



Solution of IPSec VPN-Xauth

Hillstone Networks Inc.



Submitter	Auditor		Version	Date
Tianjiao Chen	Junli Li		V1	2015-08-20

Content

1. Background.....	3
2. Demand Analysis	3
3. Solution	3
4. Implementation	4
Topology	4
Configuration.....	4
FW configuration	4
Windows Client Settings (Win7 x64 Compatible with Win10)	6
OSX Client Settings (Yosemite)	10
5. Noticing	12
Xauth Server Side	12
6. Performance	13

1. Background

Currently, remote office becomes more and more popular, people can use VPN to connect with the internal network of office. The point of remote office is the authorization of the people because they could be anywhere of the internet. However, IKE protocol did not provide a one-way authentication method for remote connection, so X-auth has been used to proceed the one-way authentication for the user with IKE.

Xauth was the draft RFC that raised in the basic of IKE protocol by IETF, the latest version is draft-ietf-ipsec-isakmp-xauth-06.txt. XAUTH is the enhancement of the existed IKE protocol, but would not instead on the existing IKE authentication method.

Because the combination of XAUTH and RADIUS brings the unprecedented security and convenience for those business user who relied on using VPN technology, so lots of international famous VPN device manuafactory, such as Cisco, Juniper and Netgear etc, their product aslo are starting to support XAUTH..

2. Demand Analysis

Need to perform mobile officing to access company internal network, include mobile phone and PC. However, the traditional IPSec VPN only support the way of site to site.

For mobile officing, now we have three solutions : SCVPN、L2TP (over IPSec)、Xauth.

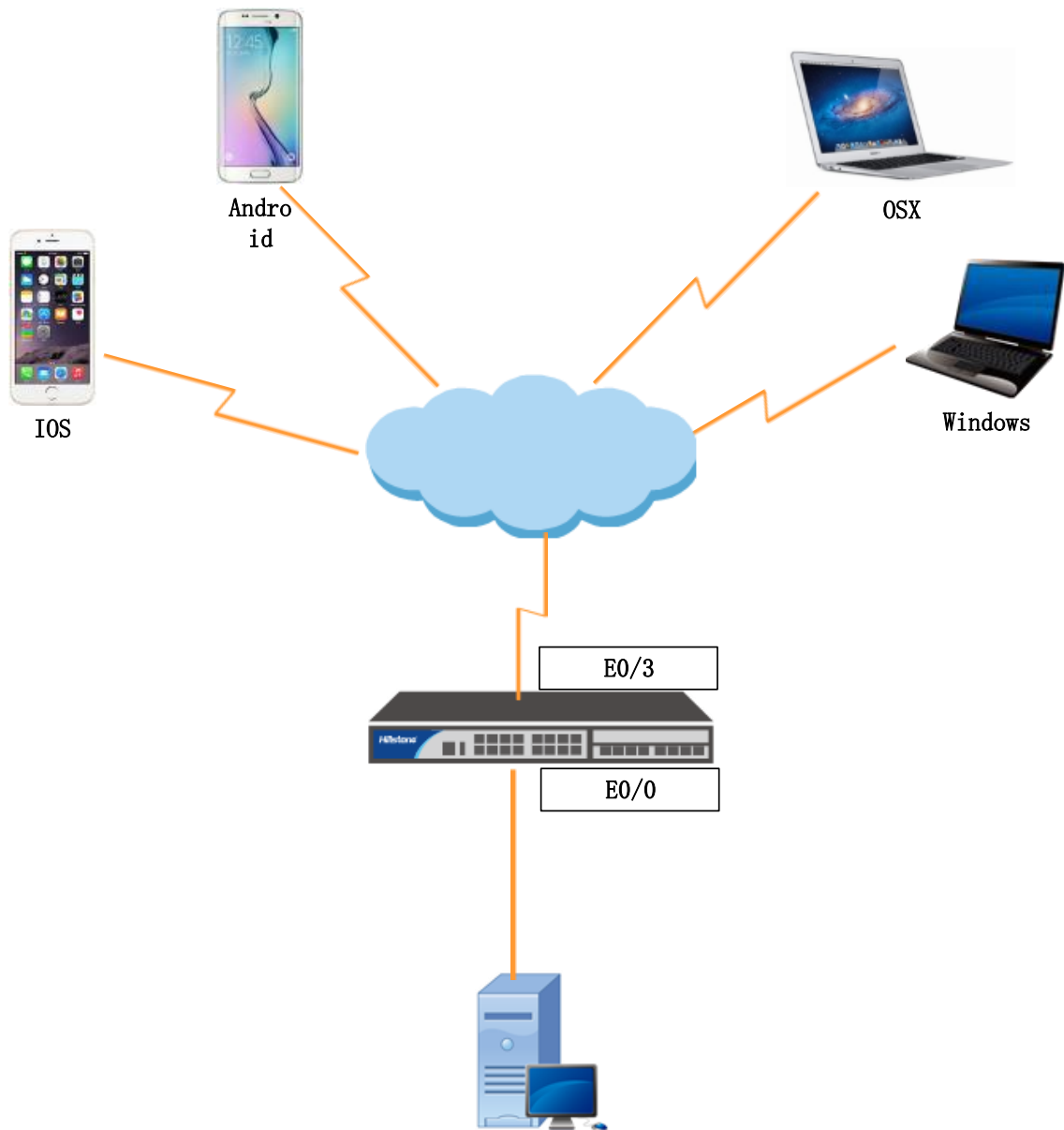
Currently, Hillstone' s SCVPN does not support IOS and OSX, IOS and OSX does not support L2TP but must use L2TP over IPSec , and the configuration of L2TP over IPSec is pretty complicated, the configuration of Windows system side is relating the system, so the XAUTH, SCVPN and L2TP would complement each other' s advantages.

3. Solution

Configure Xauth in Hillstone device and then publish to internet which would make the mainstream mobile client pass the authentication of internal network access.

4. Implementation

Topology



Configuration

FW configuration

Hardware Platform : SG-6000-E1100

Verified Firmware : SG6000-M-3-5.0R4P8.bin

Configuration :

A . Configuration of Interface:

```
interface ethernet0/3
  zone "untrust"
  ip address 200.1.1.1 255.255.255.0
  manage ping
  manage http
exit
interface ethernet0/0
  zone "trust"
  ip address 192.168.1.1 255.255.255.0
exit
interface tunnel1
  zone "trust"
  ip address 10.1.1.1 255.255.255.0
  manage ping
  tunnel ipsec "xauth"
exit
```

B . Configuration of Xauth VPN:

```
aaa-server "local" type local
  user "xauth"
  password "OVs+Vb+6lwCIfp3BF1pvil+V5qEh"
  ike-id key-id "hillstone"
exit
xauth pool "xauth-pool"
  address 10.1.1.2 10.1.1.254 netmask 255.255.255.0
  dns 10.86.249.11 10.88.7.10
exit
isakmp peer "xauth"
  mode aggressive
  type usergroup
  isakmp-proposal "psk-sha-aes128-g2"
  pre-share "9fCQ5GEqdmw6iBwm2x+9tmSbt3wB6Q"
  aaa-server "local"
  local-id key-id "hillstone"
  nat-traversal
  xauth pool-name "xauth-pool"
  xauth server
  interface ethernet0/3
exit
tunnel ipsec "xauth" auto
```

```
isakmp-peer "xauth"  
ipsec-proposal "esp-sha-aes128-g0"  
track-event-notify enable  
accept-all-proxy-id  
exit
```

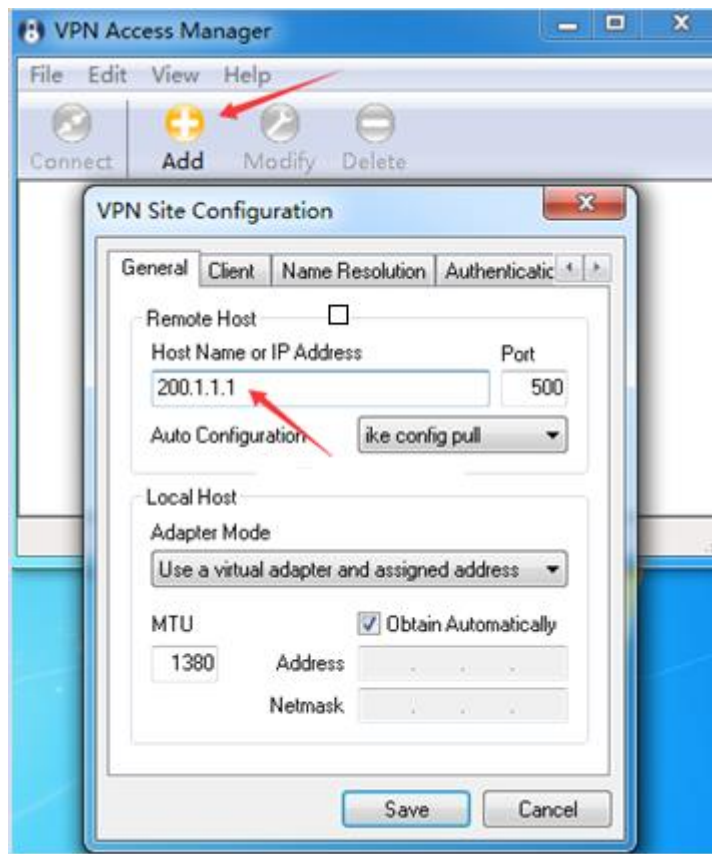
C . Others:

```
ip vrouter "trust-vr"  
  snatrule id 1 from "Any" to "Any" service "Any" eif ethernet0/3 trans-to eif-ip  
mode dynamicport  
  ip route 0.0.0.0/0 200.1.1.2  
exit  
rule id 1  
  action permit  
  src-addr "Any"  
  dst-addr "Any"  
  service "Any"  
exit
```

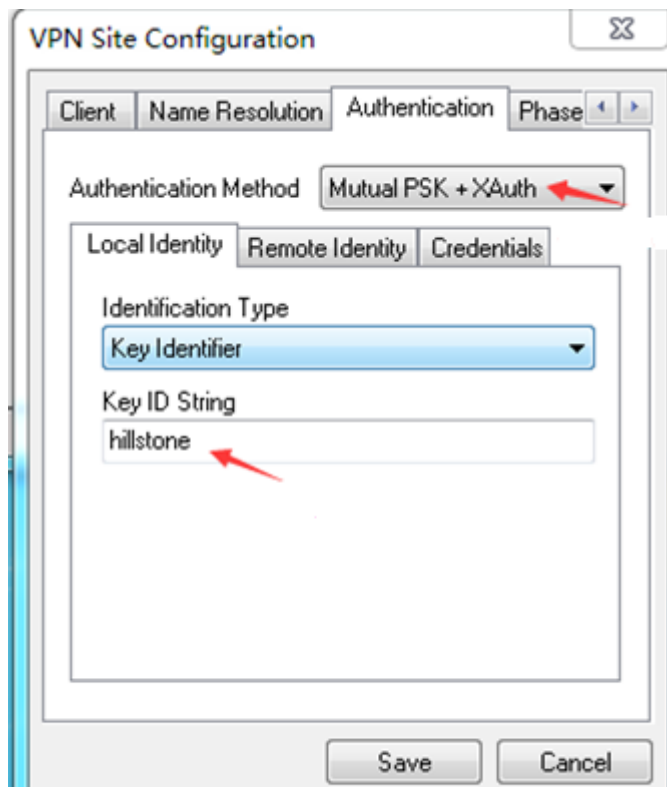
Windows Client Settings (Win7 x64 Compatible with Win10)

Cisco client compatibility is not very good, so we used a "Shrew Soft" VPN client.

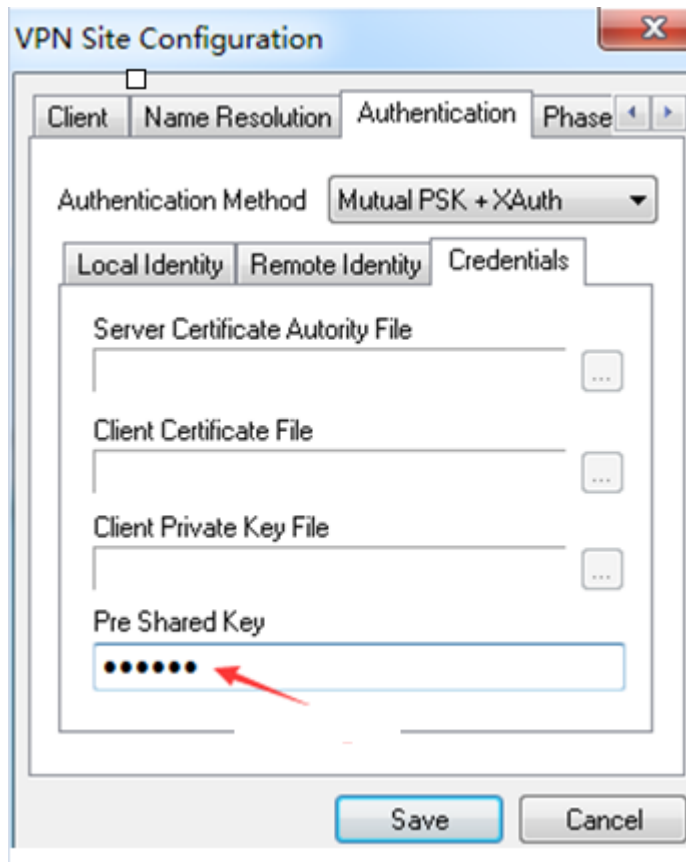
A. Create New, fill up with server IP of Xauth



B. Select Identification type, fill up with user key-id

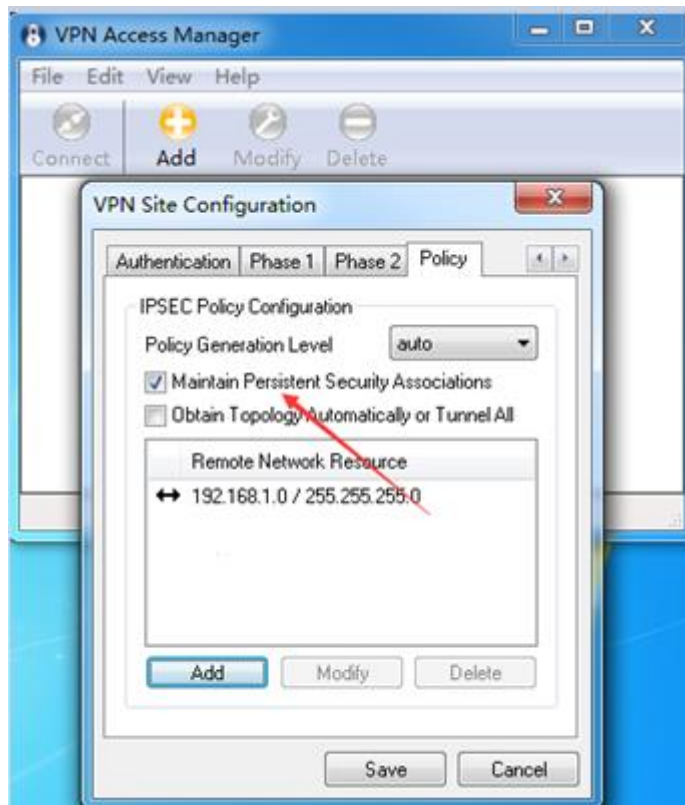


C. Fill up Pre-Shared Key

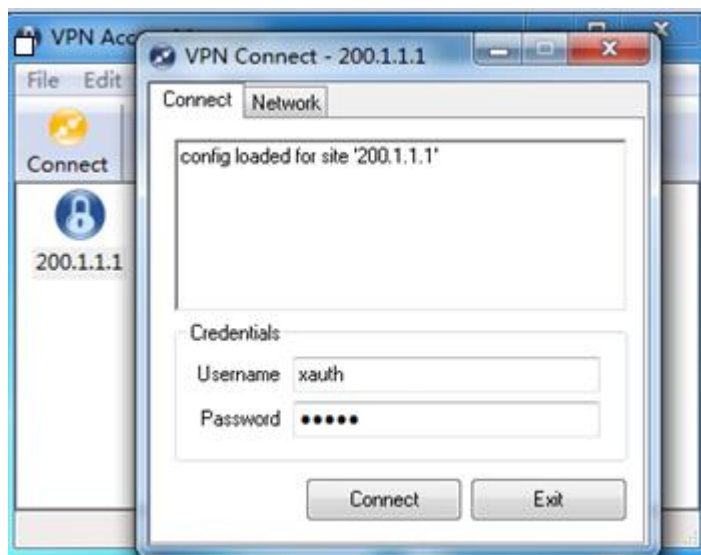


The image shows a 'VPN Site Configuration' dialog box with a blue title bar and a close button (X). It has four tabs: 'Client', 'Name Resolution', 'Authentication', and 'Phase'. The 'Authentication' tab is selected. Inside this tab, there is a dropdown menu for 'Authentication Method' set to 'Mutual PSK + XAuth'. Below this are three sub-tabs: 'Local Identity', 'Remote Identity', and 'Credentials'. The 'Credentials' sub-tab is active. It contains four fields: 'Server Certificate Authority File', 'Client Certificate File', 'Client Private Key File', and 'Pre Shared Key'. Each of the first three fields has a text input area and a browse button (three dots). The 'Pre Shared Key' field has a text input area with a red arrow pointing to it. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

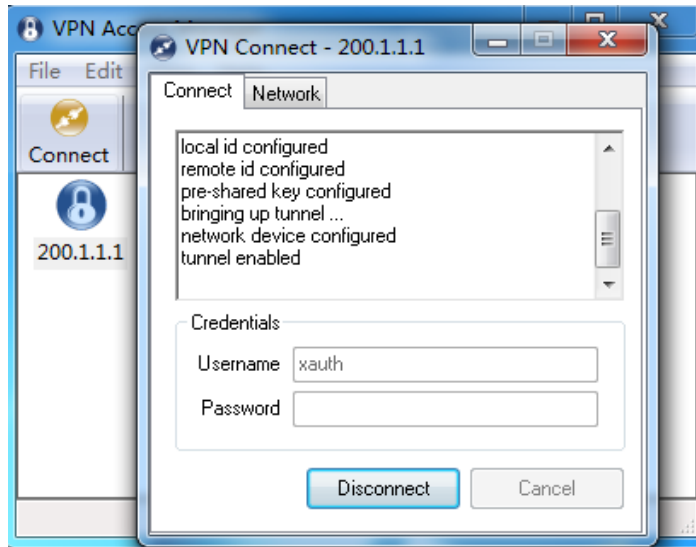
D. Add tunnel route, select "Obtain Topology Automatically or Tunnel All" as the default route.



E. Using username and password to dial in



F. Connected Successfully

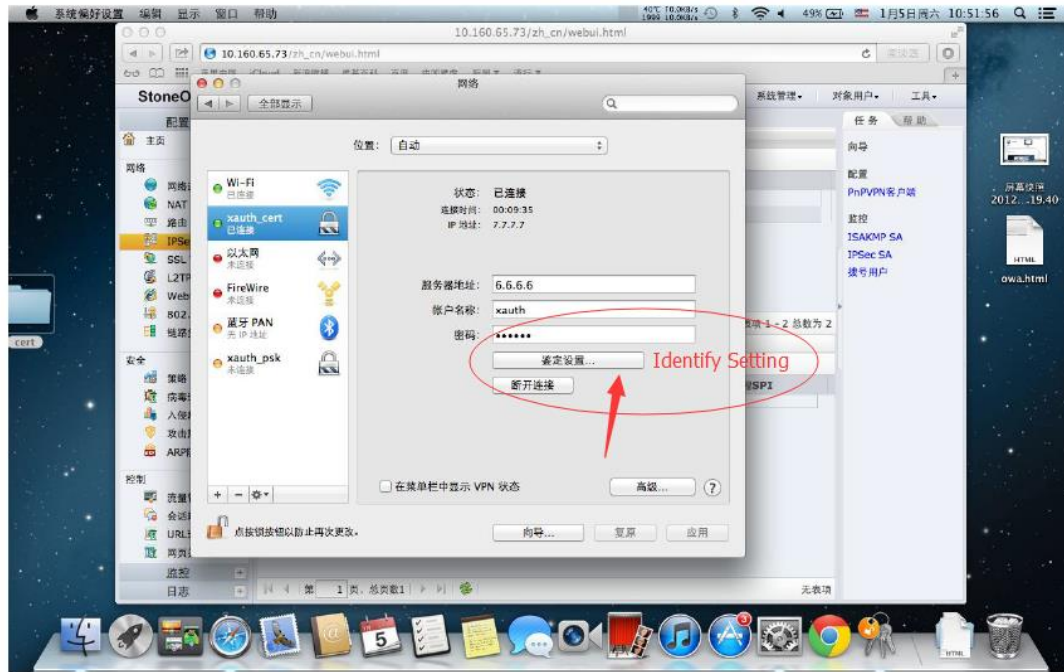


OSX Client Settings (Yosemite)

1. Configure the X-auth client of pre-share key certification, Mac OS has it already.
- 1) Make sure the network connections is available, please select "xauth_psk", not "xauth_cert", build new VPN configuration, and fill up with server address, distributed account user and password respectively.

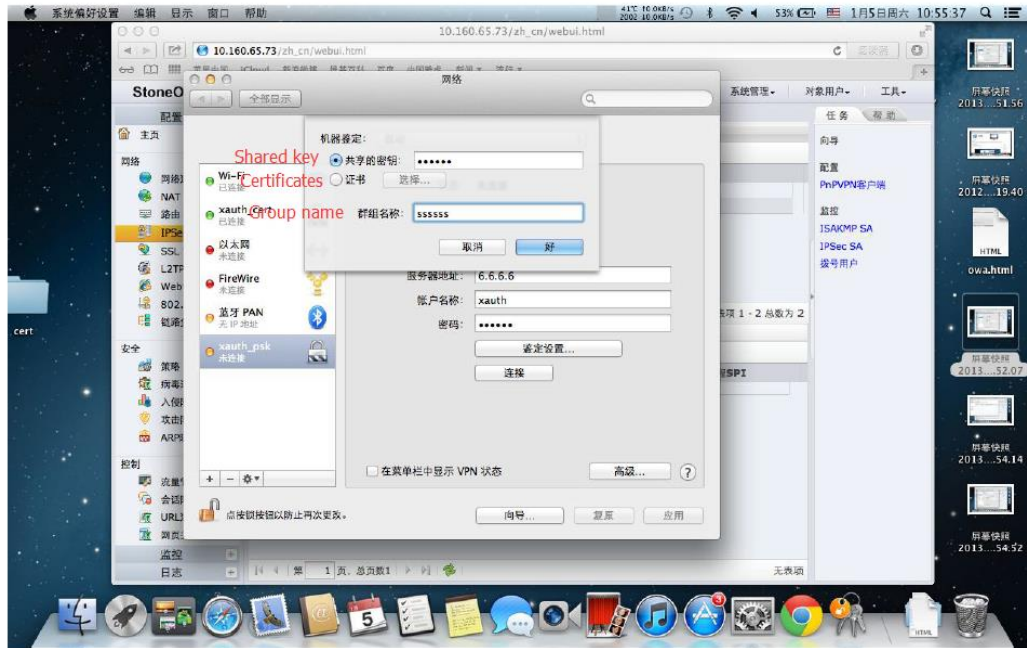


Please click "Identify Setting",



Please click "Identify Setting", select the "shared key", and fill up with share key and group name etc.





5. Noticing

Xauth Server Side

- A. Currently only support Radius and Local authentication, does not support ldap and active-directory.
- B. Xauth only support following mode : Aggressive mode+ Shared Key, Main mode+ Certification type, this case is shared key.
- C. Only need one user configure with the correct ike-id, then the other users does not need to configure again.
- D. On the second step of configuration, need to configure IPsec accept-all-proxy-id.
- E. When configuring radius server , need to add the name of "ikeid" in radius server, the password is: 123456 , for example, if the ikeid is "Hillstone" , then we need to add

new user "Hillstone" in radius server, and password is :123456.

- F. When xauth uses Radius for authentication, need to create two users, one is for real authentication user and another one is for group authentication.

6. Performance

Finally performed the mainstream mobile client access from external network, and open part of internal network resource by setting policy in the FW, which achieved the requirement of mobile officing..