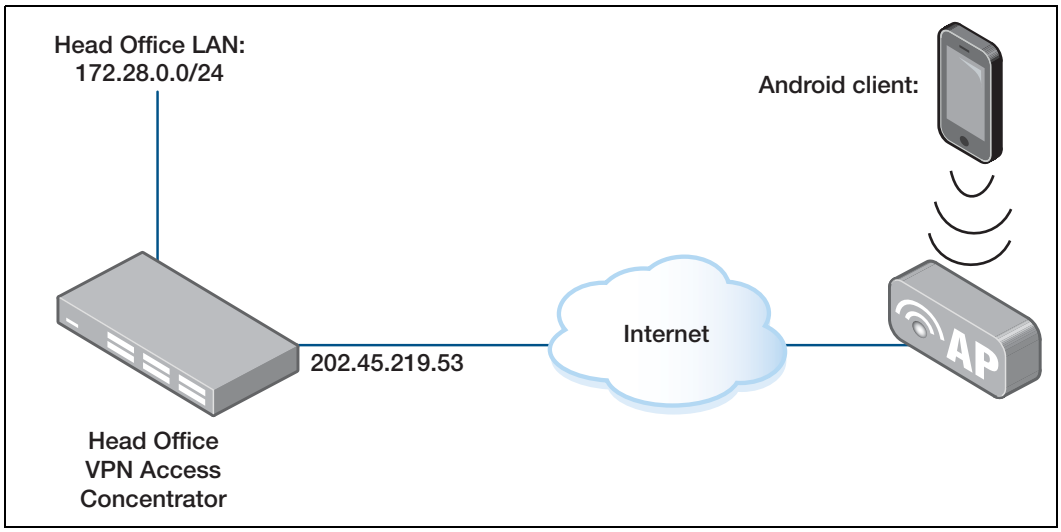
Network diagram

The Android client connects to the Internet wirelessly, and the head office has a wired connection to the Internet.



Configure the head office router

Initial security setup

Before adding the ISAKMP and IPsec configuration, set up the router with the following important details.

1. Create two keys to use for Secure Shell (SSH).

Use the commands:

```
create enco key=1 description="Server Key" type=rsa length=768 format=ssh
create enco key=2 description="Host Key" type=rsa length=1024 format=ssh
```

After each of these commands, the router displays the following information:

```
Info (1073278): RSA Key Generation process started.  Manager >
Info (1073279): RSA Key generation process completed.
```

2. Create a third key for ISAKMP to use as a preshared key.

For security reasons, do not use the same value as this example. Use the command:

```
create enco key=3 description="ISAKMP PSK" type=general value=secret
```

We use this encryption key on the Android client (see step 2 page 9).

3. Check the key configuration.

Use the command: `show enco key`

This results in the following output:

```
ID  Type       Length Digest    Description    Mod    IP
-------------------------------------------------------------------
1   RSA-PRIVATE   768 A40EB1F4  Server Key      -      -
2   RSA-PRIVATE  1024 2BB712B4  Host Key        -      -
3   GENERAL         6 EE635A9D  ISAKMP PSK      -      -
```

4. Check feature licences.

Check that you have a 3DES feature licence for the ISAKMP policy. Use the command:

```
show feature
```

You can purchase feature licences from your Allied Telesis distributor. If necessary, install the licence, using the password provided by your distributor.

```
enable feature=3des pass=<licence-number>
```

5. Add a security officer.

This step is important because a security officer must exist before you enable system security (which you do in the next step).

```
add user=secoff pass=<password> priv=securityOfficer telnet=yes
   login=yes
```

After this command, the router displays the following information.

```
Number of Radius-backup users.0

User Authentication Database
-------------------------------------------------------------------
Username: secoff ()
 Status:  enabled  Privilege: Sec Off Telnet: yes Login: yes RBU:no
Logins: 0          Fails:       0    Sent: 0         Rcvd: 0
Authentications: 0 Fails: 0
-------------------------------------------------------------------
```

6. Enable system security.

Enable system security so that the newly created keys will be stored permanently. They would otherwise be deleted if the router restarted.

```
enable system security
```

Once security mode is enabled, you need to log in as the security officer to enter most configuration-altering commands.

7. **Save the configuration and set the router to use it as startup.**

Use the command: `create config=vpn.cfg set`

Configuration template

This section contains a configuration script for the head office. You can copy and paste the script to an editor on your PC, modify addresses, passwords, and any other requirements for all your individual sites, and then use TFTP, HTTP, or ZMODEM to transfer the files to your routers.

- For more information about loading files onto the router, please refer to the **Managing Configuration Files and Software Versions** chapter in the Software Reference
- For detailed explanations about the CLI configuration, see the How To Note:
  - *How To Configure VPNs In A Corporate Network, With Optional Prioritisation Of VoIP*
  - To view this document, go to: http://www.alliedtelesis.com/support/documentation

Take particular note of the configuration of the PPP template below. The specific point to note is the setting of the **vjc** parameter. The setting **vjc=on** means that the resulting PPP link to the Android device will negotiate to a state where Van Jacobson compression is enabled on both ends of the PPP. This is required when connecting to Android devices, as they are not able to create reliable TCP connections over a PPP link where the PPP peer does not have Van Jacobson compression enabled.

PPP template configuration

```
set system name="Head Office"

#  User configuration
add user=secoff pass=<your-secoff-password> priv=securityOfficer lo=yes  set
user=secoff telnet=yes netmask=255.255.255.255
add user=remoteuser_user pass=<user-password> lo=no

#  PPP templates configuration  create ppp template=1
set ppp template=1 bap=off ippool="myippool" authentication=chap
mssheader=120 echo=30 vjc=on

#  L2TP configuration enable l2tp
enable l2tp server=both
add l2tp ip=1.1.1.1-255.255.255.254 ppptemplate=1

#  VLAN general configuration  create vlan="vlan100" vid=100

#  VLAN port configuration add vlan="100" port=1-5

#  IP configuration enable ip
add ip int=eth0 ip=202.45.219.53
add ip int=vlan100 ip=172.28.0.254 mask=255.255.255.0  add ip rou=0.0.0.0
mask=0.0.0.0 int=eth0 next=202.45.219.1
create ip pool="myippool" ip=192.168.66.66-192.168.66.77  add ip dns
prim=179.23.83.192 seco=202.49.72.50

#  Firewall configuration enable firewall
enable firewall notify=mail to=<administrator-email-address>  create
```

```
firewall policy="fw"
create firewall policy="fw" dy=dynamic
add firewall policy="fw" dy=dynamic us=ANY  enable firewall policy="fw"
icmp_f=all
add firewall policy="fw" int=vlan100 type=private
add firewall policy="fw" int=dyn-dynamic type=private  add firewall
policy="fw" int=eth0 type=public

#  NAT for local users
add firewall poli="fw" nat=enhanced int=vlan100 gblin=eth0

#  NAT for the IPSec users
add firewall poli="fw" nat=enhanced int=dyn-dynamic gblin=eth0

#  Permit incoming SSH
add firewall poli="fw" ru=1 ac=allo int=eth0 prot=tcp po=22 ip=202.45.219.53
gblip=202.45.219.53 gblp=22

#  Permit incoming ISAKMP
add firewall poli="fw" ru=2 ac=allo int=eth0 prot=udp po=500
ip=202.45.219.53  gblip=202.45.219.53 gblp=500

#  Permit ESP over UDP (for IPSec NAT-T)
add firewall poli="fw" ru=3 ac=allo int=eth0 prot=udp po=4500
ip=202.45.219.53  gblip=202.45.219.53 gblp=4500

#  Permit L2TP specifically over IPSec
add firewall poli="fw" ru=4 ac=allo int=eth0 prot=udp po=1701
ip=202.45.219.53  gblip=202.45.219.53 gblp=1701 encap=ipsec

#  Do not apply NAT on incoming traffic destined for private LAN addresses if
that traffic has come in encapsulated in IPSEC
add firewall poli="fw" ru=5 ac=non int=eth0 prot=ALL ip=172.28.0.1-
172.28.0.254 enc=ips

#  SSH configuration
enable ssh server serverkey=1 hostkey=2 expirytime=0 logintimeout=60  add
ssh user=secoff password=secoff

#  IPSEC configuration
create ipsec sas=1 key=isakmp prot=esp enc=3desouter hasha=sha  set ipsec
sas=1 mod=transport
create ipsec sas=2 key=isakmp prot=esp enc=3desouter hasha=md5  set ipsec
sas=2 mod=transport
create ipsec sas=3 key=isakmp prot=esp enc=des hasha=sha  set ipsec sas=3
mod=transport
create ipsec sas=4 key=isakmp prot=esp enc=des hasha=md5  set ipsec sas=4
mod=transport
create ipsec bund=1 key=isakmp string="1 or 2 or 3 or 4"

#  ISAKMP and NAT-T encapsulated data are permitted in/out, without being
processed by IPsec
create ipsec pol="isakmp" int=eth0 ac=permit lp=500 rp=500  create ipsec
pol="natt_udp" int=eth0 ac=permit lp=4500

#  The Android client will match the following policy
create ipsec pol="android_warriors" int=eth0 ac=ipsec key=isakmp bund=1
peer=ANY isa="android_isakmp" lp=1701 tra=UDP

#  All other traffic is defined here.
create ipsec pol="internet" int=eth0 ac=permit  enable ipsec

#  ISAKMP configuration
create isakmp pol="android_isakmp" pe=any enc=3desouter key=3 natt=true
gro=2  enable isakmp
```

Configure an Android client

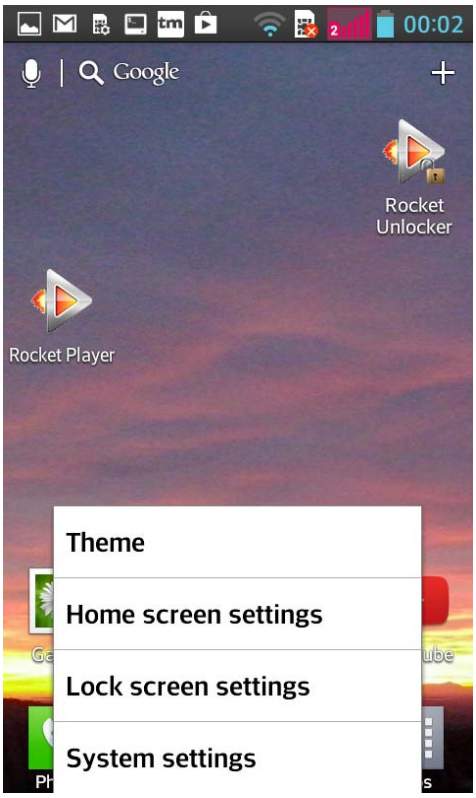
This section describes how to set up a VPN on the Android device.

Note: This configuration uses the native Android VPN client. No special apps need to be installed on the Android device to enable this VPN connection to operate.

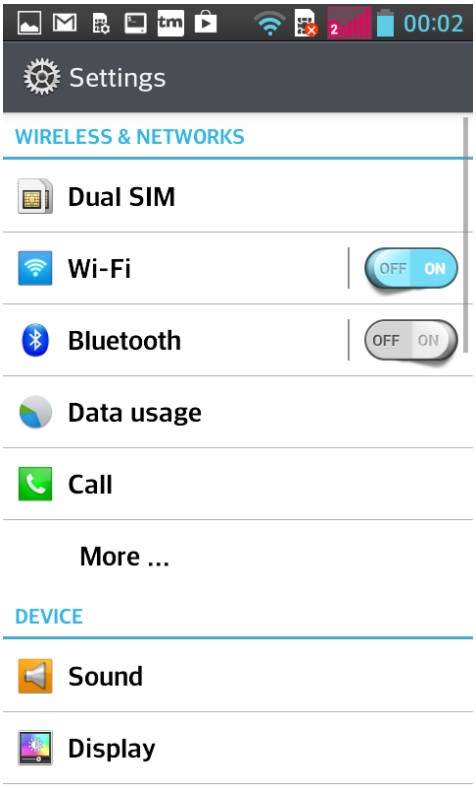
Create the connection

1. Open the VPN configuration screen.

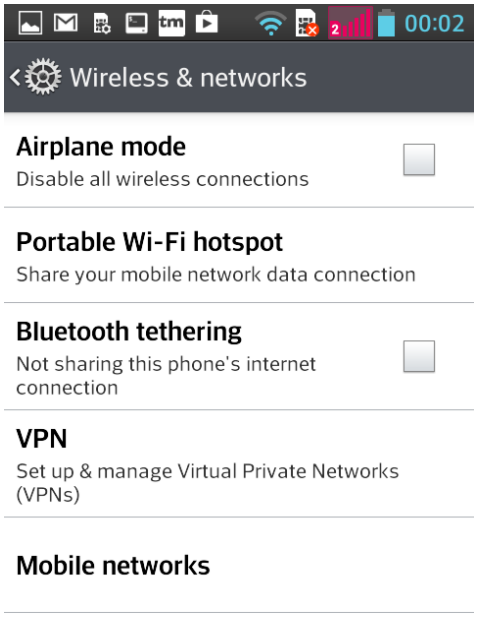
On the Home Screen, bring up the screen menu.



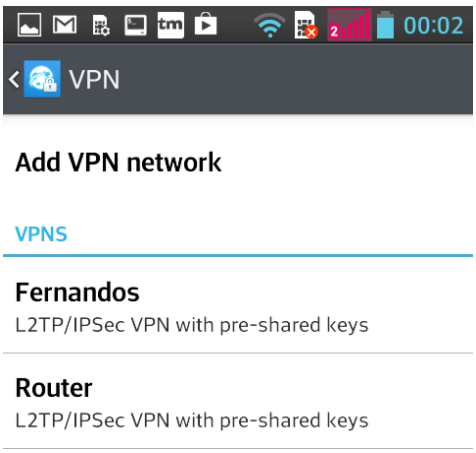
In this menu, tap the item System Settings to open the Settings app.



Tap the item More… to bring up advanced Wireless & networks settings options.



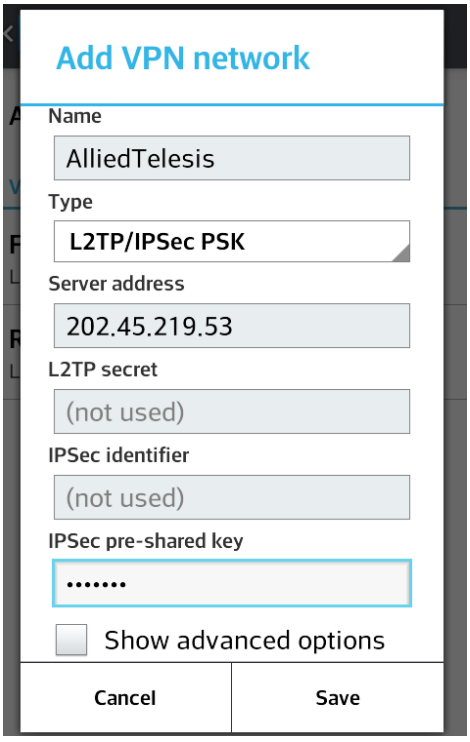
Tap VPN to bring up the VPN management screen.



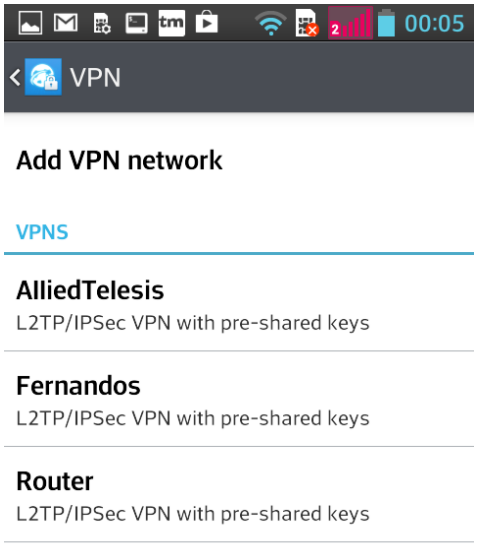
2. Set up a new connection.

- Tap Add VPN network to open up an Add VPN network dialog box.
- Fill out the dialog box as shown below.
- The Name field can contain any name you want.
- The Type must be L2TP/IPSec PSK.
- The Server Address is the public-side address of the AR router.

The IPSEC pre-shared key must be identical to the value specified in the "create enco key=3" command on the AR router, see "Initial security setup" on page 3



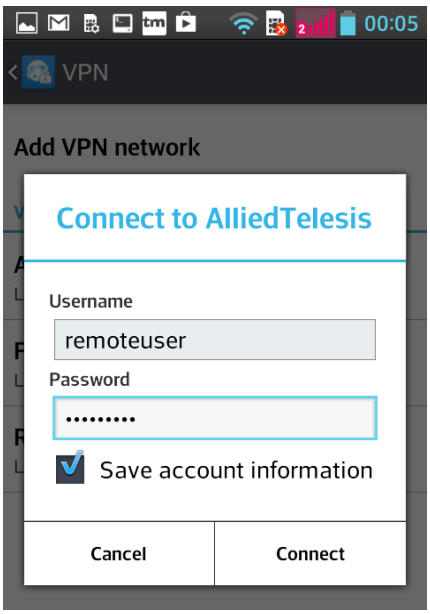
Tap **Save**, and the new VPN network is created and added to the list of networks in the Android device.

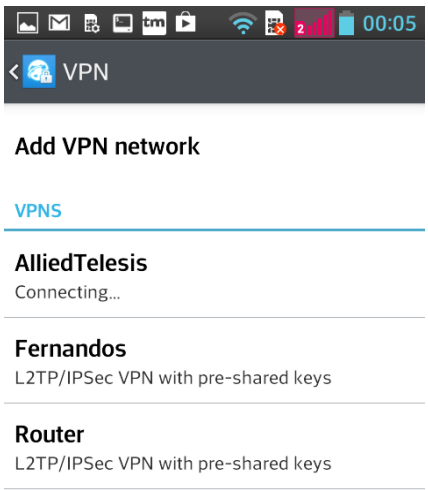


Connect

1. Start the VPN.

On the VPN screen, tap the **Allied Telesis** network. A Connect dialog box will pop up. Into the Username and Password fields, enter the Username and Password configured on the AR router for authenticating the user connecting over the VPN.





Tap **Connect**, and the VPN network will start connecting.

C613-16180-00 REV A

North America Headquarters | 19800 North Creek Parkway | Suite 100 | Bothell | WA 98011 | USA | T: +1 800 424 4284 | F: +1 425 481 3895
Asia-Pacific Headquarters | 11 Tai Seng Link | Singapore | 534182 | T: +65 6383 3832 | F: +65 6383 3830
EMEA & CSA Operations | Incheonweg 7 | 1437 EK Rozenburg | The Netherlands | T: +31 20 7950020 | F: +31 20 7950021
alliedtelesis.com