, we'd like to hear about your experiences at support@2talk.com.

Most popular / best performing (listed alphabetically):

D-Link DIR-655 - Firmware version 1.32 is necessary in order to disable the SIP ALG reliably. **Please Note: The D-Link DIR 655, hardware revision B1, is not suitable for use with VOIP, please see unsuitable list below.**

Linksys BEFSR81 - Older wired model, eight ports, fewer options, but very effective hardware QoS (by MAC address of the PBX or Ethernet port).

Linksys (Cisco) RVS4000 - Firmware version 1.2.1 or better is necessary for suitable VoIP functionality. Firmware upgrades are available at www.cisco.com

Linksys (Cisco) WRVS4400N - Wireless version of the RVS4000 above. Uses different firmware numbering so please use a recent firmware version. Runs hot if mounted vertically.

Linksys (Cisco) WRT310N - Basic QoS settings only, seems to work with small numbers of phones, say 5-6. Runs hot if mounted vertically.

Other routers with a positive mention:

D-Link DIR-625 - hardware revision: A1. Firmware version: 1.09

Linksys (Cisco) WRT300N, WRT320N and WRT400N - Appear to behave in a similar manner to the Linksys WRT310N above. Firmware update may be necessary.

Netgear FVX538 and FVS338 - Firmware update may be necessary. Please Note: configure port forward ranges under Services, but forward the ports under Rules.

Dual WAN routers:

Cisco RV042 - This router allows the use of 2 WAN connections and can be set up either with load balancing or voice can be routed via one connection and all other traffic via another.

Routers and firewalls that have been unsuitable for customers and partners:

Edgewater Networks EdgeMarc 4500T4
Cannot disable the SIP ALG without also disabling SIP QoS, unless you use a second public IP to allow remote phones to connect.

D-Link DIR-655 hardware revision b1
Unable to disable SIP ALG.

Linksys WRT45G (series)
Call quality issues, loss of registration. Can /*sometimes*/ be made to work at a remote location, but usually with slight interruptions of voice traffic

Linksys BEFSR41
Reliability issues.

Microsoft ISA Router/Firewall/Proxy
Will not pass phone traffic, and HUD traffic.

Netgear FVX538
Latest firmware *may* improve matters.

TRENDnet TEW-639GR
Poor VoIP performance, no hardware QoS. Far inferior to the 633.

DSL Modem, Cable Modem by itself
Including but not limited to: 2Wire 2701HG, Netopia 2247 and 3347WG, SMC 8014 (Comcast Business Gateway).
Put the modem/gateway into bridge/passthrough mode and use a third-party VoIP-friendly router.
Your ISP should be able to provide help or instructions for bridge/passthrough mode.

Note: Some ISPs with business-class service may be able to offer you a simple modem-only device (to use with your own third-party router) if you tell them that double-NATing will be a problem.

Larger / Enterprise-class routers - observations only

You **MUST** have someone that is qualified configure these. Unlike SOHO and Small Business routers, these can be difficult or impossible to make work if one is not familiar with them. But when properly configured by a network engineer, they're often great. Suggested for larger installations of 40 users and up. Do your research.

- Cisco router with QoS capability (2600 series, etc.) To be specific, *real* Cisco routers using the Cisco IOS. SIP fixup must be disabled.
- Edgewater Networks EdgeMarc 4200 series
- Fortinet Fortigate 50 (remote telecommuter)
- Fortinet Fortigate 60 (main office)
- Sonicwall. Reported working models include (but may not be limited to) the TZ170 and TZ180. Content filtering and SIP transformations must be turned off for the PBX. Anonymous UDP packets inbound and consistent NAT must be turned on.
  NOTE: WE DO NOT RECOMMEND SONICWALLS FOR USAGE WITH OUR 2TALK CONNECT SERVICE AS THEY ARE KNOWN TO HAVE ISSUES WITH HOSTED VOIP
- Watchguard Firebox. Disable all packet filtering to/from the IP address of the PBX. Do this even before you activate the PBX.

These lists are by no means all-inclusive.

Required / recommended outbound ports

Normally, there is no special configuration required of the firewall that connects your facility to the internet. In some situations, though, modifications may need to be made to open up specific ports on your firewall (allow outbound traffic to certain destination ports).

Destination Port	Protocol	Name	Used for:
8000	TCP	VPN	Required for the PBX to establish VPN tunnels back to the 2talk datacenter and allow you to use the 2talk Portal.
80	TCP	HTTP	Required for PBX software updates and determining the public IP. If activating the server, this must be allowed.
443	TCP	HTTPS	See above.
21	TCP	FTP	See above.
53	TCP/UDP	DNS	Recommended if your PBX is going to be the Primary DNS Server for the network, so it can access public DNS servers.
123	UDP	NTP	Allows the Network Time Protocol service on the PBX.

In most cases, the traffic goes out an arbitrary unprivileged source port; as is normal for IP.