Cisco Base Security Configuration

How to Use This Document

This document serves as a guide for the proper configuration of an ICS IT Cisco Switch. It does not aim to provide users with foundational knowledge of Cisco commands and functions.

The document is divided by configuration code intent used with Cisco IOS switches. The order of the presented code is not intended to indicate the correct implementation sequence, and additional configurations may be necessary from one block to another.

Procedures

The following code blocks can be implemented in any order after the switch has been booted to the IOS command line. Each code block can also be used independently or to verify an existing configuration.

Initial Configuration
Services
Set up switch services.
```plaintext
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
```
Hostname
Set the hostname of the switch.
```plaintext
hostname Hostname
```
Logging
Set up logging.
```plaintext
logging file flash:LOG_SWITCH8 89999 notifications
logging count
logging buffered 16000
logging console critical
```

```
no logging monitor
login on-failure log
login on-success log
```

Security
Set the main administration password.
```plaintext
enable secret 5 $1$17Sv$8ggwbemNPWiYG5OfzyDj10
```

Users
Set up users.
```plaintext
username username privilege 15 secret 5 $1$0OSy$a3Efm134K8B.CiI0FJrT9.
username username2 privilege 15 secret 5 $1$.JaZ$mQGaaM632DVlyAxIkyqxx0
```

Time Settings
Set your time zone and daylight savings time details.
```plaintext
no aaa new-model
clock timezone PST -8 0
clock summer-time PST recurring
system mtu routing 1500
```

Routing and DNS
Set the domain source and domain name server addresses.
```plaintext
no ip source-route
ip routing
no ip gratuitous-arps
!
ip domain-list pacs.local.lan
ip domain-lookup source-interface Vlan10
ip domain-name pacs.local.lan
ip name-server 192.168.0.1
ip name-server 192.168.0.2
```

Spanning-tree settings
Set the spanning-tree portfast settings.
```plaintext
spanning-tree mode pvst
spanning-tree portfast edge default
spanning-tree portfast edge bpduguard default
spanning-tree portfast edge bpdufilter default
spanning-tree extend system-id
!
```

vlan internal allocation policy ascending
no cdp run
```

## SSH Access
Set up SSH access.
```plaintext
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip tftp source-interface Loopback0
ip ssh time-out 60
ip ssh version 2
ip scp server enable
```

Access List
Set up the access list to limit device access to the shell interface. Include administration end points as IP addresses, one per line. IP addresses not listed will be denied access.
```plaintext
logging facility local1
logging source-interface Vlan10
access-list 38 remark *** Permitted Access Sources ***
access-list 38 permit 192.168.0.100
access-list 38 permit 192.168.0.101
```

Warning Banner
Set up the MOTD login working banner by following the terminal prompts and copy pasting as needed from the code below.
```plaintext
banner login
^C**********************************************************************
**********
_                **WARNING TO USERS OF THIS SYSTEM**
_
This computer system, including all related equipment, networks, and network
devices, is provided by [entity or business name] in accordance with
the policy for official use and limited personal use. This system may not
be connected to the Internet, in any way, unless specifically authorized by the
[authorizing individual or entity].

_
All computer systems may be monitored for all lawful purposes, including
but not limited to, ensuring that use is authorized, for management of the
system, to facilitate protection against unauthorized access, and to verify
security procedures, survivability and operational security. Any information on

this computer system may be examined, recorded, copied and used for authorized purposes at any time.  All information, including personal information, placed or sent over this system may be monitored, and users of this system are reminded that such monitoring does occur.  Therefore, there should be no expectation of privacy with respect to use of this system.

_
By logging into this computer system, you acknowledge and consent to the monitoring of this system.  Evidence of your use, authorized or unauthorized, collected during monitoring may be used for civil, criminal, administrative, or other adverse action.  Unauthorized or illegal use may subject you to prosecution.

_
==========
==========
```

Transport and Monitoring

Transport
Set up transport.
```plaintext
line con 0
 exec-timeout 15 0
 logging synchronous
 login local
line vty 0 4
 access-class 38 in
 exec-timeout 9 0
 logging synchronous
 login local
 transport input ssh
 transport output ssh
line vty 5 15
 access-class 38 in
 exec-timeout 9 0
 logging synchronous
 login local
 transport input ssh
 transport output ssh
```

Monitoring
Set up session-vlan monitoring.
```plaintext
monitor session 10 source vlan 10
scheduler interval 500
```
```

Interface Configuration

Loopback Interface
Set up the loopback interface.
```plaintext
interface Loopback0
 no ip address
```

Vlans
Set up the Vlans to be used. Alter for your environment and device.
```plaintext
!
interface Vlan1
 description Do not use
 no ip address
 shutdown
!
interface Vlan10
 description *** PACS Switch ***
 ip address 192.168.0.8 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
!
interface Vlan666
 description SWITCH LAN
 ip address 10.0.0.8 255.255.255.0
 no ip unreachables
```

Interface Security Configuration Settings

Set up each interface to either be shutdown (if no connection is expected), connected with macsticky security, trunk to another local switch or trunk to a remote switch using macsec encryption.

Unconnected Interface
```plaintext
interface GigabitEthernetX/X/X
 switchport access vlan 256
 switchport mode access
 shutdown
```

Connected Interface with Macsticky

```plaintext
interface GigabitEthernetX/X/X
 description YOUR-DESCRIPTION
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security violation restrict
 switchport port-security mac-address sticky
 spanning-tree bpduguard enable
```

Connected Local Trunk Port (No MACsec)
```plaintext
interface GigabitEthernet0/11
 description UPLINK to SWITCH_HOST_NAME
 switchport trunk allowed vlan 10
 switchport trunk native vlan 10
 switchport mode trunk
 no cdp enable
 spanning-tree portfast disable
```

Connected Remote Trunk Port (MACsec)
```plaintext
interface GigabitEthernetx/x/xx
 description test macsec
 switchport mode trunk
 macsec network-link
 mka policy MKA_128
 mka pre-shared-key key-chain KC_128
```

Cisco MACsec Configuration

Cisco 9300 Main Configuration MACsec Code
```plaintext
key chain KC_128 macsec
 key 12
   cryptographic-algorithm aes-128-cmac
  key-string 7 014A5651035F5F5677146F584B5143345328567C0F73786364044A21375257700F
```

Cisco 9300 Interface MACsec Code
```plaintext
interface GigabitEthernet1/1/1
 description UPLINK to KESWICK70
 switchport trunk native vlan 10
```

```
 switchport trunk allowed vlan 10
 switchport mode trunk
 no cdp enable
 macsec network-link
 mka policy MKA_128
 mka pre-shared-key key-chain KC_128
 spanning-tree portfast disable
```

Cisco 3650 Main Configuration MACsec Code
```plaintext
key chain KC_128 macsec
key 3C1337FCDCB631A33207210A261AED0C
cryptographic-algorithm aes-128-cmac
key-string 7 3c1337fcdcb631a33207210a261aed0c
```

Cisco 3650 Interface MACsec Code
```plaintext
interface GigabitEthernetx/x/xx
 description test macsec
 switchport mode trunk
 macsec network-link
 mka policy MKA_128
 mka pre-shared-key key-chain KC_128
```

Revision #3
Created 17 October 2025 16:37:58 by CGChambers
Updated 17 October 2025 16:57:16 by CGChambers