61200860L1-29.2D
March 2005

ADTRAN®

Configuration Guide

Virtual Private Network (VPN)

VPN Using Preset Keys, Mode Config, and Manual Keys

This Configuration Guide is designed to provide you with a basic understanding of the concepts behind configuring your ADTRAN Operating System (AOS) product for VPN applications. For detailed information regarding specific command syntax, refer to the *AOS Command Reference Guide* on your *ADTRAN OS Documentation* CD.

This guide consists of the following sections:

Understanding VPN

A truly private network is a network where a single entity (e.g., a company) owns all the wires from point A to point B. In a Virtual Private Network (VPN), some part of the path from A to B is a public network (e.g., the Internet or the public telephone system). VPN software technology creates a private "tunnel" through the public network system for your sensitive traffic. Using encryption and authentication methods, a VPN provides security over unsecured media.

VPN Benefits

VPNs provide a very cost-effective means of private communication by using inexpensive local call ISDN or telephone connections (with the Internet as the backbone).

VPN Limitations

Obviously, when a technology incorporates portions of the network that are physically not in its control, there are Quality of Service (QoS) limitations. With a true private network, users can demand a guaranteed QoS from the telephone company or provider. However, this is not as clear-cut with VPNs.

IPSec Encryption and Authentication

Sensitive information should not be sent over the Internet without some means of ensuring security. Internet Protocol (IP) was not originally designed to be secure. Due to its method of routing packets, IP-based networks are extremely vulnerable to spoofing, session hijacking, and many other network attacks. IPSec was developed by the Internet Engineering Task Force (IETF) to solve security issues over IP. IPSec encrypts and authenticates the data passing through the VPN tunnel, providing confidentiality and data integrity over the public network.

Encryption

VPN-provided encryption algorithms (3DES, DES, etc.) are key to data confidentiality, allowing data to pass through the network protected from unauthorized access.

Authentication

VPN-provided authentication may be used to ensure both data integrity and trusted-source data origination. The use of hash algorithms (such as MD5 or SHA) ensures that data has not changed during transfer. The use of pre-shared keys or digital certificates ensures that the data is from a trusted/accepted source.

Configuring Your Router

The following are given as examples of common configurations:

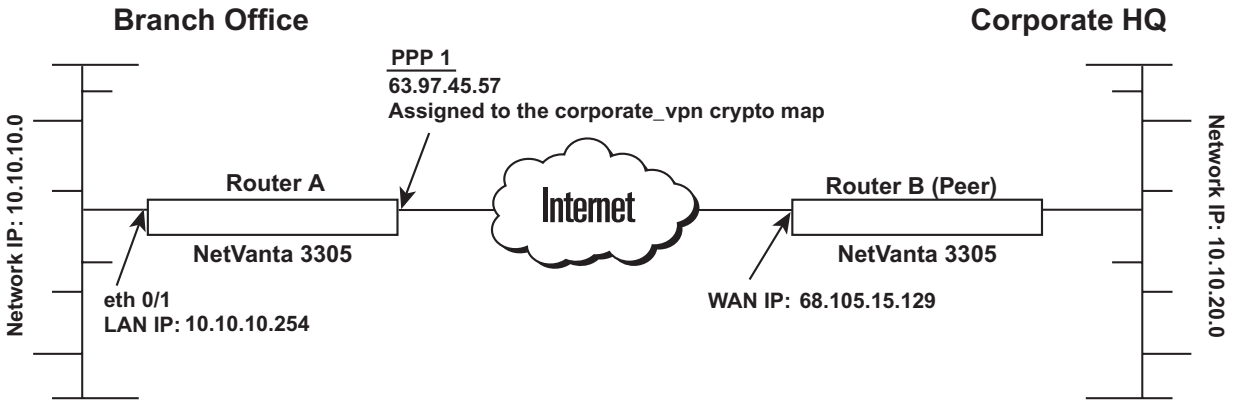
Configuration steps for each example are provided in the tables which follow the configuration descriptions. You can follow the given steps by entering the command text shown in **bold** (modifying as needed for your application).

Please note that these examples are given for your study and consideration only. They are to help you reach a better understanding of the fundamental concepts before configuring your own application. It will be necessary for you to modify these examples to match your own network's configuration.

Use the sample scripts in this section as a shortcut to configuring your unit. Use the text tool in Adobe Acrobat to select and copy the scripts, paste them into any text editing program, modify as needed, and then paste them directly into your AOS command line.

Example 1: VPN Using IKE with Pre-Shared Keys (Site-to-Site VPN)

The following example configures an AOS device for VPN using IKE main mode with pre-shared keys. This is a common configuration used to support site-to-site communication over VPN (see Figure 1). In this setup, the device is configured to initiate and respond in main mode.



Note: The VPN gateways involved may be connected through multiple routers.

Figure 1. Site-to-Site VPN

Table 1. Step-by-Step Configuration: IKE with Pre-Shared Keys

Step	Action	Command
1	Enter Enable Security mode.	>**enable**
2	Enter Global Configuration mode.	**#configure terminal**
3	Enable VPN functionality.	(config)**#ip crypto**
4	Set the local ID during IKE negotiation to be the IP address of the interface from which the traffic exits.	(config)**#crypto ike local-id address**
	Note: *You can override this setting on a per-policy basis by using the **local-id** command in the IKE Policy command set.*	
5	Create an IKE policy with a priority of 10 and enter the IKE Policy command set.	(config)**#crypto ike policy 10**
6	Configure this policy to accept the global local-id setting (as described in step 4, above).	(config-ike)**#no local-id**
7	Enter the IP address of the peer device. This policy can now initiate or respond to the peer.	(config-ike)**#peer 68.105.15.129**
	Note: Repeat this command for multiple peers, if necessary.	
8	Specify to initiate negotiations using main mode.	(config-ike)**#initiate main**

Table 1. Step-by-Step Configuration: IKE with Pre-Shared Keys *(Continued)*

Step	Action	Command
	Note: Aggressive mode can be used when one end of the VPN tunnel has a dynamically-assigned address. The side with the dynamic address must be the initiator of the traffic and tunnel. The side with the static address must be the responder. Please note that in some situations, using aggressive mode with pre-shared keys can compromise network security.	
9	Allow the IKE policy to respond to IKE negotiations from peers using main mode.	(config-ike)**#respond main**
10	Enter the IKE Policy Attribute command mode, assigning this attribute a priority of 10.	(config-ike)**#attribute 10**
	Note: Multiple attributes can be created for a single IKE policy. The attribute's priority number specifies the order in which the resulting VPN proposals get sent to the far end.	
11	Choose the 3DES encryption algorithm for this IKE policy to use to transmit data over the IKE-generated SA.	(config-ike-attribute)**#encryption 3des**
12	Specify the hash SHA algorithm to be used to authenticate the data transmitted over the IKE SA.	(config-ike-attribute)**#hash sha**
13	Configure this IKE policy to use pre-shared secrets during IKE negotiation to validate the peer.	(config-ike-attribute)**#authentication pre-share**
14	Specify Diffie-Hellman Group 1 to be used by this IKE policy to generate the keys (which are then used to create the IPSec SA).	(config-ike-attribute)**#group 1**
15	Specify that the IKE SA is valid for 24 hours (i.e., 86400 seconds).	(config-ike-attribute)**#lifetime 86400**
16	Exit to Global Configuration mode.	(config-ike-attribute)**#exit**
17	Specify the remote ID and associate it with a pre-shared key (**mysecret123**).	(config)**#crypto ike remote-id address 68.105.15.129 preshared-key mysecret123**
18	Create a transform set (**highly_secure**) consisting of two security algorithms (up to three algorithms may be defined).	(config)**#crypto ipsec transform-set highly_secure esp-3des esp-sha-hmac**
19	Place this transform set in tunnel mode (used almost exclusively in VPN configurations involving multiple subnets).	(cfg-crypto-trans)**#mode tunnel**
20	Create an empty access list and enter the extended access list command set.	(cfg-crypto-trans)**#ip access-list extended corporate_traffic**
	Note: The following message is displayed once you enter this command: **Configuring New Extended ACL "corporate_traffic"**.	
21	Specify the traffic to be sent through the VPN tunnel (see note, below).	(config-ext-nacl)**#permit ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255 log**

Table 1. Step-by-Step Configuration: IKE with Pre-Shared Keys *(Continued)*

Step	Action	Command
	Note: In this example, traffic with a source IP of our LAN network (10.10.10.0) and a destination IP of the peer private network (10.10.20.0) is allowed.	
22	Specify that all other traffic (not permitted in the previous step) is denied.	(config-ext-nacl)**#deny ip any any**
23	Create an IPSec crypto map (**corporate_vpn**) to define the IPSec tunnel. Assign a map index of 1.	(config-ext-nacl)**#crypto map corporate_vpn 1 ipsec-ike**
	Note: *The map index number allows the AOS device to rank crypto maps. When multiple maps are defined, this number determines the order in which they are considered. Maps with the lowest number are evaluated first.*	
24	Assign the access list **corporate_traffic** to this crypto map.	(config-crypto-map)**#match address corporate_traffic**
25	Set the IP address of the peer device.	(config-crypto-map)**#set peer 68.105.15.129**
26	Assign the transform set **highly_secure** to this crypto map.	(config-crypto-map)**#set transform-set highly_secure**
27	Define the lifetime (in seconds) for the IPSec SAs created by this crypto map.	(config-crypto-map)**#set security-association lifetime seconds 28800**
28	Configure the unit to not use PFS (perfect forward secrecy) when creating new IPSec SAs.	(config-crypto-map)**#no set pfs**
29	Access configuration parameters for the PPP interface.	(config-crypto-map)**#interface ppp 1**
30	Assign an IP address and subnet mask to the WAN interface.	(config-ppp 1)**#ip address 63.97.45.57 255.255.255.248**
31	Apply the crypto map **corporate_vpn** to the WAN interface.	(config-ppp 1)**#crypto map corporate_vpn**
32	Activate the WAN interface.	(config-ppp 1)**#no shutdown**
33	Access configuration parameters for the Ethernet port.	(config-ppp 1)**#interface ethernet 0/1**
34	Assign an IP address and subnet mask to the Ethernet port.	(config-eth 0/1)**#ip address 10.10.10.254 255.255.255.0**
35	Activate the Ethernet port.	(config-eth 0/1)**#no shutdown**
36	Exit to Global Configuration mode.	(config-eth 0/1)**#exit**

Sample Script

```
! Enter the Configure Terminal Mode
enable
configure terminal

! Turn on VPN Support
ip crypto
```



```
! By default, the local-id of the device will be the IPv4 address
! of the interface over which the IKE negotiation is occurring
crypto ike local-id address

! Create an IKE policy with priority of 10
! Mode: main
! Local-id: Do NOT override the system local-id policy
! Peer: 68.105.15.129
! Can Initiate or Respond to IKE negotiation
! One attribute configured - Number: 10
!   Encryption Algorithm: 3DES
!   Hash Algorithm:  SHA1
!   Authentication Type:  Pre-shared Keys
!   Group:  Diffie-Hellman Group 1
!   IKE SA Lifetime:  86400 seconds
crypto ike policy 10
  no local-id
  peer 68.105.15.129
  initiate main
  respond main
  attribute 10
    encryption 3des
    hash sha
    authentication pre-share
    group 1
    lifetime 86400

! Define the remote-id and pre-shared key for peer 68.105.15.129
crypto ike remote-id address 68.105.15.129 preshared-key mysecret123

! Define the transform-set to be used to secure data transmitted
! and received over the IPSec tunnel
crypto ipsec transform-set highly_secure esp-3des esp-sha-hmac
mode tunnel

! Specify the traffic to be sent over the VPN tunnel.
! With respect to this unit, that traffic would be anything with
! a source IP of our LAN network (10.10.10.0) and a destination
! IP of the Peer Private network (10.10.20.0).
! All other traffic will not be allowed over the tunnel.
ip access-list extended corporate_traffic
  permit ip 10.10.10.0 0.0.0.255 10.10.20.0 0.0.0.255 log
  deny ip any any

! Create an IPSec Crypto Map to define the IPSec tunnel
! Crypto Map Name:  corporate_vpn
! Crypto Map Index: 1
```



```
! Select VPN tunnel traffic using named ACL "corporate_traffic"
! Peer: 68.105.15.129
! Use the encryption and authentication transform-set as specified
!  in "highly_secure"
! IPSec Lifetime: 8000 Kbytes or 28800 seconds, whichever comes first
! Do not use Perfect Forward Secrecy when creating new IPSec SAs
crypto map corporate_vpn 1 ipsec-ike
  match address corporate_traffic
  set peer 68.105.15.129
  set transform-set highly_secure
  set security-association lifetime seconds 28800
  no set pfs

! Configure the public interface (ppp 1)
! Apply the specified crypto map to our public interface,
interface ppp 1
  ip address 63.97.45.57 255.255.255.248
  crypto map corporate_vpn
  no shutdown

! Configure the private interface (ethernet 0/1)
interface ethernet 0/1
  ip address 10.10.10.254 255.255.255.0
  no shutdown
```

Example 2: VPN Using Mode Config Support (Remote Access VPN)

The following example configures an AOS device for VPN using IKE main mode with pre-shared keys and mode config support (i.e., IPv4 address, primary and secondary DNS, and NBNS addresses). This is a common configuration to support remote access over VPN (see Figure 2). In this configuration, the device is configured to initiate and respond in main mode.

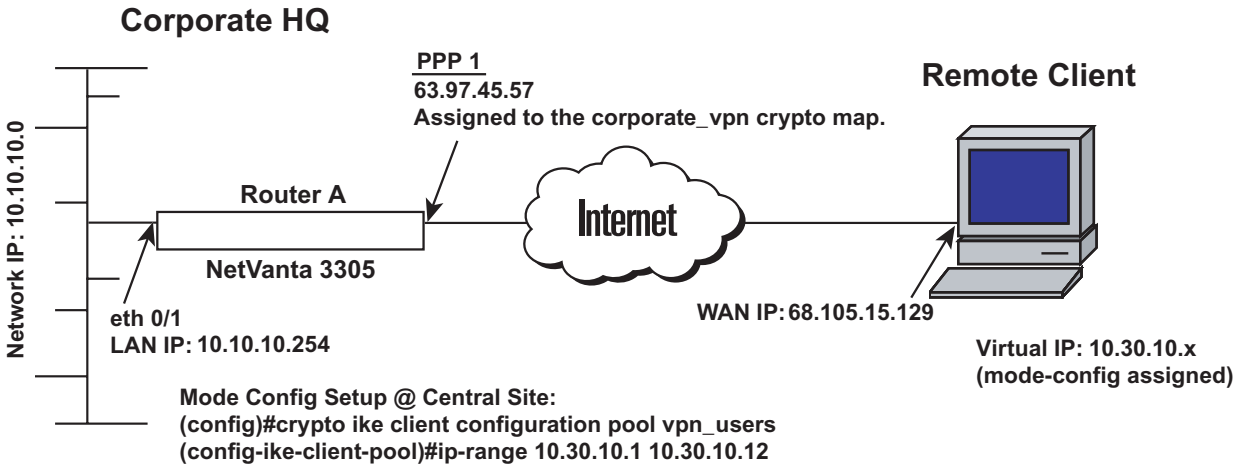


Figure 2. Remote Access VPN

Table 2. Step-by-Step Configuration: Adding Mode Config Support

Step	Action	Command
1	Enter Enable Security mode.	>**enable**
2	Enter Global Configuration mode.	**#configure terminal**
3	Enable VPN functionality.	(config)**#ip crypto**
4	Set the local ID during IKE negotiation to be the IP address of the interface from which the traffic exits.	(config)**#crypto ike local-id address**
	*Note: You can override this setting on a per-policy basis by using the **local-id** command in the IKE Policy command set.*	
5	Create a client configuration pool (**vpn_users**) and enter its command set.	(config)**#crypto ike client configuration pool vpn_users**
6	Specify the range of addresses from which the router draws when assigning an IP address to a client.	(config-ike-client-pool)**#ip-range 10.30.10.1 10.30.10.12**
	Note: Define the range by entering the first IP address in the range for this pool, followed by the last IP address in the range for this pool.	
7	Specify the primary and secondary DNS server addresses to assign to a client.	(config-ike-client-pool)**#dns-server 10.30.10.250 10.30.10.251**
8	Specify the primary and secondary NetBIOS Windows Internet Naming Service (WINS) name servers to assign to a client.	(config-ike-client-pool)**#netbios-name-server 10.30.10.253 10.30.10.254**
9	Exit to Global Configuration mode.	(config-ike-client-pool)**#exit**
10	Create an IKE policy with a priority of 10 and enter the IKE Policy command set.	(config)**#crypto ike policy 10**
11	Configure this policy to accept the global local ID setting (as described previously in step 4).	(config-ike)**#no local-id**
12	Enter the IP address of the peer device. This policy can now initiate or respond to the peer.	(config-ike)**#peer 68.105.15.129**
	Note: Repeat this command for multiple peers, if necessary.	
13	Specify to initiate negotiations using aggressive mode.	(config-ike)**#initiate main**
	Note: Aggressive mode can be used when one end of the VPN tunnel has a dynamically-assigned address. The side with the dynamic address must be the initiator of the traffic and tunnel. The side with the static address must be the responder. Please note that in some situations, using aggressive mode with pre-shared keys can compromise network security.	
14	Allow the IKE policy to respond to IKE negotiations from peers using main mode.	(config-ike)**#respond main**

Table 2. Step-by-Step Configuration: Adding Mode Config Support *(Continued)*

Step	Action	Command
15	Set the client configuration pool for this IKE policy to **vpn_users**.	(config-ike)**#client configuration pool vpn_users**
16	Enter the IKE Policy Attribute command mode, assigning this attribute a priority of 10.	(config-ike)**#attribute 10**
	Note: Multiple attributes can be created for a single IKE policy. The attribute's priority number specifies the order in which the resulting VPN proposals get sent to the far-end.	
17	Choose the 3DES encryption algorithm for this IKE policy to use to transmit data over the IKE-generated SA.	(config-ike-attribute)**#encryption 3des**
18	Specify the hash SHA algorithm to be used to authenticate the data transmitted over the IKE SA.	(config-ike-attribute)**#hash sha**
19	Configure this IKE policy to use pre-shared secrets during IKE negotiation to validate the peer.	(config-ike-attribute)**#authentication pre-share**
20	Specify Diffie-Hellman Group 1 to be used by this IKE policy to generate the keys (which are then used to create the IPSec SA).	(config-ike-attribute)**#group 1**
21	Specify that the IKE SA is valid for 24 hours (i.e., 86400 seconds).	(config-ike-attribute)**#lifetime 86400**
22	Exit to Global Configuration mode.	(config-ike-attribute)**#exit**
23	Specify the remote ID and associate it with a pre-shared key (**mysecret123**).	(config)**#crypto ike remote-id address 68.105.15.129 preshared-key mysecret123**
24	Create a transform set (**highly_secure**) consisting of two security algorithms (up to three algorithms may be defined).	(config)**#crypto ipsec transform-set highly_secure esp-3des esp-sha-hmac**
25	Place this transform set in tunnel mode (used almost exclusively in VPN configurations involving multiple subnets).	(cfg-crypto-trans)**#mode tunnel**
26	Create an empty access list and enter the extended access list command set.	(cfg-crypto-trans)**#ip access-list extended corporate_traffic**
	Note: The following message is displayed once you enter this command: **Configuring New Extended ACL "corporate_traffic"**.	
27	Specify the traffic to be sent through the VPN tunnel (see note, below).	(config-ext-nacl)**#permit ip 10.10.10.0 0.0.0.255 any log**
	Note: In this example, traffic with a source IP of our LAN network (10.10.10.0) and a destination IP of any private network is allowed.	
28	Specify that all *other* traffic (not permitted in the previous step) is denied.	(config-ext-nacl)**#deny ip any any**

Table 2. Step-by-Step Configuration: Adding Mode Config Support *(Continued)*

Step	Action	Command
29	Create an IPSec crypto map (**corporate_vpn**) to define the IPSec tunnel. Assign a map index of 1.	(config-ext-nacl)**#crypto map corporate_vpn 1 ipsec-ike**
	Note: *The map index number allows the AOS device to rank crypto maps. When multiple maps are defined, this number determines the order in which they are considered. Maps with the lowest number are evaluated first.*	
30	Assign the access list **corporate_traffic** to this crypto map.	(config-crypto-map)**#match address corporate_traffic**
31	Set the IP address of the peer device.	(config-crypto-map)**#set peer 68.105.15.129**
32	Assign the transform set **highly_secure** to this crypto map.	(config-crypto-map)**#set transform-set highly_secure**
33	Define the lifetime (in seconds) for the IPSec SAs created by this crypto map.	(config-crypto-map)**#set security-association lifetime seconds 28800**
34	Configure the unit to not use PFS (perfect forward secrecy) when creating new IPSec SAs.	(config-crypto-map)**#no set pfs**
35	Access configuration parameters for the PPP interface.	(config-crypto-map)**#interface ppp 1**
36	Assign an IP address and subnet mask to the WAN interface.	(config-ppp 1)**#ip address 63.97.45.57 255.255.255.248**
37	Apply the crypto map **corporate_vpn** to the WAN interface.	(config-ppp 1)**#crypto map corporate_vpn**
38	Activate the WAN interface.	(config-ppp 1)**#no shutdown**
39	Access configuration parameters for the Ethernet port.	(config-ppp 1)**#interface ethernet 0/1**
40	Assign an IP address and subnet mask to the Ethernet port.	(config-eth 0/1)**#ip address 10.10.10.254 255.255.255.0**
41	Activate the Ethernet port.	(config-eth 0/1)**#no shutdown**
42	Exit to Global Configuration mode.	(config-eth 0/1)**#exit**

Sample Script

```
! Enter the Configure Terminal Mode
enable
configure terminal

! Turn on VPN Support
ip crypto

! By default, the local-id of the device will be the IPv4 address
! of the interface over which the IKE negotiation is occurring
crypto ike local-id address
```



```
! Create a Client Configuration Pool with a name of vpn_users
! Address Range:  10.30.10.1 10.30.10.12
! DNS Primary Address: 10.30.10.250
! DNS Secondary Address: 10.30.10.251
! NBNS Primary Address: 10.30.10.253
! NBNS Secondary Address: 10.30.10.254
crypto ike client configuration pool vpn_users
  ip-range 10.30.10.1 10.30.10.12
  dns-server 10.30.10.250 10.30.10.251
  netbios-name-server 10.30.10.253 10.30.10.254

! Create an IKE policy with priority of 10
! Mode: main
! Local-id: Do NOT override the system local-id policy
! Peer: 68.105.15.129
! Can Initiate or Respond to IKE negotiation
! Set the client configuration pool to vpn_users
! One attribute configured - Number: 10
!   Encryption Algorithm: 3DES
!   Hash Algorithm:  SHA1
!   Authentication Type:  Pre-shared Keys
!   Group:  Diffie-Hellman Group 1
!   IKE SA Lifetime:  86400 seconds
crypto ike policy 10
  no local-id
  peer 68.105.15.129
  initiate main
  respond main
  client configuration pool vpn_users
  attribute 10
    encryption 3des
    hash sha
    authentication pre-share
    group 1
    lifetime 86400

! Define the remote-id and pre-shared key for peer 68.105.15.129
crypto ike remote-id address 68.105.15.129 preshared-key mysecret123

! Define the transform-set to be used to secure data transmitted
! and received over the IPSec tunnel
crypto ipsec transform-set highly_secure esp-3des esp-sha-hmac
mode tunnel
```



```
! Specify the traffic to be sent over the VPN tunnel.
! With respect to this unit, that traffic would be anything with
! a source IP of our LAN network (10.10.10.0) and a destination
! IP of the Peer Private network (10.10.20.0).
! All other traffic will not be allowed over the tunnel.
ip access-list extended corporate_traffic
  permit ip 10.10.10.0 0.0.0.255 any log
  deny ip any any

! Create an IPSec Crypto Map to define the IPSec tunnel
! Crypto Map Name:  corporate_vpn
! Crypto Map Index: 1
! Select VPN tunnel traffic using named ACL "corporate_traffic"
! Peer: 68.105.15.129
! Use the encryption and authentication transform-set as specified
!  in "highly_secure"
! IPSec Lifetime: 8000 Kbytes or 28800 seconds, whichever comes first
! Do not use Perfect Forward Secrecy when creating new IPSec SAs
crypto map corporate_vpn 1 ipsec-ike
  match address corporate_traffic
  set peer 68.105.15.129
  set transform-set highly_secure
  set security-association lifetime seconds 28800
  no set pfs

! Configure the public interface (ppp 1)
! Apply the specified crypto map to our public interface,
interface ppp 1
  ip address 63.97.45.57 255.255.255.248
  crypto map corporate_vpn
  no shutdown

! Configure the private interface (ethernet 0/1)
interface ethernet 0/1
  ip address 10.10.10.254 255.255.255.0
  no shutdown
```


Verifying Your Configuration Using Show Commands

Use the following AOS **show** commands to display information regarding your configuration. Enter **show** commands at any prompt using the **do** command.

For example:
(config-eth 0/1)#**do show access-lists**

Table 3. Show Commands

Command	Description	Sample Output
show access-lists	Displays all configured access lists in the system (or a specific list).	**#show access-lists** Standard access list MatchAll permit host 10.3.50.6 (0 matches) permit 10.200.5.0 wildcard bits 0.0.0.255 (0 matches) Extended access list UnTrusted deny icmp 10.5.60.0 wildcard bits 0.0.0.255 any source-quench (0 matches) deny tcp any any (0 matches)
show crypto ike	Displays information regarding the IKE configuration. Variations of this command include the following: **show crypto ike client configuration pool** **show crypto ike client configuration pool** <*poolname*> **show crypto ike policy** **show crypto ike policy** <*policy priority*> **show crypto ike remote-id** <*remote-id*> **show crypto ike sa**	**#show crypto ike policy** Crypto IKE Policy 100 Main mode Using System Local ID Address Peers: 63.105.15.129 initiate main respond anymode Attributes:10 Encryption: 3DES Hash: SHA Authentication: Pre-share Group: 1 Lifetime: 900 seconds
show crypto ipsec	Displays information regarding the IPSec configuration. Variations of this command include the following: **show crypto ipsec sa** **show crypto ipsec sa address** <*ip address*> **show crypto ipsec sa map** <*mapname*> **show crypto ipsec transform-set** **show crypto ipsec transform-set** <*setname*>	**#show crypto ipsec transform-set** Transform Set "MySet" ah-md5-hmac mode tunnel Transform Set "Set1" esp-3des esp-sha-hmac mode tunnel Transform Set "esp-des" esp-des mode tunnel

Table 3. Show Commands *(Continued)*

Command	Description	Sample Output
show crypto map	Displays information regarding crypto map settings. Variations of this command include the following: **show crypto map** **show crypto map interface ethernet** <#/#> **show crypto map interface frame-relay** <#> **show crypto map interface loopback** <#> **show crypto map interface ppp** <#> **show crypto map** <*map name*> **show crypto map** <*map name*> <*map #*>	**#show crypto map testMap** Crypto Map "testMap" 10 ipsec-ike Extended IP access list NewList Peers:63.97.45.57 Transform sets:esp-des Security-association lifetimes: 0 kilobytes 86400 seconds No PFS group configured Interfaces using crypto map testMap: eth 0/1

