CHAPTER 12

Configuring Monitoring and Accounting

This chapter provides information about configuring monitoring and accounting using the VSPA on the Catalyst 6500 Series switch. It includes the following sections:

Note For detailed information on Cisco IOS IPsec cryptographic operations and policies, see the *Cisco IOS Security Configuration Guide, Release 12.2* at this URL:

http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/fsecur_c.html

For more information about the commands used in this chapter, see the *Cisco IOS Security Command Reference* at this URL:

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html

Also refer to the related Cisco IOS Release 12.2 software configuration guide, command reference, and master index publications. For more information about accessing these publications, see the "Related Documentation" section on page xvi.

Tip To ensure a successful configuration of your VPN using the VSPA, read all of the configuration summaries and guidelines before you perform any configuration tasks.

Overview of Monitoring and Accounting for the VSPA

This chapter describes some IPsec features that can be used to monitor and manage the VSPA. These features include:

- The IPsec VPN monitoring feature, which provides VPN session monitoring enhancements that will allow you to troubleshoot the VPN and monitor the end-user interface.
- The IPsec VPN accounting feature, which enables session accounting records to be generated by indicating when the session starts and when it stops.

- The IPsec and IKE MIB support for Cisco VRF-aware IPsec feature, which provides manageability of VPN routing and forwarding- (VRF-) aware IPsec using MIBs.

Monitoring and Managing IPsec VPN Sessions

The IPsec VPN monitoring feature provides VPN session monitoring enhancements that will allow you to troubleshoot the Virtual Private Network (VPN) and monitor the end-user interface. A crypto session is a set of IPsec connections (flows) between two crypto endpoints. If the two crypto endpoints use IKE as the keying protocol, they are IKE peers to each other. Typically, a crypto session consists of one IKE security association (for control traffic) and at least two IPsec security associations (for data traffic, one per each direction). There may be duplicated IKE security associations (SAs) and IPsec SAs or duplicated IKE SAs or IPsec SAs for the same session in the duration of rekeying or because of simultaneous setup requests from both sides.

Session monitoring enhancements include the following:

- Ability to specify an Internet Key Exchange (IKE) peer description in the configuration file
- Summary listing of crypto session status
- Syslog notification for crypto session up or down status
- Ability to clear both IKE and IP Security (IPsec) security associations (SAs) using one command-line interface (CLI)

Adding the Description of an IKE Peer

To add the description of an IKE peer to an IPsec VPN session, perform this task beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# crypto isakmp peer {ip-address` *ip-address*`}`	Enables an IPsec peer for IKE querying of authentication, authorization, and accounting (AAA) for tunnel attributes in aggressive mode and enters ISAKMP peer configuration mode. • *ip-address*—IP address of the peer.
Step 2	`Router(config-isakmp-peer)# description` *description*	Adds a description for an IKE peer. • *description*—Description identifying the peer.

This example shows how to add a description of an IKE peer:

```
Router(config)# show crypto isakmp peer 10.2.2.9
Router(config-isakmp-peer)# description connection from site A
```

Verifying Peer Descriptions

To verify peer descriptions, enter the **show crypto isakmp peer** command:

```
Router# show crypto isakmp peer
```

```
Peer: 10.2.2.9 Port: 500
Description: connection from site A
flags: PEER_POLICY
```

When the peer at address 10.2.2.9 connects and the session comes up, the syslog status will be shown as follows:

```
%CRYPTO-5-SESSION_STATUS: Crypto tunnel is UP. Peer 10.2.2.9:500 Description: connection
from site A Id: ezvpn
```

Getting a Summary Listing of Crypto Session Status

You can get a list of all the active VPN sessions by entering the **show crypto session** command. The listing will include the following:

- Interface
- IKE peer description, if available
- IKE SAs that are associated with the peer by which the IPsec SAs are created
- IPsec SAs serving the flows of a session

Multiple IKE or IPsec SAs may be established for the same peer, in which case IKE peer descriptions will be repeated with different values for the IKE SAs that are associated with the peer and for the IPsec SAs that are serving the flows of the session.

You can also use the **show crypto session detail** variant of this command to obtain more detailed information about the sessions.

The following is sample output for the **show crypto session** command without the **detail** keyword:

```
Router# show crypto session

Crypto session current status

Interface: FastEthernet0/1
Session status: UP-ACTIVE
Peer: 172.0.0.2/500
IKE SA: local 172.0.0.1/500 remote 172.0.0.2/500 Active
IPSEC FLOW: permit ip 10.10.10.0/255.255.255.0 10.30.30.0/255.255.255.0
Active SAs: 2, origin: crypto map
```

The following is sample output using the **show crypto session** command with the **detail** keyword:

```
Router# show crypto session detail

Interface: Tunnel0
Session status: UP-ACTIVE
Peer: 10.1.1.3 port 500 fvrf: (none) ivrf: (none)
Desc: this is my peer at 10.1.1.3:500 Green
Phase1_id: 10.1.1.3
IKE SA: local 10.1.1.4/500 remote 10.1.1.3/500 Active
Capabilities:(none) connid:3 lifetime:22:03:24
IPSEC FLOW: permit 47 host 10.1.1.4 host 10.1.1.3
Active SAs: 0, origin: crypto map
Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 0/0
IPSEC FLOW: permit ip host 10.1.1.4 host 10.1.1.3
Active SAs: 4, origin: crypto map
Inbound: #pkts dec'ed 4 drop 0 life (KB/Sec) 4605665/2949
Outbound: #pkts enc'ed 4 drop 1 life (KB/Sec) 4605665/2949
```

Syslog Notification for Crypto Session Up or Down Status

The syslog notification for crypto session up or down status function provides syslog notification every time the crypto session comes up or goes down. To enable syslog logging of the session status, enter the **crypto logging session** and **crypto logging ezvpn** commands in configuration mode.

The following is a sample syslog notification showing that a crypto session is up:

```
%CRYPTO-5-SESSION_STATUS: Crypto session is UP. Peer 10.6.6.1:500 fvrf=name10 ivrf=name20
Description: SJC24-2-VPN-Gateway Id: 10.5.5.2
```

The following is a sample syslog notification showing that a crypto session is down:

```
%CRYPTO-5-SESSION_STATUS: Crypto session is DOWN. Peer 10.6.6.1:500 fvrf=name10
ivrf=name20 Description: SJC24-2-VPN-Gateway Id: 10.5.5.2
```

Clearing a Crypto Session

In previous Cisco IOS software releases, there was no single command to clear both IKE and IPsec security associations (SAs). Instead, you entered the **clear crypto isakmp** command to clear IKE and the **clear crypto ipsec** command to clear IPsec. The **clear crypto session** command allows you to clear both IKE and IPsec with a single command. To clear a specific crypto session or a subset of all the sessions (for example, a single tunnel to one remote site), you must provide session-specific parameters, such as a local or remote IP address, a local or remote port, a front-door VPN routing and forwarding (FVRF) name, or an inside VRF (IVRF) name. Typically, the remote IP address will be used to specify a single tunnel to be deleted.

If a local IP address is provided as a parameter when you enter the **clear crypto session** command, all the sessions (and their IKE SAs and IPsec SAs) that share the IP address as a local crypto endpoint (IKE local address) will be cleared. If you do not provide a parameter when you enter the **clear crypto session** command, all IPsec SAs and IKE SAs in the switch will be deleted.

To clear a crypto session, enter the **clear crypto session** command in privileged EXEC mode from the switch command line. No configuration statements are required in the configuration file to use this command:

```
Router# clear crypto session
```

For complete configuration information for IPsec VPN Monitoring, refer to this URL:

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_ipsvm.html

For IPsec VPN monitoring configuration examples, see the "IPsec VPN Monitoring Configuration Example" section on page 12-12.

Configuring SPAN Monitoring for the VSPA

You can monitor VSPA port traffic using the local Switched Port Analyzer (SPAN) or remote SPAN (RSPAN). By configuring two SPAN sessions, one on the inside port and one on the outside port, you can monitor clear traffic and encrypted traffic simultaneously.

For detailed information on using SPAN, see the "Configuring Local SPAN, RSPAN, and ERSPAN" chapter of the *Catalyst 6500 Release 12.2SXH and Later Software Configuration Guide* at this URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/span.html

Note Do not configure one VSPA port as a source for more than one SPAN session.

Configuring a SPAN Session

To configure a local SPAN session using a VSPA port as a source, perform this task beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# monitor session` *session_number* `source [interface` *type slot/subslot/port* `| vlan` *vlan_number*`] rx`	Associates the local SPAN source session number with the source port or VLAN and selects the traffic direction to be monitored. • *session_number*—A user-defined identifying number for the session. Range is 1 to 66.
Step 2	`Router(config)# monitor session` *session_number* `destination interface` *type slot/port*	Specifies the destination for local SPAN session traffic.

This example shows how to configure a local SPAN session to capture inbound traffic before decryption from a VSPA in subslot 0 of module 2 and send the captured traffic to port 16 of module 5:

```
Router(config)# monitor session 1 source interface gi2/0/2 tx
Router(config)# monitor session 1 destination interface gi5/16
```

This example shows how to capture inbound traffic after decryption:

```
Router(config)# monitor session 1 source interface gi2/0/1 rx
```

This example shows how to capture outbound traffic before encryption:

```
Router(config)# monitor session 1 source interface gi2/0/1 tx
```

This example shows how to capture outbound traffic after encryption:

```
Router(config)# monitor session 1 source interface gi2/0/2 rx
```

Configuring IPsec VPN Accounting

The IPsec VPN accounting feature enables session accounting records to be generated by indicating when the session starts and when it stops.

A VPN session is defined as an Internet Key Exchange (IKE) security association (SA) and the one or more SA pairs that are created by the IKE SA. The session starts when the first IP Security (IPsec) pair is created and stops when all IPsec SAs are deleted. If IPsec accounting is configured, after IKE phases are complete, an accounting start record is generated for the session. New accounting records are not generated during a rekeying.

Session-identifying information and session-usage information is passed to the Remote Authentication Dial-In User Service (RADIUS) server by standard RADIUS attributes and vendor-specific attributes (VSAs).

To enable IPsec VPN accounting, perform this task beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# aaa new-model`	Enables periodic interim accounting records to be sent to the accounting server.
Step 2	`Router(config)# aaa authentication login` *list-name* `group radius`	Sets authentication, authorization, and accounting (AAA) authentication at login using RADIUS servers. • *list-name*—Character string used to name the list of authentication methods activated when a user logs in. • **group radius**—Uses the list of all RADIUS servers for authentication.
Step 3	`Router(config)# aaa authorization network` *list-name* `group radius`	Runs authorization for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Programs (NCPs), and AppleTalk Remote Access (ARA). • *list-name*—Character string used to name the list of authorization methods activated when a user logs in. • **group radius**—Uses the list of all RADIUS servers for authentication.

	Command	Purpose
Step 4	`Router(config)# aaa accounting network list-name start-stop [broadcast] group radius`	Enables AAA accounting of network-related requested services for billing or security purposes when you use RADIUS. • *list-name*—Character string used to name the list of the accounting methods. • **start-stop**—Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested user process begins regardless of whether the start accounting notice was received by the accounting server. • **broadcast**—(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, failover occurs using the backup servers defined within that group. • **group radius**—Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.
Step 5	`Router(config)# aaa accounting update periodic minutes`	(Optional) Sends accounting updates to the accounting server while a session is up. • *minutes* — Specifies the interval (in number of minutes) at which accounting records are to be sent to the accounting server.
Step 6	`Router(config)# aaa session-id common`	Specifies whether the same session ID will be used for each AAA accounting service type within a call or whether a different session ID will be assigned to each accounting service type. • **common**—Ensures that all session identification (ID) information that is sent out for a given call will be made identical. The default behavior is common.
Step 7	`Router(config)# crypto isakmp profile profile-name`	Audits IP security (IPsec) user sessions and enters isakmp-profile configuration mode. • *profile-name*—Name of the user profile. To associate a user profile with the RADIUS server, the user profile name must be identified.
Step 8	`Router(conf-isa-prof)# vrf ivrf`	Associates the on-demand address pool with a Virtual Private Network (VPN) routing and forwarding (VRF) instance name. • *ivrf*—VRF to which the IPsec tunnel will be mapped.

	Command	Purpose
Step 9	`Router(conf-isa-prof)# match identity group group-name`	Matches an identity from a peer in an ISAKMP profile. • *group-name*—A unity group that matches identification (ID) type ID_KEY_ID. If unity and main mode Rivest, Shamir, and Adelman (RSA) signatures are used, the *group-name* argument matches the Organizational Unit (OU) field of the Distinguished Name (DN).
Step 10	`Router(conf-isa-prof)# client authentication list list-name`	Configures Internet Key Exchange (IKE) extended authentication (XAUTH) in an Internet Security Association and Key Management Protocol (ISAKMP) profile. • *list-name*—Character string used to name the list of authentication methods activated when a user logs in. The list name must match the list name that was defined during the authentication, authorization, and accounting (AAA) configuration.
Step 11	`Router(conf-isa-prof)# isakmp authorization list list-name`	Configures an IKE shared secret and other parameters using the AAA server in an ISAKMP profile. The shared secret and other parameters are generally pushed to the remote peer via mode configuration (MODECFG). • *list-name*—AAA authorization list used for configuration mode attributes or preshared keys for aggressive mode.
Step 12	`Router(conf-isa-prof)# client configuration address [initiate | respond]`	Configures IKE mode configuration (MODECFG) in the ISAKMP profile. • **initiate**—(Optional) Switch will attempt to set IP addresses for each peer. • **respond**—(Optional) Switch will accept requests for IP addresses from any requesting peer.
Step 13	`Router(conf-isa-prof)# accounting list-name`	Enables AAA accounting services for all peers that connect via this ISAKMP profile. • *list-name*— Name of a client accounting list.
Step 14	`Router(conf-isa-prof)# exit`	Exits isakmp profile configuration mode and returns to global configuration mode.
Step 15	`Router(config)# crypto dynamic-map dynamic-map-name dynamic-seq-num`	Creates a dynamic crypto map template and enters the crypto map configuration command mode. • *dynamic-map-name*—Name of the dynamic crypto map set that should be used as the policy template. • *dynamic-seq-num*—Sequence number you assign to the dynamic crypto map entry.

	Command	Purpose
Step 16	`Router(config-crypto-map)# set transform-set transform-set-name`	Specifies which transform sets can be used with the crypto map template. A transform set defines IPsec security protocols and algorithms. Transform sets and their accepted values are described in the *Cisco IOS Security Command Reference*. • *transform-set-name*—Name of the transform set.
Step 17	`Router(config-crypto-map)# set isakmp-profile profile-name`	Sets the ISAKMP profile name. • *profile-name*—Name of the ISAKMP profile.
Step 18	`Router(config-crypto-map)# reverse-route [remote-peer]`	Allows routes (IP addresses) to be injected for destinations behind the VPN remote tunnel endpoint and may include a route to the tunnel endpoint itself (using the **remote-peer** keyword for the crypto map). • **remote-peer**—(Optional) Routes of public IP addresses and IP security (IPsec) tunnel destination addresses are inserted into the routing table.
Step 19	`Router(config-crypto-map)# exit`	Exits crypto map configuration mode and returns to global configuration mode.
Step 20	`Router(config)# crypto map map-name ipsec-isakmp dynamic dynamic-map-name`	Creates a crypto profile that provides a template for configuration of dynamically created crypto maps. • *map-name*—Name that identifies the crypto map set. • *dynamic-map-name*—Name of the dynamic crypto map set that should be used as the policy template.
Step 21	`Router(config)# radius-server host ip-address [auth-port auth-port-number] [acct-port acct-port-number]`	Specifies a RADIUS server host. • *ip-address* —IP address of the RADIUS server host. • *auth-port-number*—(Optional) UDP destination port number for authentication requests; the host is not used for authentication if set to 0. If unspecified, the port number defaults to 1645. • *acct-port-number*—(Optional) UDP destination port number for accounting requests; the host is not used for accounting if set to 0. If unspecified, the port number defaults to 1646.
Step 22	`Router(config)# radius-server key string`	Sets the authentication and encryption key for all RADIUS communications between the switch and the RADIUS daemon. • *string*—The unencrypted (cleartext) shared key.

	Command	Purpose
Step 23	`Router(config)# interface type slot/[subslot]/port`	Configures an interface type and enters interface configuration mode. • *slot*/[*subslot*]/*port*—Number of the slot, subslot (optional), and port to be configured.
Step 24	`Router(config-if)# crypto map map-name`	Applies a previously defined crypto map set to an interface. • *map-name*—Name that identifies the crypto map set.

For complete configuration information for IPsec VPN Accounting, refer to this URL:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_evpna.html

For IPsec VPN accounting configuration examples, see the "IPsec VPN Accounting Configuration Example" section on page 12-10.

Configuration Examples

This section provide examples of the following configurations:

IPsec VPN Accounting Configuration Example

The following example shows how to enable the IPsec VPN accounting feature:

```
aaa new-model
!
!
aaa group server radius r1
 server-private 10.30.1.52 auth-port 1812 acct-port 1813 key allegro
!
aaa authentication login test_list group r1
aaa authorization network test_list group r1
aaa accounting update periodic 10 jitter maximum 0
aaa accounting network test_list start-stop group r1
!
ip vrf ivrf1
 rd 1:2
!
crypto engine mode vrf
!
crypto isakmp policy 5
 encr 3des
 authentication pre-share
 group 2
 lifetime 14400
!
crypto isakmp client configuration group test
 key world
 pool pool1
!
```

```
crypto isakmp profile test_pro
   vrf ivrf1
   match identity group test
   client authentication list test_list
   isakmp authorization list test_list
   client configuration address respond
   accounting test_list
!
crypto ipsec transform-set t3 esp-3des esp-sha-hmac
!
!
crypto dynamic-map dyn-ra 10
 set transform-set t3
 set isakmp-profile test_pro
 reverse-route
!
!
crypto map map-ra local-address GigabitEthernet3/15
crypto map map-ra 1 ipsec-isakmp dynamic dyn-ra
!
!
interface GigabitEthernet1/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,1002-1005
 switchport mode trunk
 mtu 9216
 mls qos trust ip-precedence
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast edge trunk
!
interface GigabitEthernet1/0/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,1002-1005
 switchport mode trunk
 mtu 9216
 mls qos trust ip-precedence
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast edge trunk
!
!

interface GigabitEthernet3/15
 mtu 9216
 ip address 120.0.0.254 255.255.255.0
crypto engine outside
!
!
!
interface Vlan100
 ip vrf forwarding ivrf1
 ip address 120.0.0.100 255.255.255.0
 ip flow ingress
 crypto map map-ra
crypto engine slot 1/0 inside
!
!
!
ip local pool pool1 100.0.1.1 100.0.5.250
```

IPsec VPN Monitoring Configuration Example

The following example shows how to configure an IKE peer for IPsec VPN monitoring:

```
!
upgrade fpd auto
version 12.2
service timestamps debug datetime
service timestamps log datetime
no service password-encryption
service counters max age 5
!
hostname Ez-DCM-CC
!
boot-start-marker
boot system disk1:s72033-adventerprisek9_wan-mz.122-33.SXI
boot-end-marker
!
logging buffered 1000000 debugging
enable secret 5 $1$i5FZ$47ybx5dEaUKc3eRaDIZ/z.
!
aaa new-model
aaa authentication login myuserlist local
aaa authorization network myuserlist local
!
aaa session-id common
clock timezone PST -7
ip subnet-zero
!
no ip domain-lookup
ip domain-name cisco.com
ipv6 mfib hardware-switching replication-mode ingress
vtp mode transparent
no mls acl tcam share-global
mls netflow interface
no mls flow ip
no mls flow ipv6
mls cef error action freeze
!
redundancy
 keepalive-enable
 mode sso
 linecard-group 0 feature-card
  class load-sharing
  subslot 4/0
 main-cpu
  auto-sync running-config
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
diagnostic monitor syslog
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
!
power redundancy-mode combined
port-channel per-module load-balance
!
vlan internal allocation policy descending
vlan access-log ratelimit 2000
!
vlan 2-3,16-17
!
crypto logging session
```

```
crypto logging ezvpn
!
crypto logging ezvpn group mygroup
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
 lifetime 43200
crypto isakmp key WorldCup2006 address 0.0.0.0 0.0.0.0
!
crypto isakmp client configuration group mygroup
 key mykey
 pool mypool
!
crypto isakmp peer address 16.0.0.3
 description first-ezvpn-client
!
crypto isakmp peer address 16.0.0.4
 description second-ezvpn-client
!
crypto ipsec security-association lifetime seconds 21600
!
crypto ipsec transform-set MyTranSet esp-aes esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto call admission limit ike in-negotiation-sa 10
!
crypto dynamic-map DynMap1 10
 set transform-set MyTranSet
 reverse-route
!
crypto map MyMap1 client authentication list myuserlist
crypto map MyMap1 isakmp authorization list myuserlist
crypto map MyMap1 client configuration address respond
crypto map MyMap1 500 ipsec-isakmp dynamic DynMap1
!
interface GigabitEthernet1/25
 no ip address
 crypto connect vlan 16
!
interface GigabitEthernet1/27
 no ip address
 crypto connect vlan 17
!
interface GigabitEthernet1/29
 ip address 26.0.0.2 255.255.255.0
!
interface GigabitEthernet4/0/1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 16,17,1002-1005
 switchport mode trunk
 mtu 9216
 mls qos vlan-based
 mls qos trust cos
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet4/0/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1002-1005
```

```
 switchport mode trunk
 mtu 9216
 mls qos trust cos
 flowcontrol receive on
 flowcontrol send off
 spanning-tree portfast trunk
!
interface GigabitEthernet5/2
 ip address 44.0.111.114 255.0.0.0
 media-type rj45
!
interface Vlan1
 no ip address
 ip flow ingress
 ip igmp snooping querier
 shutdown
!
interface Vlan16
 ip address 16.0.0.2 255.255.224.0
 no mop enabled
 crypto map MyMap1
 crypto engine slot 4/0
!
interface Vlan17
 ip address 16.0.32.2 255.255.224.0
 no mop enabled
 crypto map MyMap1
 crypto engine slot 4/0
!
ip local pool mypool 36.0.0.1 36.0.15.254
ip local pool mypool 36.0.16.1 36.0.31.254
ip local pool mypool 36.0.32.1 36.0.47.254
ip local pool mypool 36.0.48.1 36.0.63.254
ip default-gateway 44.0.100.1
ip classless
ip route 43.0.0.0 255.0.0.0 44.0.100.1
ip route 45.0.0.0 255.0.0.0 44.0.100.1
ip route 223.255.254.53 255.255.255.255 44.0.100.1
ip route 223.255.254.54 255.255.255.255 44.0.100.1
!
no ip http server
no ip http secure-server
!
radius-server source-ports 1645-1646
!
control-plane
!
dial-peer cor custom
!
line con 0
 exec-timeout 0 0
line vty 0 4
 password cisco
 transport input lat pad mop udptn telnet rlogin ssh nasi acercon
line vty 5 15
 transport input lat pad mop udptn telnet rlogin ssh nasi acercon
!
monitor event-trace platform cmfi lc agg-label
monitor event-trace platform cmfi lc error
ntp clock-period 17280219
ntp update-calendar
ntp server 223.255.254.254
ntp server 223.255.254.53
mac-address-table aging-time 0
```

```
!
end
```