6.7.3 Router Security Facts

Take the following general actions to secure your routers:

Security Measure	Description
Change Factory Defaults	Change default settings on the router to increase security. ▪ Change the default manufacturer's user name and password and encrypt the new password. Use a complex password instead of passwords that are easy to guess or crack. Complex passwords are typically over eight characters in length, contain a mix of character types (numbers and symbols) and are not words, variations of words, or derivatives of the user name. ▪ Change the default network address. Some routers are defaulted to 192.168.1.1 or 10.0.0.1.

Secure Protocols	Use encrypted protocols when managing the device. The protocols function as follows:
	▪ Secure Shell (SSH) allows for secure interactive control of remote systems.
	  ▪ SSH uses RSA public key cryptography for both connection and authentication.
	  ▪ SSH is a protocol that can also be used to provide security services for other protocols.
	▪ Secure Copy Protocol (SCP) is a secure file copy protocol that uses SSH for security.
	▪ HTTP over SSL (HTTPS) is a secure form of HTTP that uses SSL to encrypt data before it is transmitted.
	
	Do not use HTTP, Telnet, or FTP/TFTP. These protocols send data in cleartext. The most secure way to manage a router's configuration is to connect the management station to the router's console port. This creates a dedication transmission path that can't be sniffed by hosts on the network. Also, avoid using UPnP, which is for universal plug-and-play devices and has been plagued with exploits since it was implemented.

Physical Security	Ensure physical security by keeping network devices in a locked room. If someone can gain access to the physical device, they can easily bypass any configured passwords. Passwords are useless if physical access is not controlled. Implement the following physical security measure: ▪ Perimeter barriers ▪ Closed-circuit television (CCTV) ▪ Doors ▪ Door locks ▪ Physical access logs ▪ Physical access controls
Secure Configuration File	If possible, store the router configuration file in encrypted form and back up the file to a secure location.
Update Firmware	One of the first things you should do when setting up a new router is update the firmware. The updates to the firmware will fix any vulnerabilities that have been resolved by the manufacturer in the past.
Anti-spoofing	Anti-spoofing rules counter spoofing attacks where IP packets have a source address that does not belong to the sender. Anti-spoofing rules analyze the IP packet and match the router interface and direction where the packet is received. Inbound packets that come to the external interface must not have source addresses that match the internal network or the router itself. A typical anti-spoofing rule will be configured as follows: ▪ **Source**: An IP address belonging to the internal network or the IP address of the router itself ▪ **Destination**: Any ▪ **Service**: Any ▪ **Interface**: Any external interface ▪ **Direction**: Inbound ▪ **Action**: Deny ▪ **Time**: Any

Router access control lists can be configured to increase security and limit traffic much like a firewall, but on the router level.