TeleDynamic COMMUNICATIONS | we get it

digium®

Best Practices:
Switchvox on Your Network

TeleDynamic COMMUNICATIONS | we get it

Best Practices: Switchvox on Your Network

These best practices and guidelines help you get started on the right track with Switchvox and a network that is ready for VOIP. Your network doesn't have to be expensive or complex, in fact simplicity is best!

Keep your network simple. You can use basic routers such as Linksys, Netgear, or D-Link home models. If you are considering a more complex network, check your business requirements to be sure you need it. Most issues with VoIP systems can be traced to networks, not to the phones or Switchvox.

Static IP vs. DHCP

We recommend using a static IP address. Because Switchvox is a server, it is important that you assign it an IP address that does not change after it has been configured and users are connecting to it.

If you use Dynamic Host Configuration Protocol (DHCP), we recommend you configure your DHCP server to reserve an IP address just for Switchvox.

You might want to use DHCP to **obtain** your network address information, then set those numbers as your static IP address, subnet mask (netmask), gateway, and DNS server. Be careful, though, because it is **possible** that the DHCP server might give away that IP address, if at some later date, you shut down Switchvox and the DHCP server can't find it. If you decide to do this, you can find all of the addressing information the DHCP server has provided by going to your Switchvox Web Admin **Setup > Networking > IP Configuration**.

Switchvox and Phone Placement

Place Switchvox on the same LAN segment as the phones, and Switchvox, phones, and other networked computers on the same subnet or private network.

Most customers keep Switchvox on a private IP; however, it can be put on a public IP in a DMZ. In either case, place a firewall in front of your Switchvox system, even if it is on a public IP address. A firewall lets you control which IPs have access to your Switchvox services.

You can use an alternate network or VLAN to segment the Switchvox system and phones from the LAN.

Quality of Service (QoS)

If you plan on using a VoIP service provider, it's a good idea to use QoS to prioritize your traffic. QoS lets your voice quality be top notch even if your internet connection is saturated with other traffic. It does that by giving higher priority to the traffic going in and out of Switchvox. Consult your router's documentation for how to set up QoS rules to prioritize VoIP traffic. This can be done by giving priority to your PBX's MAC address or IP address.

If you are using QoS in your network equipment, you can set up Switchvox to send the correct ToS or DSCP field in all VoIP packets. This field can be used by firewalls and switches to distinguish specific types of traffic to apply QoS rules, such as favoring all voice traffic for better quality.

To do this, go to your Switchvox Web Admin website and select **Setup > Networking > IP Configuration**. On IP Configuration page, click Advanced Options, then select the Audio and Video options you want. The default settings should work fine; however, if you know what you are doing you might want to change these.

In most cases, you do not need a QoS switch. Unless you consume massive amounts of bandwidth transferring large files among computers in your local network, you do not need a managed switch. Remember that QoS on the switch is not a replacement for QoS on your router.

Access Control

Switchvox's Access Control tool (**Setup > Networking > Access Control**) lets you set network access to Switchvox services based on IP address and netmask. The default action is to deny access. So if you do not allow a service for a network, then the network is denied access to that service.

If you need to use the Switchboard, be sure to enable access to the XMPP services.

Port Forwarding

If you plan to use phones or to access Switchvox from remote locations, you must forward certain ports back to Switchvox. A good resource for documentation on how to forward ports on most routers is: www.portforward.com.

To enable port forwarding, open

Setup > Networking > IP Configuration

The following table lists the TCP/UDP port assignments and how Switchvox uses them.

TCP/UDP	Port(s)	Switchvox Use
UDP	5060	SIP signaling port needed for phones outside your network
UDP	5062	SIP signaling port needed for phones for configuration communications
UDP	10000-20000	RTP audio ports needed for phones outside your network
SIP UDP	4000-4999	UDPTL ports for T.38 faxing over SIP
IAX UDP	4569	IAX Signalling Port needed for communicating with IAX provider
TCP	80	HTTP port for remote web admin, API, and phone-firmware access
TCP	443	HTTPS port for remote web admin and API access
TCP	5222 & 843	**SMB Systems Only** - ports for using the Switchboard remotely
TCP	5269	**SMB Systems Only** - port for remote XMPP (Jabber/chat) access (Extensible Messaging and Presence Protocol)
UDP	1194	Must be open to outgoing traffic for Digium / Switchvox technical support vpn.