7.3.2 SOHO Configuration Facts

A small office/home office (SOHO) is a small network that is typically based in the home or a small business center.

This lesson covers the following topics:

- SOHO characteristics
- SOHO devices
- SOHO router configuration

SOHO Characteristics

Most SOHO networks have the following characteristics:

- Supports between 1–10 connected hosts (computers, mobile devices, or printers)
- Uses Ethernet or 802.11 wireless networking (or both) as the network medium
- Uses a single internet connection that is shared among all hosts
- Uses a single subnet
- Employs a workgroup networking model (i.e., there are no dedicated servers and a domain is not used)

SOHO Devices

A typical SOHO network uses the following devices:

- A modem or router connects the location to the internet. This connection provides a single IP address for connecting to the internet.
- A router connects the private network to the internet connection. This router is typically a multifunction device, which includes a four port switch, wireless access point, and firewall functionality.
- Additional wired connections can be provided by connecting additional switches to the router.

A SOHO network uses multiple devices that share a single internet connection. The connection to the internet is typically through an access point or router that includes switch ports and/or a wireless access point to connect devices to the local area network and the internet. The type of device you use depends on the internet connection type (DSL, cable, fiber, etc.). The following table describes general steps you would take to configure a SOHO router and set up the network:

SOHO Router Configuration

The following table describes the general steps you would take to configure a SOHO router and set up the network:

Action	Description
Configure the Internet Connection	Begin by connecting the router to the internet connection using the device's WAN port. - For a DSL or ISDN router, connect the device directly to the DSL/ISDN line. - For a cable, fiber optic, or satellite connection, connect the router to the Ethernet port on the modem or connection device. Many routers will automatically detect and configure the internet connection. If not, follow the ISP instructions for setting up the connection. This could include: - Configuring the internet connection with a static IP address assigned by the ISP or configuring the device to use DHCP for addressing - Configuring the protocol used for the connection. This will often be PPPoE for an always-on internet connection - Configuring logon information (username and password) to access the internet - Configuring a default gateway and DNS server addresses that the router will use in order to access the internet
Configure the Router	Before setting up the network, some basic settings on the router need to be configured. Most important is to change the default administrator username and password. Default usernames and passwords are easily guessed or discovered by checking the device documentation. By changing the password, you protect the system from unauthorized access.
Enable NAT	Small networks use a single public IP address to connect to the internet. This IP address is shared by all devices on the private network. Network address translation (NAT) is a protocol that allows multiple computers to share a single public IP address used on the internet. - The internet is classified as a *public* network. All devices on the public network must have a registered IP address. This address is assigned by the ISP. - The SOHO network is classified as a *private* network. All devices on the private network use private IP addresses internally, but share the public IP address when accessing the internet. - A NAT router associates a port number with each private IP address. Communications with the private hosts from the internet are sent to the public IP address and the associated port number. Port assignments are made automatically by the NAT router.

	▪ The private network can use addresses in the following ranges that have been reserved for private use (i.e., they will not be used by hosts on the internet): ▪ 10.0.0.0 to 10.255.255.255 ▪ 172.16.0.0 to 172.31.255.255 ▪ 192.168.0.0 to 192.168.255.255
Secure the SOHO Network	Although the router should now be configured to connect hosts to the private network and provide internet access, the following steps should be taken to properly secure the network from external threats: ▪ Configure the firewall on the device. Enabling the basic firewall on the router provides an additional level of security for the private network. If necessary, configure exceptions on the firewall to allow specific traffic through the firewall. ▪ Configure content filtering and parental controls. Most SOHO routers provide content filtering and parental controls that prevent hosts from accessing specific websites or using a specific internet service, such as chat, torrent, or gaming applications. ▪ Physically secure the router. Anyone with physical access to the router can make configuration changes and gain access to the network. To prevent this, limit physical access to the router. For example, place the router and other networking equipment in a locked closet.
Create a Whitelist and Blacklist	When securing devices or navigation access, there are two options to create lists that either allow or deny access through the Firewall security: ▪ Whitelisting means that only the devices on the list are allowed access. Basically, everyone is blocked access except for the devices on the whitelist. ▪ Blacklisting means all devices are allowed access except for the ones on the blacklist. It's just the opposite of Whitelisting.
Configure for a Network Environment	Depending on the implementation, it may be necessary to take the following steps in order to configure the SOHO router for a particular network environment: ▪ Enable and configure a DMZ (demilitarized zone) host. Configuring a DMZ on a SOHO router causes all incoming port traffic to be forwarded to the specified DMZ host. Because this can open up the network to a variety of external threats, configure a DMZ only if you understand all the implications associated with it. ▪ Configure quality of service (QoS) settings. Most SOHO routers provide basic QoS functionality. When enabled, QoS prioritizes certain network communications over others. For example, VoIP network traffic would be given higher priority and more bandwidth than HTTP (web browser) traffic. ▪ Enable the Universal Plug and Play (UPnP) networking protocol. UPnP is a networking protocol that allows UPnP enabled devices to easily discover each other on the network and share data and media content.

TestOut Corporation All rights reserved.