



Cisco Integrated Services Router Security Policy

Cisco 819G-4G-A-K9, 819G-4G-V-K9, 819H-K9, 819G-S-K9, 819HG-4G-G-K9, 891, 881,
1905, 1921 and 1941

Firmware Version: IOS 15.2(4)M5

FIPS 140-2 Non Proprietary Security Policy Level 2 Validation

Version 0.6

April 2014

Table of Contents

1	INTRODUCTION.....	3
1.1	PURPOSE.....	3
1.2	MODULE VALIDATION LEVEL	3
1.3	REFERENCES.....	3
1.4	TERMINOLOGY	3
1.5	DOCUMENT ORGANIZATION	3
2	MODULE DESCRIPTION.....	5
2.1	MODULE INTERFACES.....	8
2.2	ROLES AND SERVICES.....	9
2.3	UNAUTHENTICATED SERVICES	10
2.4	CRYPTOGRAPHIC KEY MANAGEMENT	10
2.5	CRYPTOGRAPHIC ALGORITHMS	13
2.6	NON-FIPS APPROVED ALGORITHMS	13
2.7	SELF-TESTS	14
2.8	PHYSICAL SECURITY	14
2.9	MODULE OPACITY	15
3	SECURE OPERATION	25
3.1	INITIAL SETUP	25
3.2	SYSTEM INITIALIZATION AND CONFIGURATION.....	25
3.3	IPSEC REQUIREMENTS AND CRYPTOGRAPHIC ALGORITHMS	26
3.4	SSLV3.1/TLS REQUIREMENTS AND CRYPTOGRAPHIC ALGORITHMS.....	26
3.5	ACCESS.....	26

1 Introduction

1.1 Purpose

This is the non-proprietary Cryptographic Module Security Policy for the Cisco 819G-4G-A-K9, 819G-4G-V-K9, 819H-K9, 819G-S-K9, 819HG-4G-G-K9, 891, 881, 1905, 1921 and 1941 Integrated Services Router (Firmware Version: IOS 15.2(4)M5). This security policy describes how the modules meet the security requirements of FIPS 140-2 Level 2 and how to run the modules in a FIPS 140-2 mode of operation and may be freely distributed.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at <http://csrc.nist.gov/groups/STM/index.html>.

1.2 Module Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

No.	Area Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	3
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key management	2
8	Electromagnetic Interface/Electromagnetic Compatibility	2
9	Self-Tests	2
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A
	Overall module validation level	2

Table 1 Module Validation Level

1.3 References

This document deals only with the capabilities and operations of the Cisco 819G-4G-A-K9, 819G-4G-V-K9, 819H-K9, 819G-S-K9, 819HG-4G-G-K9, 891, 881, 1905, 1921 and 1941 routers in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the routers from the following sources:

For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at www.cisco.com.

The NIST Validated Modules website (<http://csrc.nist.gov/groups/STM/cmvp/validation.html>) contains contact information for answers to technical or sales-related questions for the module.

1.4 Terminology

In this document, these Cisco Integrated Services Router models identified above are referred to as Integrated Services Router, ISR or the systems.

1.5 Document Organization

The Security Policy document is part of the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

Vendor Evidence document
Finite State Machine

Other supporting documentation as additional references

This document provides an overview of the routers and explains their secure configuration and operation. This introduction section is followed by Section 2, which details the general features and functionality of the router. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

2 Module Description

Cisco Integrated Service Routers (ISRs) are multifunctional networking devices delivering fast, reliable, data transfers with a high standard in security. These routers offer full network security, and other capabilities to fill networking needs for a small to medium size network. The Cisco Integrated Services Router (ISR) provides a scalable, secure, manageable remote access server that meets FIPS 140-2 Level 2 requirements.

The following subsections describe the physical characteristics of the ISRs which contains a multiple-chip standalone cryptographic module. This module is used to support SSH, TLS (VPN,Mgt), IPSec, GetVPN, and SNMPv3.

The Cisco 819G-4G-A-K9, 819G-4G-V-K9, 819H-K9, 819G-S-K9 and 819HG-4G-G-K9 are all Cisco 819. Designed in a compact hardened and non-hardened form factor and differ in support for 3G, 4G, and 3G combined with full features of Cisco IOS Software. The Cisco 819 ISR combines the latest cellular standards (4G LTE), 3G standards (High-Speed Packet Access Plus [HSPA+] release 7 and Evolution Data Optimized [EVDO] Rev A) with Cisco enterprise-class LAN solutions into a single platform.

The cryptographic boundary of the module is defined as the device's case along with opacity shields associated with the system. All of the functionality discussed in this document is provided by components within this cryptographic boundary. The CF card that stored the IOS image is considered an internal memory module, because the IOS image stored in the card may not be modified or upgraded. The card itself must never be removed from the drive. Tamper evident seal will be placed over the card in the drive.

The following configurations are tested:

Hardware Models	Firmware Version
Cisco 819G-4G-A-K9 Integrated Solutions Router	IOS 15.2(4)M5
Cisco 819G-4G-V-K9 Integrated Solutions Router	
Cisco 819H-K9 Integrated Solutions Router	
Cisco 819G-S-K9 Integrated Solutions Router	
Cisco 819HG-4G-G-K9 Integrated Solutions Router	
Cisco 891 Integrated Solutions Router	
Cisco 881 Integrated Solutions Router	
Cisco 1905 Integrated Solutions Router	
Cisco 1921 Integrated Solutions Router	
Cisco 1941 Integrated Solutions Router	

Table 2: ISR Test Configurations

The following pictures are representative each of the modules hardware model:



Figure 1 - Cisco 819G-4G-A-K9 ISR



Figure 2 - Cisco 819G-4G-V-K9 ISR



Figure 3 - Cisco 819H-K9 ISR



Figure 4 - Cisco 819G-S-K9 ISR



Figure 5 - Cisco 819HG-4G-G-K9 ISR



Figure 6 - Cisco 891 ISR



Figure 7 - Cisco 881 ISR



Figure 8 - Cisco 1905 ISR



Figure 9 - Cisco 1921 ISR

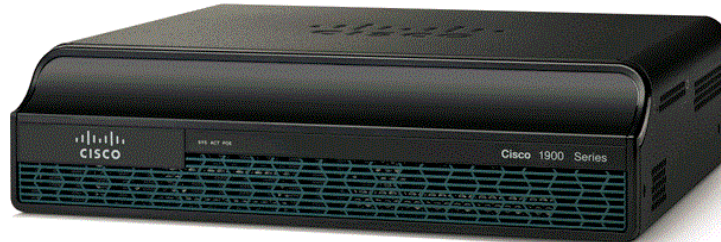


Figure 10 - Cisco 1941 ISR

2.1 Module Interfaces

Each of ISRs is a multiple-chip standalone cryptographic module. The module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to the following FIPS 140-2 defined logical interfaces: data input, data output, control input, status output, and power. The module provided no power to external devices and takes in its power through normal power input/cord. The following table lists all possible logical interface configurations and their associated mapping for all of the various ISR systems detailed in this Security Policy.

Logical Interface	819G-4G-A-K9, 819G-4G-V-K9, 819H-K9, 819G-S-K9, 819HG-4G-G-K9	891	881	1905	1921	1941
Data Input	Fast Ethernet (FE) ports (4), Gigabit Ethernet (GE) port (1), Console/ Aux Port	Fast Ethernet (FE) ports (9), Gigabit Ethernet (GE) port (1), Console Port, Auxiliary Port	Fast Ethernet (FE) ports (5), Console/ Aux Port	EHWIC (1), Gigabit Ethernet (GE) ports (2), Console Port, Auxiliary Port	EHWIC (2), Gigabit Ethernet (GE) ports (2), Console Port, Auxiliary Port	EHWIC (2), Gigabit Ethernet (GE) ports (2), Console Port, Auxiliary Port
Data Output	Fast Ethernet (FE) ports (4), Gigabit Ethernet (GE) port (1), Console/ Aux Port	Fast Ethernet (FE) ports (9), Gigabit Ethernet (GE) port (1), Console Port, Auxiliary Port	Fast Ethernet (FE) ports (5), Console/ Aux Port	EHWIC (1), Gigabit Ethernet (GE) ports (2), Console Port, Auxiliary Port	EHWIC (2), Gigabit Ethernet (GE) ports (2), Console Port, Auxiliary Port	EHWIC (2), Gigabit Ethernet (GE) ports (2), Console Port, Auxiliary Port
Control Input	Fast Ethernet (FE) ports (4), Gigabit Ethernet (GE) port (1), Console/ Aux Port	Fast Ethernet (FE) ports (9), Gigabit Ethernet (GE) port (1), Console Port, Auxiliary Port	Fast Ethernet (FE) ports (5), Console/ Aux Port	EHWIC (1), Gigabit Ethernet (GE) ports (2), Console Port, Auxiliary Port	EHWIC (2), Gigabit Ethernet (GE) ports (2), Console Port, Auxiliary Port	EHWIC (2), Gigabit Ethernet (GE) ports (2), Console Port, Auxiliary Port
Status Output	Console/ Aux Port, Fast Ethernet (FE) ports (4), Gigabit Ethernet (GE) port (1)	Console Port, Auxiliary Port, Fast Ethernet (FE) ports (9), Gigabit Ethernet (GE) port (1)	Console/ Aux Port, Fast Ethernet (FE) ports (5)	Console Port, Auxiliary Port, USB Console Port, Gigabit Ethernet (GE) ports (2)	Console Port, Auxiliary Port, USB Console Port, Gigabit Ethernet (GE) ports (2)	Console Port, Auxiliary Port, USB Console Port, Gigabit Ethernet (GE) ports (2)
Power	5v DC power supply	12v DC power supply, POE power port	12v DC power supply, POE power port	110v ~240v AC power supply, POE power port	110v ~240v AC power supply, POE power port	110v ~240v AC power supply, POE power port

Table 3: ISR Interfaces

2.2 Roles and Services

Authentication is identity-based. Each user is authenticated upon initial access to the module. The module also supports RADIUS or TACACS+ for authentication. There are two roles in the router that operators can assume: the Crypto Officer role and the User role. The administrator of the router assumes the Crypto Officer role and associated services in order to configure the router, while the Users exercise only the basic User services. A complete description of all the management and configuration capabilities of the router can be found in the Performing Basic System Management manual or Configuration Guide Manual and in the online help for the routers.

All CO/User passwords must be 8 characters up to 25 characters with a minimum of one letter and one number. If six (6) integers, one (1) special character and one (1) alphabet are used without repetition for an eight (8) digit PIN, the probability of randomly guessing the correct sequence is one (1) in 251,596,800 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. The calculation should be $10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 32 \times 52 = 251, 596, 800$). Therefore, the associated probability of a successful random attempt is approximately 1 in 251,596,800, which is less than 1 in 1,000,000 required by FIPS 140-2.

When using RSA based authentication, RSA key pair has modulus size of 2048 bit, thus providing 112 bits of strength. Therefore, an attacker would have a 1 in 2^{112} chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2.

2.2.1 User Services

Users enter the system by accessing the console port through a terminal program or via IPSec protected telnet or SSH session to a LAN port. The IOS prompts the User for username and password. If the password is correct, the User is allowed entry to the IOS executive program.

The services available to the User role consist of the following:

Services and Access	Description	Keys and CSPs
Status Functions (r)	View state of interfaces and protocols, version of IOS currently running.	User password
Network Functions (r,w)	Connect to other network devices through outgoing telnet, PPP, etc. and initiate diagnostic network services (i.e., ping, mtrace).	User password
Terminal Functions (r)	Adjust the terminal session (e.g., lock the terminal, adjust flow control).	User password
Directory Services (r)	Display directory of files kept in flash memory.	User password
Self-Tests (r)	Execute the FIPS 140 start-up tests on demand	N/A
SSL VPN (TLSv1.0) (r, w, d)	Negotiation and encrypted data transport via SSL VPN (TLSv1.0)	User password
IPsec VPN (r, w, d)	Negotiation and encrypted data transport via IPsec VPN	User password
GetVPN (GDOI) (r, w, d)	Negotiation and encrypted data transport via GetVPN	User password
SSH Functions(r, w, d)	Negotiation and encrypted data transport via SSH	User password
HTTPS Functions (TLS) (r, w, d)	Negotiation and encrypted data transport via HTTPS	User password
SNMPv3 Functions(r, w, d)	Negotiation and encrypted data transport via SNMPv3	User password

Table 4: User Services (r = read w = write d = delete)

2.2.2 Crypto Officer Services

During initial configuration of the router, the Crypto Officer password (the “enable” password) is defined. A Crypto Officer can assign permission to access the Crypto Officer role to additional accounts, thereby creating additional Crypto Officers. The Crypto Officer role is responsible for the configuration of the router.

The Crypto Officer services consist of the following:

Services and Access	Description	Keys and CSPs
Configure the router (r,w)	Define network interfaces and settings, create command aliases, set the protocols the router will support, enable interfaces and network services, set system date and time, and load authentication information.	ISAKMP pre-shared keys, IKE Authentication key, IKE Encryption Key, IPsec authentication keys, IPsec traffic keys, User passwords, Enable password, Enable secret,

Define Rules and Filters (r,w,d)	Create packet Filters that are applied to User data streams on each interface. Each Filter consists of a set of Rules, which define a set of packets to permit or deny based on characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.	password
View Status Functions (r)	View the router configuration, routing tables, active sessions, use gets to view SNMP MIB statistics, health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.	password
Manage the router (r,w,d)	Log off users, shutdown or reload the router, erase the flash memory, manually back up router configurations, view complete configurations, manager user rights, and restore router configurations.	password
Configure Encryption/Bypass (r,w,d)	Set up the configuration tables for IP tunneling. Set preshared keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address.	ISAKMP pre-shared keys, IKE Authentication key, IKE Encryption Key, IPSec authentication keys, IPSec traffic keys, Enable secret,
SNMPv3 (r)	Non security-related monitoring by the CO using SNMPv3.	password
SSL VPN (using TLSv1.0) (r,w,d)	Configure SSL VPN parameters, provide entry and output of CSPs.	TLS pre-master secret, TLS Traffic Keys
SSH v2 (r, w, d)	Configure SSHv2 parameter, provide entry and output of CSPs.	SSHv2 Traffic Keys
HTTPS (using TLSv1.0) (r,w,d)	Configure HTTPS parameters, provide entry and output of CSPs.	TLS pre-master secret, TLS Traffic Keys
IPsec VPN (r, w, d)	Configure IPsec VPN parameters, provide entry and output of CSPs.	skeyid, skeyid_d, IKE session encryption key, IKE session authentication key, ISAKMP pre-shared, IKE authentication private Key, IKE authentication public key, IPSec encryption key, IPSec authentication key
GetVPN (GDOI) (r, w, d)	Configure GetVPN parameters, provide entry and output of CSPs.	GDOI key encryption key (KEK), GDOI traffic encryption key (TEK), GDOI TEK integrity key
Self-Tests (r)	Execute the FIPS 140 start-up tests on demand	N/A
User services. (r,w,d)	The Crypto Officer has access to all User services.	password
Zeroization (d)	Zeroize cryptographic keys	All CSPs

Table 5: Crypto Officer Services (r = read w = write d = delete)

2.3 Unauthenticated Services

The services available to unauthenticated users are:

- Viewing the status output from the module's LEDs
- Powering the module on and off using the power switch
- Sending packets in bypass

2.4 Cryptographic Key Management

The router securely administers both cryptographic keys and other critical security parameters such as passwords. All keys are protected by the Crypto Officer role login password-protection, and these keys can be zeroized by the Crypto Officer. Zeroization consists of overwriting the memory that stored the key.

The router is in the approved mode of operation only when FIPS 140-2 approved algorithms are used (except DH and RSA key transport which are allowed in the approved mode for key establishment despite being non-approved).

All pre-shared keys are associated with the CO role that created the keys, and the CO role is protected by a password. Therefore, the CO password is associated with all the pre-shared keys. The Crypto Officer needs to be authenticated to store keys. All Diffie-Hellman (DH) keys agreed upon for individual tunnels are directly associated with that specific tunnel only via the Internet Key Exchange (IKE)/Group Domain of Interpretation (GDOI). RSA Public keys are entered into the modules using digital certificates which contain relevant data such as the name of

the public key's owner, which associates the key with the correct entity. All other keys are associated with the user/role that entered them.

The module supports the following keys and critical security parameters (CSPs).

Key/CSP Name	Algorithm	Description	Storage Location	Zeroization Method
DRBG entropy input	SP 800-90 CTR_DRBG (256-bits)	This is the entropy for SP 800-90a RNG.	SDRAM (plaintext)	power cycle the device
DRBG seed	SP 800-90 CTR_DRBG (384-bits)	This is the seed for SP 800-90a RNG.	SDRAM (plaintext)	power cycle the device
DRBG V	SP 800-90 CTR_DRBG (256-bits)	Internal V value used as part of SP 800-90a CTR_DRBG	SDRAM (plaintext)	power cycle the device
DRBG key	SP 800-90 CTR_DRBG (256-bits)	Internal Key value used as part of SP 800-90a CTR_DRBG	SDRAM (plaintext)	power cycle the device
Diffie-Hellman private key	DH (224 – 379 bits)	The private key used in Diffie-Hellman (DH) exchange.	SDRAM (plaintext)	Automatically after shared secret generated.
Diffie-Hellman public key	DH (2048 – 4096 bits)	The p used in Diffie-Hellman (DH) exchange.	SDRAM (plaintext)	Automatically after shared secret generated.
Diffie-Hellman shared secret	DH (2048 – 4096 bits)	The shared key used in Diffie-Hellman (DH) exchange. Created per the Diffie-Hellman protocol.	SDRAM (plaintext)	Zeroized upon deletion.
EC Diffie- Hellman private key	ECDH (P-256/P-384)	The private key used in Elliptic Curve Diffie-Hellman (ECDH) exchange.	SDRAM (plaintext)	Automatically after shared secret generated.
EC Diffie-Hellman public key	ECDH (P-256/P-384)	The p used in Elliptic Curve Diffie-Hellman (ECDH) exchange.	SDRAM (plaintext)	Automatically after shared secret generated.
EC Diffie-Hellman shared secret	ECDH (P-256/P-384)	The shared key used in Elliptic Curve Diffie-Hellman (ECDH) exchange. Created per the Elliptic Curve Diffie-Hellman (ECDH) protocol.	SDRAM (plaintext)	Zeroized upon deletion.
skeyid	HMAC-SHA-1 (160-bits)	Value derived from the shared secret within IKE exchange. Zeroized when IKE session is terminated.	SDRAM (plaintext)	Automatically after IKE session terminated.
skeyid_d	HMAC-SHA-1 (160-bits)	The IKE key derivation key for non ISAKMP security associations.	SDRAM (plaintext)	Automatically after IKE session terminated.
IKE session encryption key	Triple-DES (168-bits/AES (128/196/256-bits)	The IKE session encrypt key.	SDRAM (plaintext)	Automatically after IKE session terminated.
IKE session authentication key	HMAC-SHA-1 (160-bits)	The IKE session authentication key.	SDRAM (plaintext)	Automatically after IKE session terminated.
ISAKMP pre-shared	Shared secret (8 – 25 characters)	The key used to generate IKE skeyid during preshared-key authentication.	NVRAM (plaintext)	“# no crypto isakmp key”
IKE authentication private Key	RSA (2048/3072 bits); ECDSA (P-256/P-384)	RSA private key for IKE authentication.	NVRAM (plaintext)	“# crypto key zeroize rsa”
IKE authentication public key	RSA (2048/3072 bits); ECDSA (P-256/P-384)	RSA public key for IKE authentication.	SDRAM (plaintext)	“# crypto key zeroize rsa”

Key/CSP Name	Algorithm	Description	Storage Location	Zeroization Method
IPSec encryption key	Triple-DES (168-bits/AES (128/196/256-bits))	The IPSec encryption key. Zeroized when IPSec session is terminated.	SDRAM (plaintext)	"# Clear Crypto IPSec SA"
IPSec authentication key	HMAC-SHA-1 (160-bits)	The IPSec authentication key. The zeroization is the same as above.	SDRAM (plaintext)	"# Clear Crypto IPSec SA"
SSH RSA private key	RSA (2048/3072 bits)	The SSH v2 private key for the module.	SDRAM (plaintext)	"# crypto key zeroize rsa"
SSH RSA public key	RSA (2048/3072 bits)	The SSH v2 public key for the module.	SDRAM (plaintext)	"# crypto key zeroize rsa"
SSH session keys	Triple-DES (168-bits/AES (128/196/256-bits))	This is the SSH v2 session key. It is zeroized when the SSH v2 session is terminated.	SDRAM (plaintext)	Automatically when SSH v2 session terminated
TLS server private key	RSA (2048/3072 bits)	Private key used for SSLv3.1/TLS.	NVRAM (plaintext)	"# crypto key zeroize rsa"
TLS server public key	RSA (2048/3072 bits)	Public key used for SSLv3.1/TLS.	NVRAM (plaintext)	"# crypto key zeroize rsa"
TLS pre-master secret	Shared Secret (384-bits)	Shared Secret created using asymmetric cryptography from which new TLS session keys can be created	SDRAM (plaintext)	Automatically when TLS session is terminated
TLS session encryption key	Triple-DES (168-bits/AES (128/196/256-bits))	Key used to encrypt TLS session data	SDRAM (plaintext)	Automatically when TLS session is terminated
TLS session integrity key	HMAC-SHA-1 (160-bits)	HMAC-SHA-1 used for TLS data integrity protection	SDRAM (plaintext)	Automatically when TLS session is terminated
GDOI key encryption key (KEK)	AES (128, 192 and 256 bits)	This key is created using the "GROUPKEY-PULL" registration protocol with GDOI. It is used protect GDOI rekeying data."	SDRAM (plaintext)	Automatically when session terminated.
GDOI traffic encryption key (TEK)	Triple-DES (168-bits/AES (128/196/256-bits))	This key is created using the "GROUPKEY-PULL" registration protocol and updated using the "GROUPKEY-PUSH" registration protocol with GDOI. It is used to encrypt data traffic between Get VPN peers	SDRAM (plaintext)	Automatically when session terminated.
GDOI TEK integrity key	HMAC-SHA-1 (160-bits)	This key is created using the "GROUPKEY-PULL" registration protocol and updated using the "GROUPKEY-PUSH" registration protocol with GDOI. It is used to ensure data traffic integrity between Get VPN peers.	SDRAM (plaintext)	Automatically when session terminated.
snmpEngineID	Shared Secret (32-bits)	A unique string used to identify the SNMP engine.	NVRAM (plaintext)	Overwrite with new engine ID
SNMP v3 password	Shared Secret (8 – 25 characters)	The password use to setup SNMP v3 connection.	NVRAM (plaintext)	Overwrite with new password
SNMP session key	AES (128 bits)	Encryption key used to protect SNMP traffic.	SDRAM (plaintext)	Automatically when session terminated.
User password	Shared Secret (8 – 25 characters)	The password used to authenticate the User role.	NVRAM (plaintext)	Overwrite with new password
Enable secret	Shared Secret (8 – 25 characters)	The password used to authenticate the CO role.	NVRAM (plaintext)	Overwrite with new password
RADIUS secret	Shared Secret (8 – 25 characters)	The RADIUS shared secret. This shared secret is zeroized by executing the "no radius-server key" command.	NVRAM (plaintext)	"# no radius-server key"

Key/CSP Name	Algorithm	Description	Storage Location	Zeroization Method
TACACS+ secret	Shared Secret (8 – 25 characters)	The TACACS+ shared secret. This shared secret is zeroized by executing the “no tacacs-server key” command.	NVRAM (plaintext)	“# no tacacs-server key”

Table 6: CSPs Table

2.5 Cryptographic Algorithms

The router is in the approved mode of operation only when FIPS 140-2 approved/allowed algorithms are used. The module implements a variety of approved and non-approved algorithms.

2.5.1 Approved Cryptographic Algorithms

The routers support the following FIPS 140-2 approved algorithm implementations:

	IOS on Router	Router HW Accelerator	IOS Image Signing
AES	#2620	#962, #1115, #1535 and #1648	N/A
Triple-DES	#1566	#757, #758 and #812	N/A
SHS	#2182	#933, 934 and #1038	#2208
HMAC	#1606	#537, #538 and #627	N/A
RSA	#1338	N/A	#1347
ECDSA	#450	N/A	N/A
CVL	#231	N/A	N/A
DRBG	#401	N/A	N/A

Table 7: Algorithm Certificates

Note:

- RSA (Cert. #1338; non-compliant with the functions from the CAVP Historical RSA List).
 - FIPS186-4:
 - 186-4KEY(gen): PGM(ProvPrimeCondition) (1024 SHA(256))
 - ALG[RSASSA-PKCS1_V1_5] SIG(gen) (1024 SHA(1 , 256)) (2048 SHA(1)) (3072 SHA(1))

The following key establishments despite being non-approved are available:

- Diffie-Hellman (key establishment methodology provides between 112 and 150 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- EC Diffie-Hellman (key establishment methodology provides between 128 and 192 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides between 112 and 128 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
- GDOI (key wrapping; key establishment methodology provides between 112 and 150 bits of encryption strength)

2.6 Non-FIPS Approved Algorithms

Integrated Services Routers (ISRs) cryptographic module implements the following non-Approved algorithms:

- MD5
- DES,
- HMAC-MD5
- RC4

2.7 Self-Tests

In order to prevent any secure data from being released, it is important to test the cryptographic components of a security module to insure all components are functioning correctly. The router includes an array of self-tests that are run during startup and periodically during operations. In the error state, all secure data transmission is halted and the router outputs status information indicating the failure.

2.7.1 Power-On Self-Tests (POSTs)

- IOS Algorithm Self-Tests
 - AES (encrypt/decrypt) Known Answer Tests
 - AES GCM Known Answer Test
 - DRBG Known Answer Test
 - ECDSA Sign/Verify
 - HMAC (SHA-1) Known Answer Test
 - RSA Known Answer Test
 - SHS (SHA-1/256/512) Known Answer Tests
 - Triple-DES (encrypt/decrypt) Known Answer Tests
- Hardware Accelerator Self-Tests
 - AES (encrypt/decrypt) Known Answer Tests
 - Triple-DES (encrypt/decrypt) Known Answer Tests
 - HMAC (SHA-1) Known Answer Test
- Firmware Integrity Test
 - RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-512

2.7.2 Conditional tests

- Conditional Bypass test
- Continuous random number generation test for approved and non-approved RNGs
- Pairwise consistency test for ECDSA
- Pairwise consistency test for RSA

2.8 Physical Security

The router is entirely encased by a metal, opaque case requiring tamper evidence labels and opacity shields (1905/1921). The exact physical make-up differs over models but once the routers have been configured to meet FIPS 140-2 Level 2 requirements, the routers cannot be accessed without signs of tampering. Any attempt to open the router will damage the tamper evidence seals or the material of the module cover.

All Critical Security Parameters are stored and protected within each module's tamper evident enclosure. The Crypto Officer is responsible for properly placing all tamper evident labels. The security labels recommended for FIPS 140-2 compliance are provided in the FIPS Kit (CISCO-FIPS-KIT=), Revision -B0. The FIPS kit includes 15 of the seals, as well as a document detailing the number of seals required per platform and placement information. Please be aware that the extra tamper evident labels/seals shall be securely stored by the Crypto Officer. These security labels are very fragile and cannot be removed without clear signs of damage to the labels.

For models that leverage an opacity shield (1905/1921), the shield must be installed on the right side of the router with the vent downward facing. Tamper Evident Labels must then be placed over the opacity shield. This is illustrated in table 12 below.

Tamper evidence seals can be inspected for signs of tampering, which include the following: curled corners, bubbling, crinkling, rips, tears, and slices. The word "OPEN" will appear if the label was peeled back.

Model	# Tamper labels	Tamper Evident Labels	Opacity Shields
819G-4G-A-K9	8	FIPS Kit (CISCO-FIPS-KIT=), Revision -B0	N/A
819G-4G-V-K9	8	FIPS Kit (CISCO-FIPS-KIT=), Revision -B0	N/A
819H-K9	4	FIPS Kit (CISCO-FIPS-KIT=), Revision -B0	N/A
819G-S-K9	8	FIPS Kit (CISCO-FIPS-KIT=), Revision -B0	N/A
819HG-4G-G-K9	8	FIPS Kit (CISCO-FIPS-KIT=), Revision -B0	N/A
891	6	FIPS Kit (CISCO-FIPS-KIT=), Revision -B0	N/A
881	5	FIPS Kit (CISCO-FIPS-KIT=), Revision -B0	N/A
1905	10	FIPS Kit (CISCO-FIPS-KIT=), Revision -B0	FIPS-SHIELD-1900=
1921	10	FIPS Kit (CISCO-FIPS-KIT=), Revision -B0	FIPS-SHIELD-1900=
1941	8	FIPS Kit (CISCO-FIPS-KIT=), Revision -B0	N/A

Table 8: Tamper Evident Labels

2.9 Module Tamper Evidence

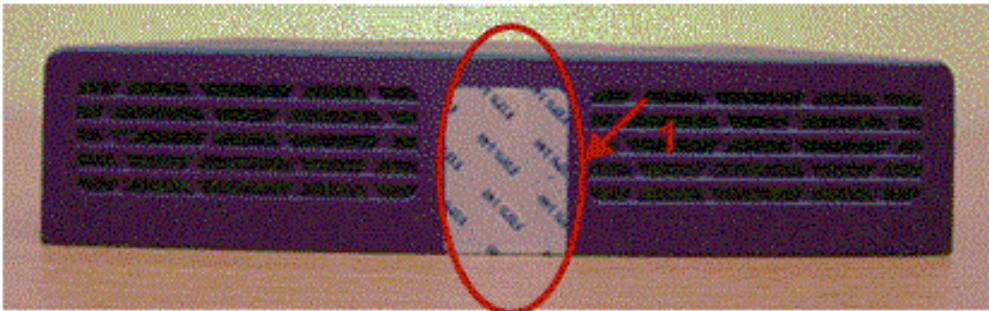
To install the Tamper Evident Labels, please follow these steps

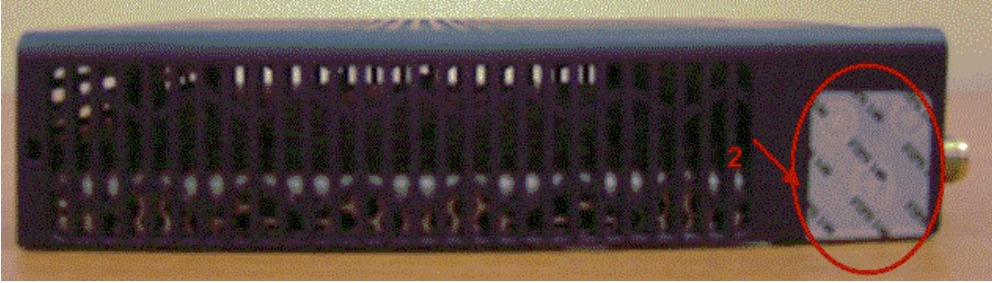
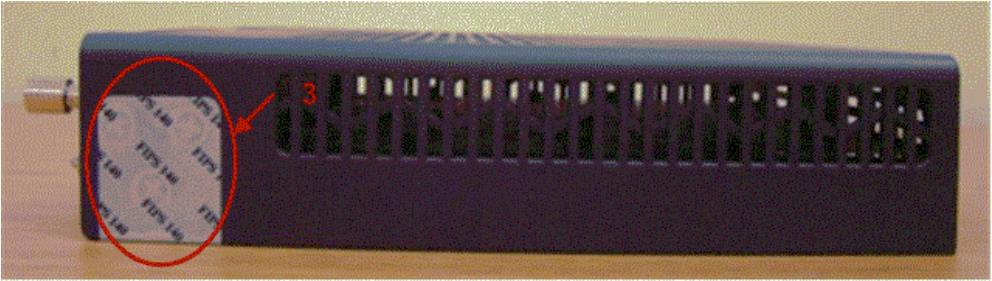
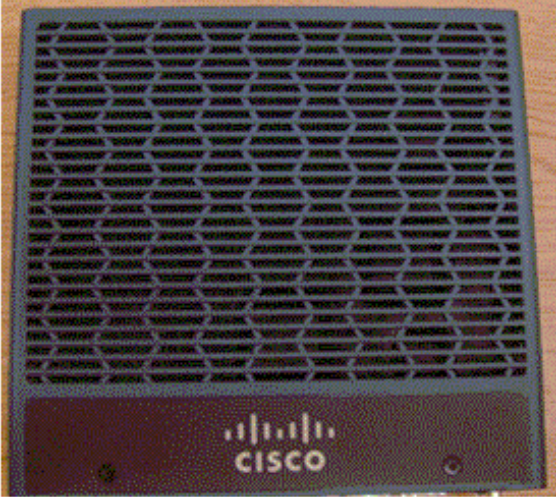
- 1 Clean the cover of any grease, dirt, or oil before applying the tamper evidence labels. Alcohol-based cleaning pads are recommended for this purpose. The temperature of the router should be above 10°C.
- 2 The tamper evidence label should be placed over the CF card in the slot so that any attempt to remove the card will show sign of tampering.
- 3 The tamper evidence label should be placed as indicated in the pictures below associated with the actual unit.
- 4 Place tamper evident labels on the opacity shield when used.
- 5 The labels completely cure within five minutes.

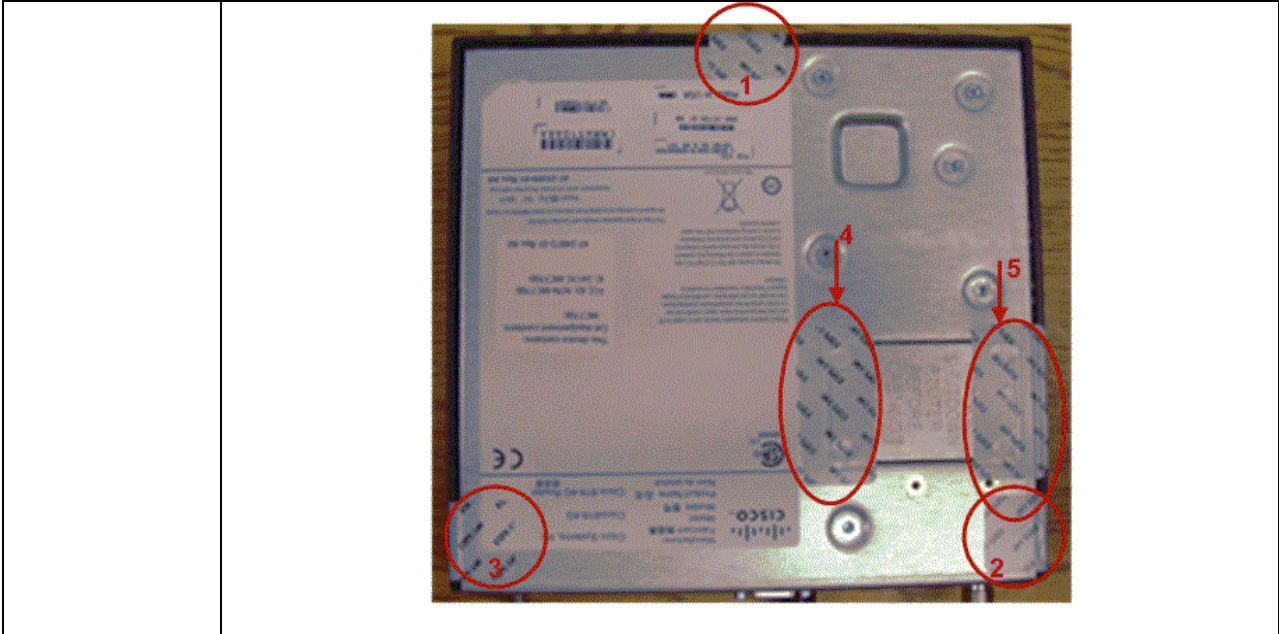
NOTE: Any unused TELs must be securely stored, accounted for, and maintained by the CO in a protected location.

NOTE: These security labels are very fragile and cannot be removed without clear signs of damage to the labels. The Crypto-Officer should inspect the seals for evidence of tamper as determined by their deployment policies (every 30 days is recommended). If the seals show evidence of tamper, the Crypto-Officer should assume that the modules have been compromised and contact Cisco accordingly.

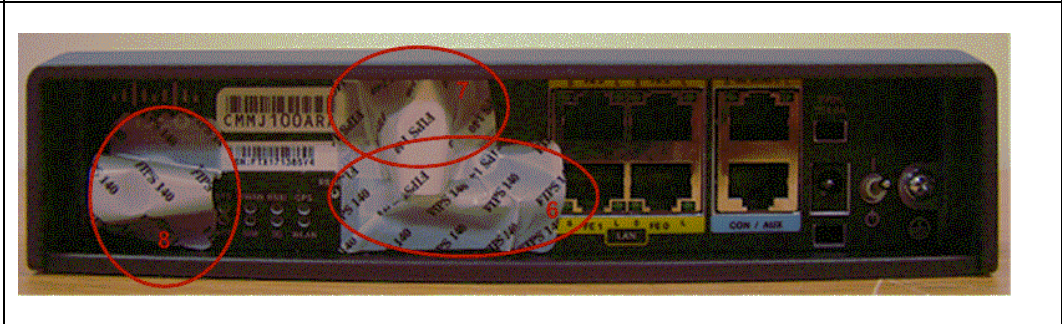
The following figures identify the placement of each TEL for each hardware model:

ISR 819G-4G-A-K9, 819G-4G-V-K9, 819G-S-K9, 819HG-4G-G-K9	
Front	
Right	

	
Left	
Top	
Bottom	



Back 819G-S-K9



Back
819G-4G-A-K9,
819G-4G-V-K9,
819HG-4G-G-K9

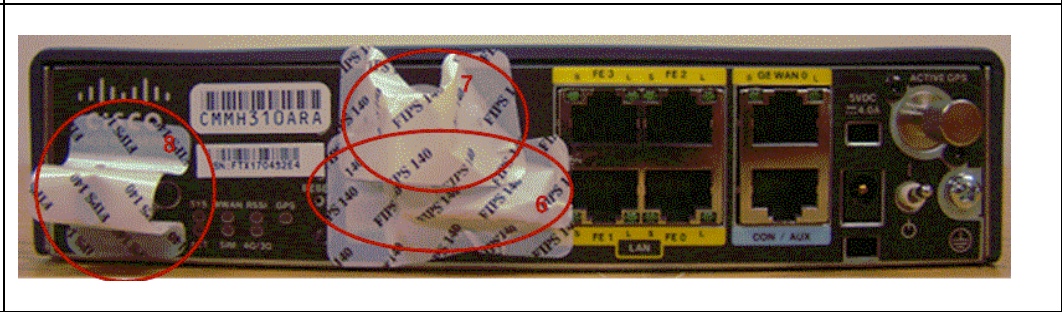
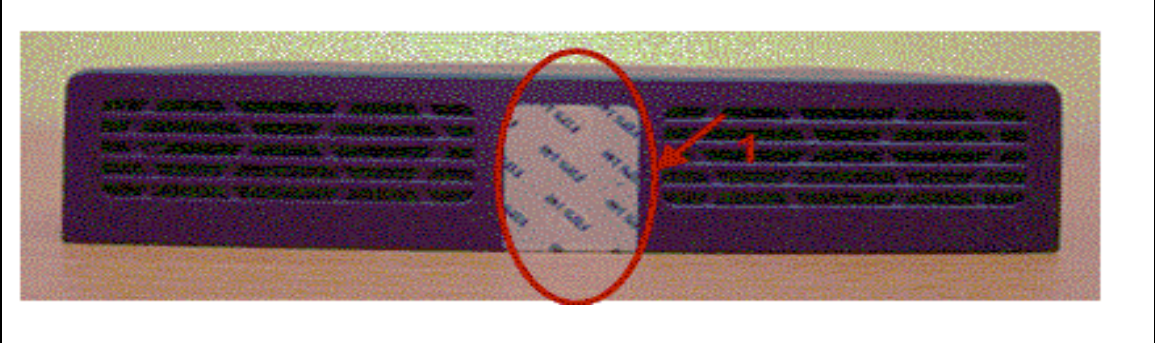


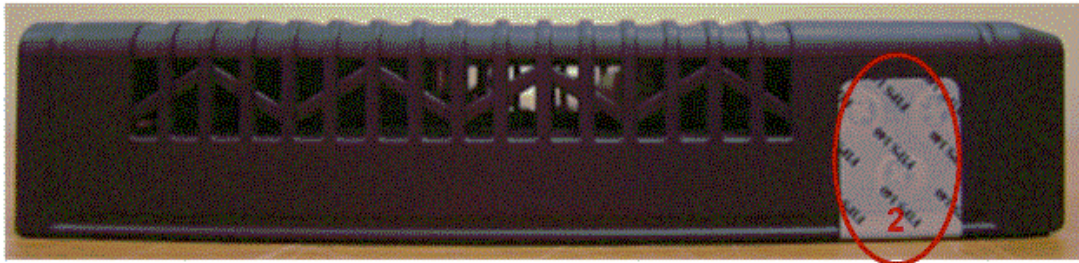
Table 9: ISR 819G-4G-A-K9, 819G-4G-V-K9, 819G-S-K9, 819HG-4G-G-K9 TELs

ISR 819H-K9

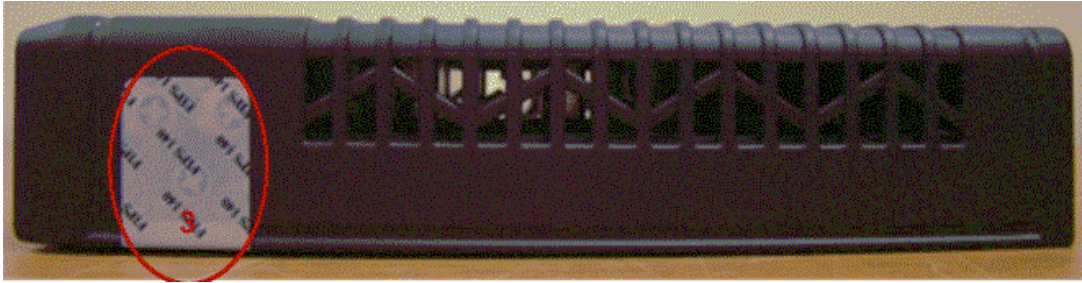
Front



Right



Left



Top



Bottom



Back

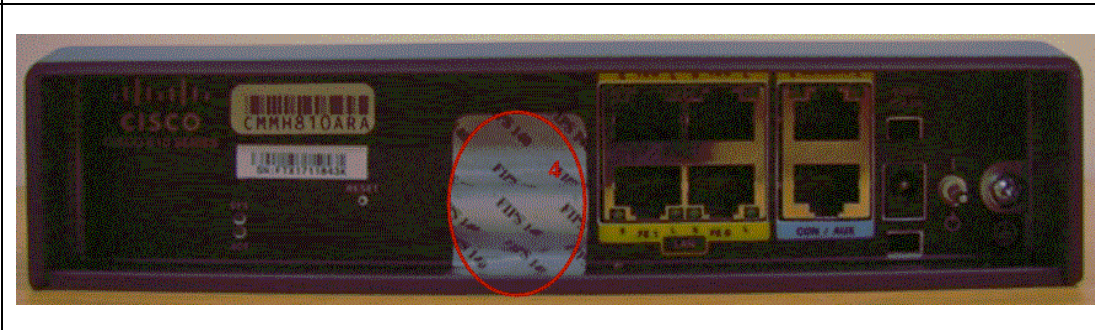
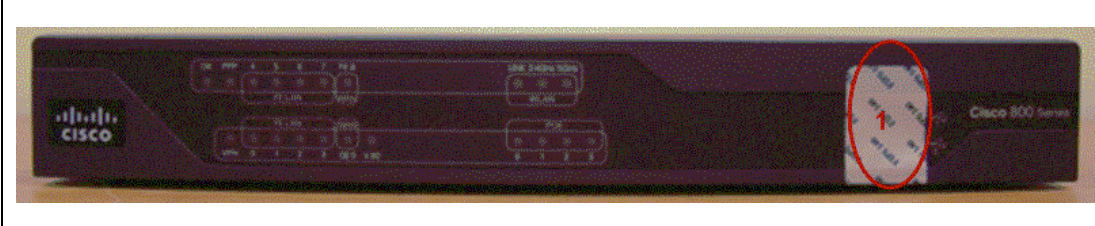


Table 10: ISR 819H-K9 TELs

ISR 881/ISR 891




Front



Right



Left

	
Top	
Bottom	
Back ISR 881	

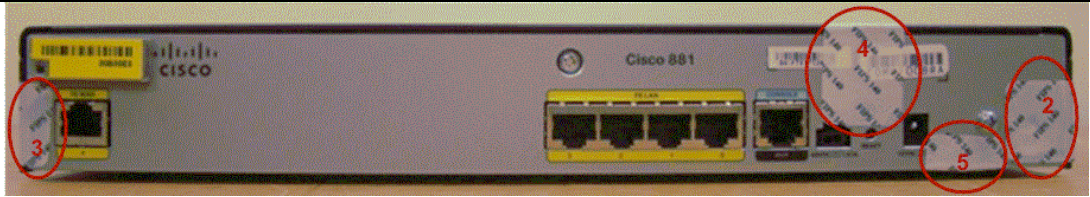
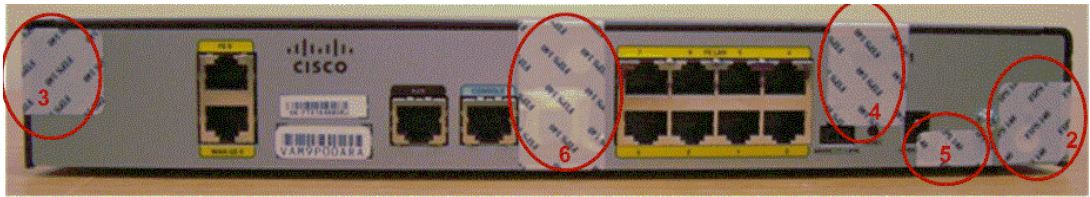
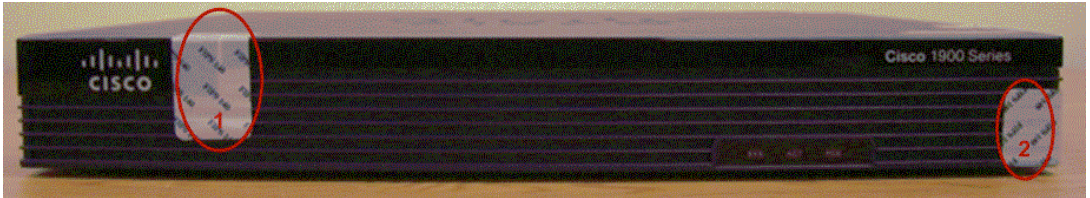
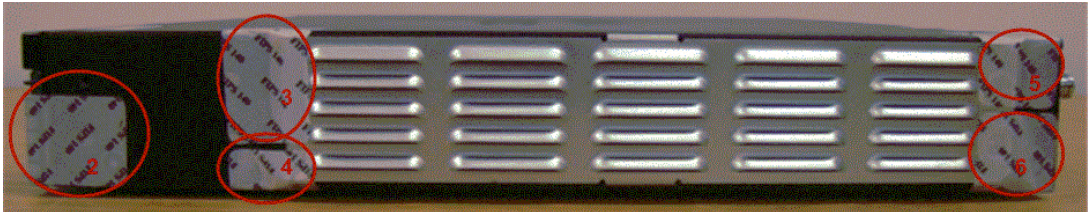

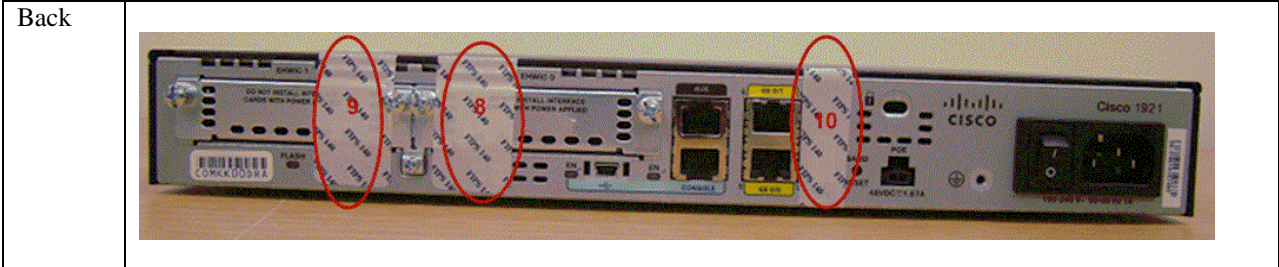
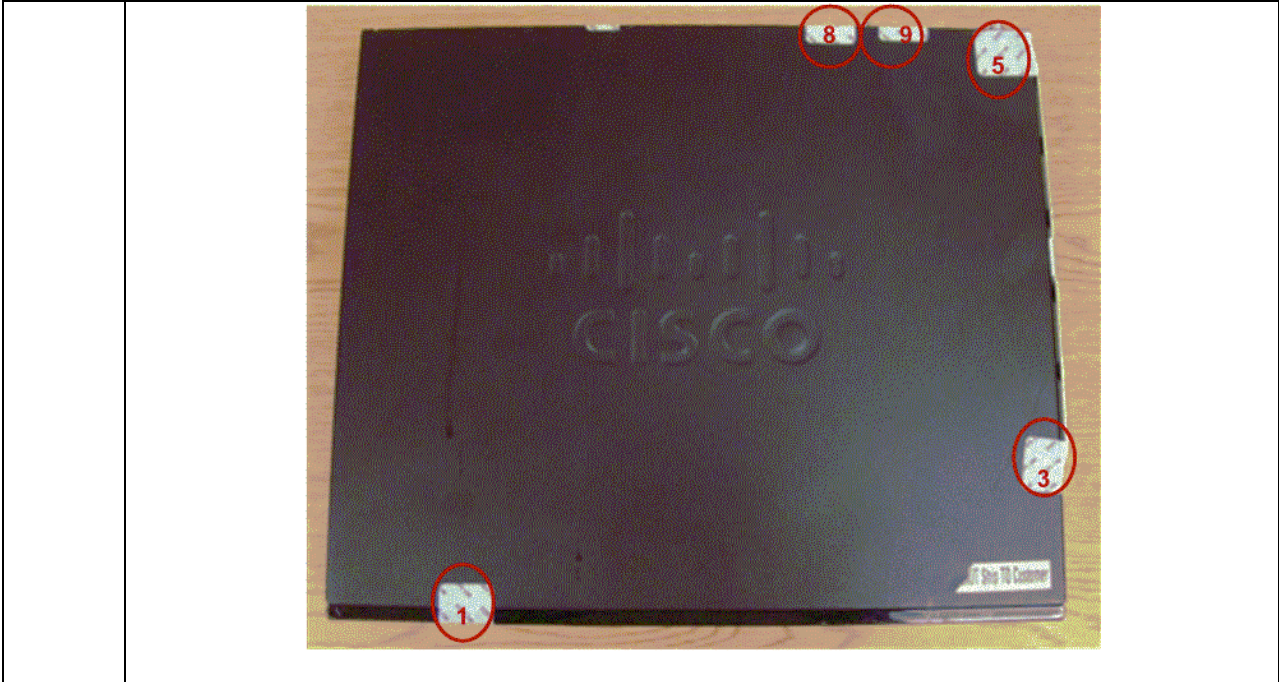
	
Back ISR 891	



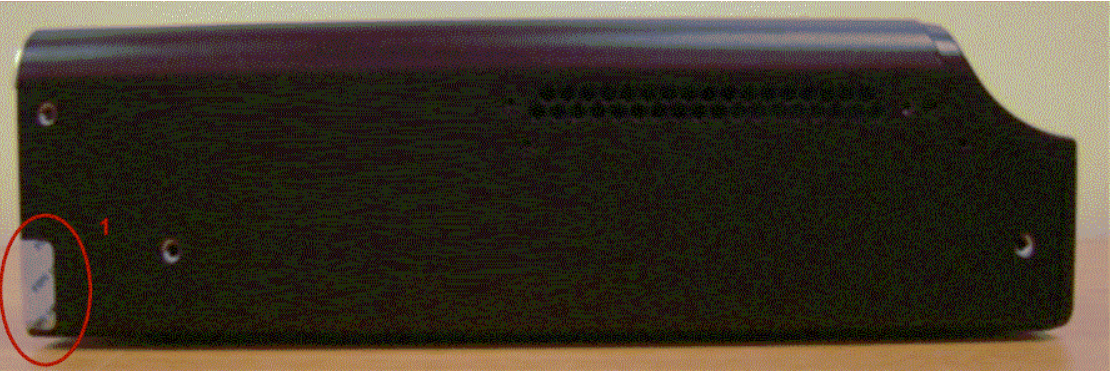
Table 11: ISR 881/891 TELs

ISR 1905/ISR 1921	
Front	
Right	
Left	
Top	



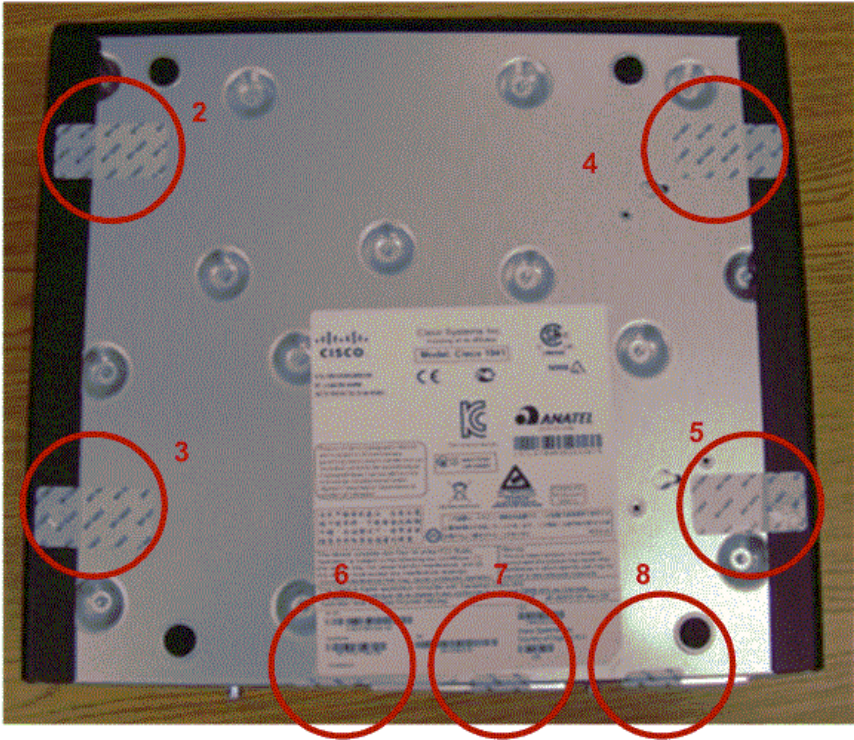
Note: The 1905 and 1921 ISRs are physically identical. All ports and interfaces are the same.

Table 12: ISR 1941 TELs

ISR 1941	
Front	
Right	
Left	
Top	



Bottom



Back

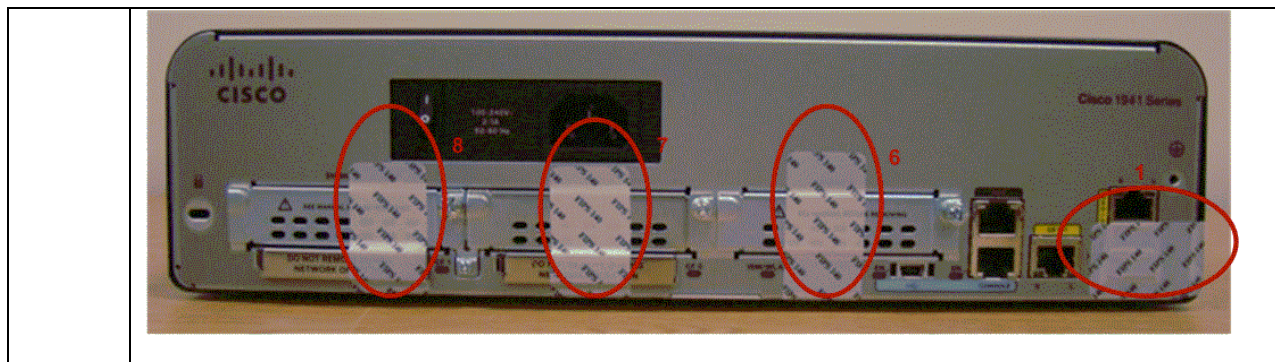


Table 73: ISR 1941 TELs

3 Secure Operation

The Cisco C819G-4G-A-K9, C819H-K9, 891, 881, 1905, 1921, 1941, C819G-4G-V-K9, C819G-S-K9 and C819HG-4G-G-K9 Integrated Services Routers meet all the Level 2 requirements for FIPS 140-2. Follow the setting instructions provided below to place the module in FIPS-approved mode. Operating this router without maintaining the following settings will remove the module from the FIPS approved mode of operation.

3.1 Initial Setup

- 1 The Crypto Officer must install opacity shields as described in this document (if applicable)
- 2 The Crypto Officer must apply tamper evidence labels as described in Section 2.4 of this document.
- 3 The Crypto Officer must disable IOS Password Recovery by executing the following commands:

```
configure terminal
no service password-recovery
end
show version
```

NOTE: Once Password Recovery is disabled, administrative access to the module without the password will not be possible.

3.2 System Initialization and Configuration

- 1 The Crypto Officer must perform the initial configuration. IOS 15.2(4)M5, Advanced Security build (advsecurity) is the only allowable image; no other image should be loaded. Once this image has been installed, no updates to software or firmware are permitted in FIPS mode of operations.
- 2 The value of the boot field must be 0x0102. This setting disables break from the console to the ROM monitor and automatically boots the IOS image. From the “configure terminal” command line, the Crypto Officer enters the following syntax:

```
config-register 0x0102
```

- 3 The Crypto Officer must create the “enable” password for the Crypto Officer role. The password must be at least 8 characters (all digits; all lower and upper case letters; and all special characters except ‘?’ are accepted) and is entered when the Crypto Officer first engages the “enable” command. The Crypto Officer enters the following syntax at the “#” prompt:

```
enable secret [PASSWORD]
```

- 4 The Crypto Officer must always assign passwords (of at least 8 characters) to users. Identification and authentication on the console port is required for Users. From the “configure terminal” command line, the Crypto Officer enters the following syntax:

```
line con 0
```

password [PASSWORD]
login local

- 5 RADIUS and TACACS+ shared secret key sizes must be at least 8 characters long.

3.3 IPSec Requirements and Cryptographic Algorithms

- 1 The only type of key management protocol that is allowed in FIPS mode is Internet Key Exchange (IKE), although manual creation of security associations is also permitted.
- 2 Although the IOS implementation of IKE allows a number of algorithms, only the following algorithms are allowed in a FIPS 140-2 configuration:
 - ah-sha-hmac
 - esp-sha-hmac
 - esp-Triple-DES
 - esp-aes
- 3 The following algorithms are not FIPS approved and should not be used during FIPS-approved mode:
 - DES
 - MD-5 for signing
 - MD-5 HMAC

3.4 SSLV3.1/TLS Requirements and Cryptographic Algorithms

When negotiating TLS cipher suites, only FIPS approved algorithms must be specified. All other versions of SSL except version 3.1 must not be used in FIPS mode of operation. The following algorithms are not FIPS approved and should not be used in the FIPS-approved mode:

- MD5
- RC4
- DES

3.5 Access

- 1 Telnet access to the module is only allowed via a secure IPSec tunnel between the remote system and the module. The Crypto officer must configure the module so that any remote connections via telnet are secured through IPSec, using FIPS-approved algorithms. Note that all users must still authenticate after remote access is granted.
- 2 SSH access to the module is only allowed if SSH is configured to use a FIPS-approved algorithm. The Crypto officer must configure the module so that SSH uses only FIPS-approved algorithms. Note that all users must still authenticate after remote access is granted.
- 3 SNMP access is only allowed via when SNMP v3 is configured with AES encryption.