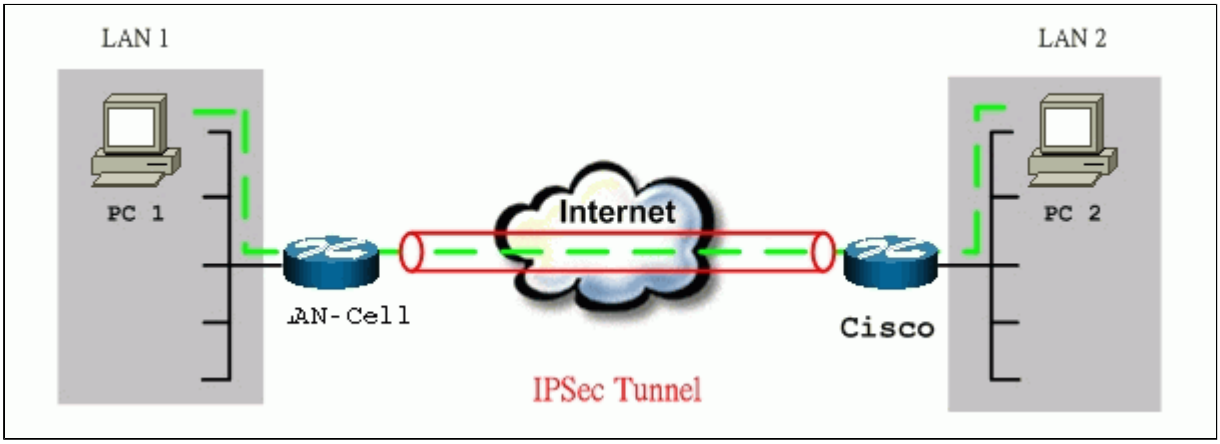
LAN-Cell to Cisco Tunneling

This Tech Note guides you through setting up a VPN connection between a LAN-Cell and a Cisco router. As the figure below shows, the tunnel between the LAN-Cell and the Cisco router ensures that the packets flowing between them are secure. To set up this VPN tunnel, the required settings for the LAN-Cell and the Cisco router are explained in the following sections.



The IP addresses we use in this example are as shown below.

LAN 1	LAN-Cell	CISCO	LAN 2
192.168.1.0/24	LAN: 192.168.1.1 WAN: 172.21.10.50 (dynamic IP)	LAN: 192.168.2.1 WAN: 140.113.10.50 (static IP)	192.168.2.0/24

Notes:

1. When using a Cisco Router to establish VPN, back-to-back connection is not applicable. In other words, the WAN IP of the LAN-Cell and the Cisco router can't be in the same subnet.

2. If the WAN IP of the LAN-Cell is dynamically assigned by the ISP, enter **0.0.0.0** as its **My IP Address.** When the ISP assigns the LAN-Cell's WAN IP, it will update this field.

3. It is most helpful if you can have simultaneous side-by-side access to the LAN-Cell and Cisco configuration screens to compare settings. A difference in a single parameter (e.g. unmatched subnet ranges) can prevent the tunnel from being successfully created.

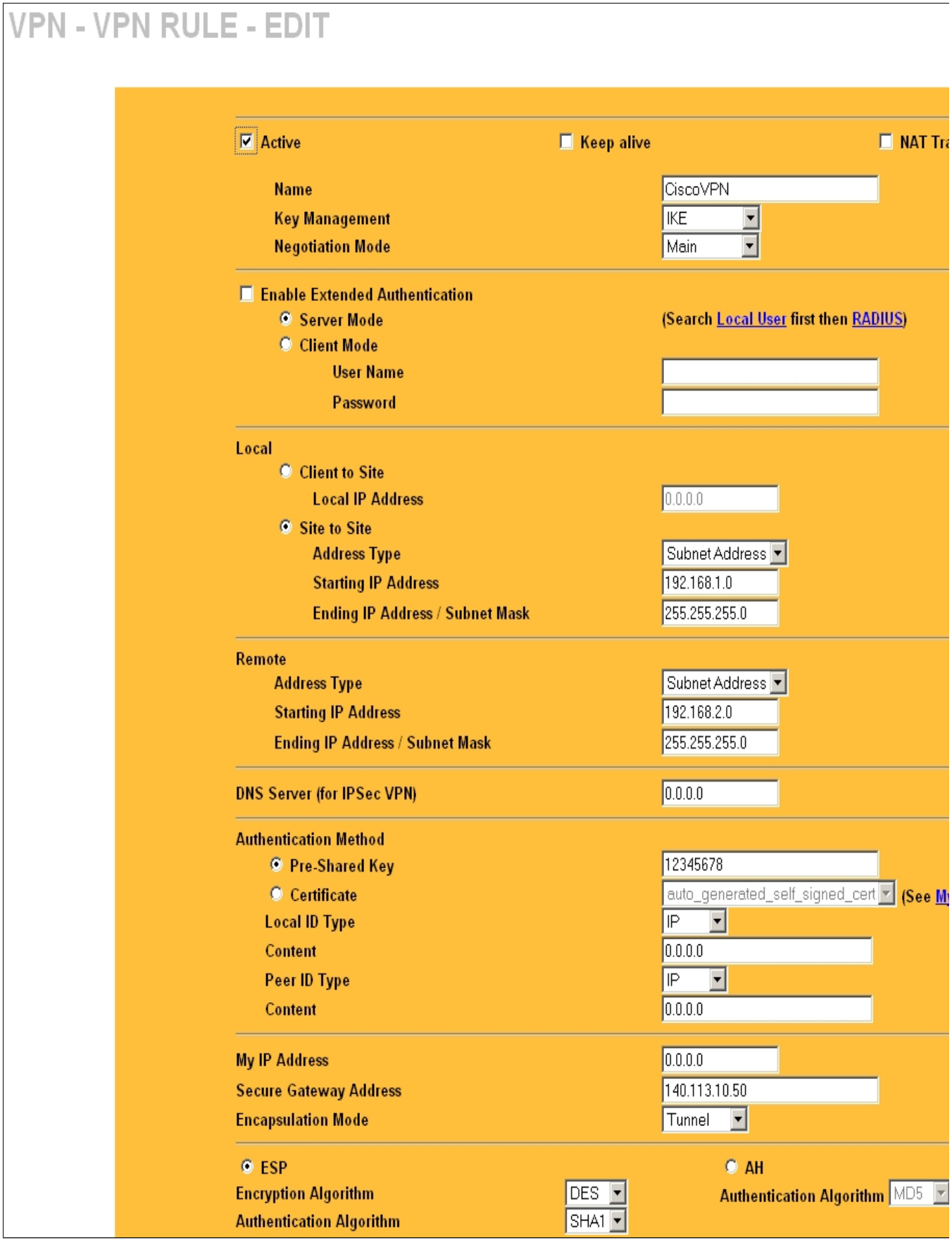
4. If you have difficulty establishing the VPN connection, refer to the LAN-Cell's IKE & IPSec Logs for information on where in the process the VPN is failing to be established. You may wish to clear the log between attempts to more easily identify status and error messages.

5. The most common errors when configuring VPN connections are incorrect subnets specified for each LAN side of the tunnel and mismatched encryption and authentication protocols. Please check your settings carefully. A simple network diagram noting the various LAN and WAN IP addresses/subnets (such as the one above) is often helpful in highlighting misconfiguration issues.

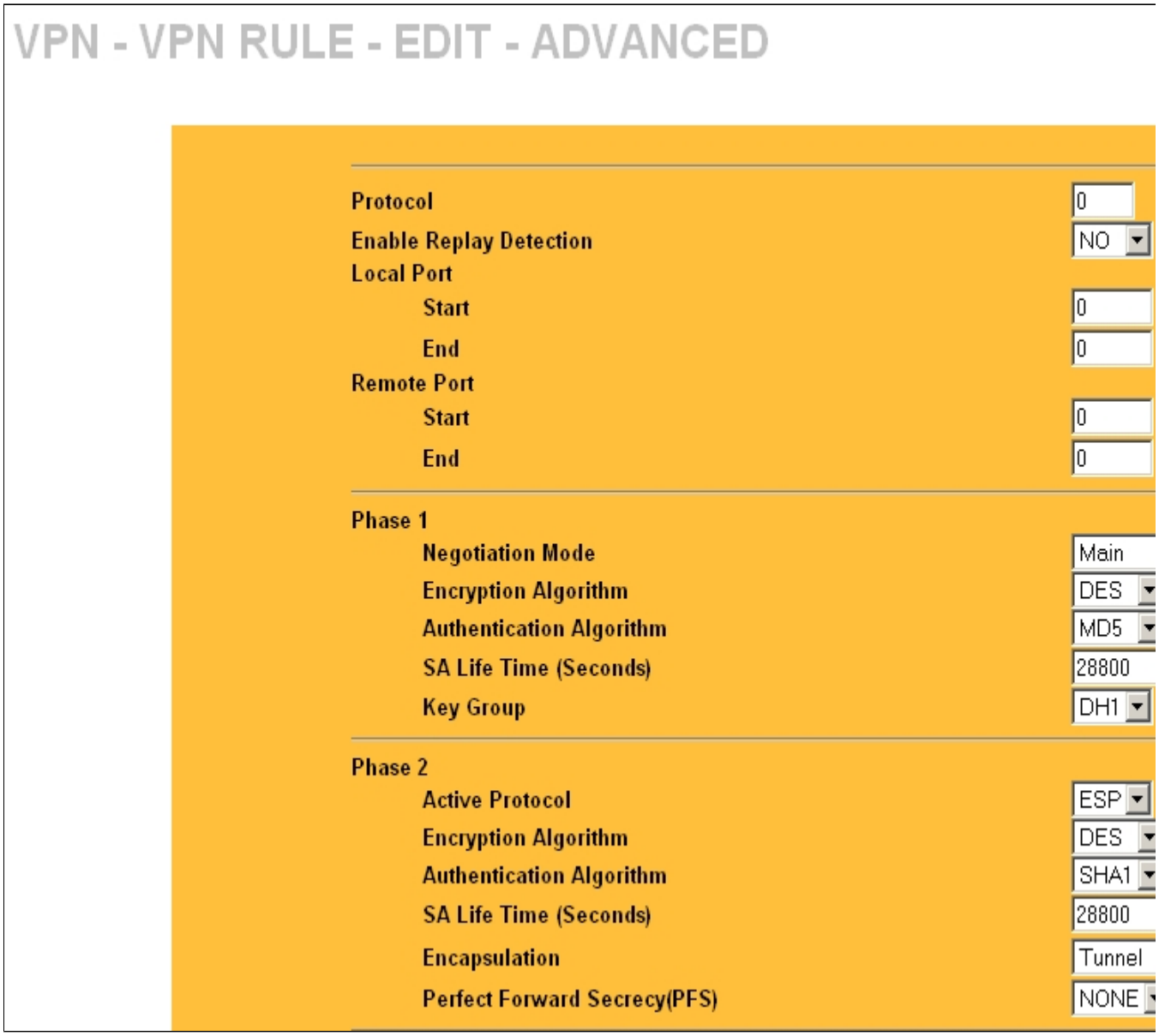
1. Setup LAN-Cell

1. Login to the LAN-Cell by giving the LAN IP address of LAN-Cell in URL field. The default LAN IP is **192.168.1.1**, and the default password is **1234**.
2. Click the **VPN** menu item on the left.
3. On the **VPN RULES** tab, select a policy to edit by clicking **Edit**.
4. On the **VPN RULE EDIT** page, check the **Active** check box and give a name to this policy (e.g. CiscoVPN).
5. Select **Key Management** to **IKE** and **Negotiation Mode** to **Main.** These same options must be configured in the Cisco router.
6. In the **Local** section, select the Address Type to **Subnet Address**. Specify the **network IP** of LAN-Cell's LAN segment in the **IP Address Start** field and the subnet mask in **End/Subnet Mask** field.
7. In **Remote** section, select the Address Type to **Subnet Address**. Specify the **network IP** of peer's LAN segment (private side of the Cisco router) in the **IP Address Start** field and the subnet mask in **End/Subnet Mask** field.
8. When specifying Local & Remote subnet addresses, the range should start at the network address (e.g. 192.168.1.0).
9. Enter the **Preshared Key** that is common between the LAN-Cell and Cisco router.
10. Choose **Local ID** type as **IP** and set the **Content** value to 0.0.0.0.
11. Choose **Remote ID** type as **IP** and set the **Content** value to 0.0.0.0.
12. Set **My IP Address** to the **WAN IP of LAN-Cell.** If the LAN-Cell's WAN IP address is dynamically assigned by your ISP (cellular carrier), then enter 0.0.0.0 as **My IP Address**.
13. Set the **Secure Gateway Address** to the Cisco's Public WAN IP address (140.113.10.50 in this example). If the Cisco router's WAN IP is mapped to a DNS entry, you may enter the router's FQDN in this field as long as the LAN-Cell has a suitable DNS server defined for resolving WAN addresses (see the DNS settings on the **System** menu).
14. Select **Encapsulation Mode** to **Tunnel**.
15. Check the **ESP** check box. (AH can not be used in the SUA/NAT case)
16. Select **Encryption Algorithm** to **DES/SHA1** and **Authentication Algorithm** to **MD5**, or as configured in the Cisco router.

See the screen shot:


VPN - VPN RULE - EDIT
Active
Keep alive
NAT Tra
Name
CiscoVPN
Key Management
IKE
Negotiation Mode
Main
Enable Extended Authentication
Server Mode
(Search Local User first then RADIUS)
Client Mode
User Name
Password
Local
Client to Site
Local IP Address
0.0.0.0
Site to Site
Address Type
Subnet Address
Starting IP Address
192.168.1.0
Ending IP Address / Subnet Mask
255.255.255.0
Remote
Address Type
Subnet Address
Starting IP Address
192.168.2.0
Ending IP Address / Subnet Mask
255.255.255.0
DNS Server (for IPSec VPN)
0.0.0.0
Authentication Method
Pre-Shared Key
12345678
Certificate
auto_generated_self_signed_cert
(See My
Local ID Type
IP
Content
0.0.0.0
Peer ID Type
IP
Content
0.0.0.0
My IP Address
0.0.0.0
Secure Gateway Address
140.113.10.50
Encapsulation Mode
Tunnel
ESP
AH
Encryption Algorithm
DES
Authentication Algorithm
MD5
Authentication Algorithm
SHA1

You can further adjust IKE Phase 1/Phase 2 parameters by pressing **Advanced** button. The setting for each value on this page must match the corresponding settings in the Cisco router.



2 Set Up Cisco Router

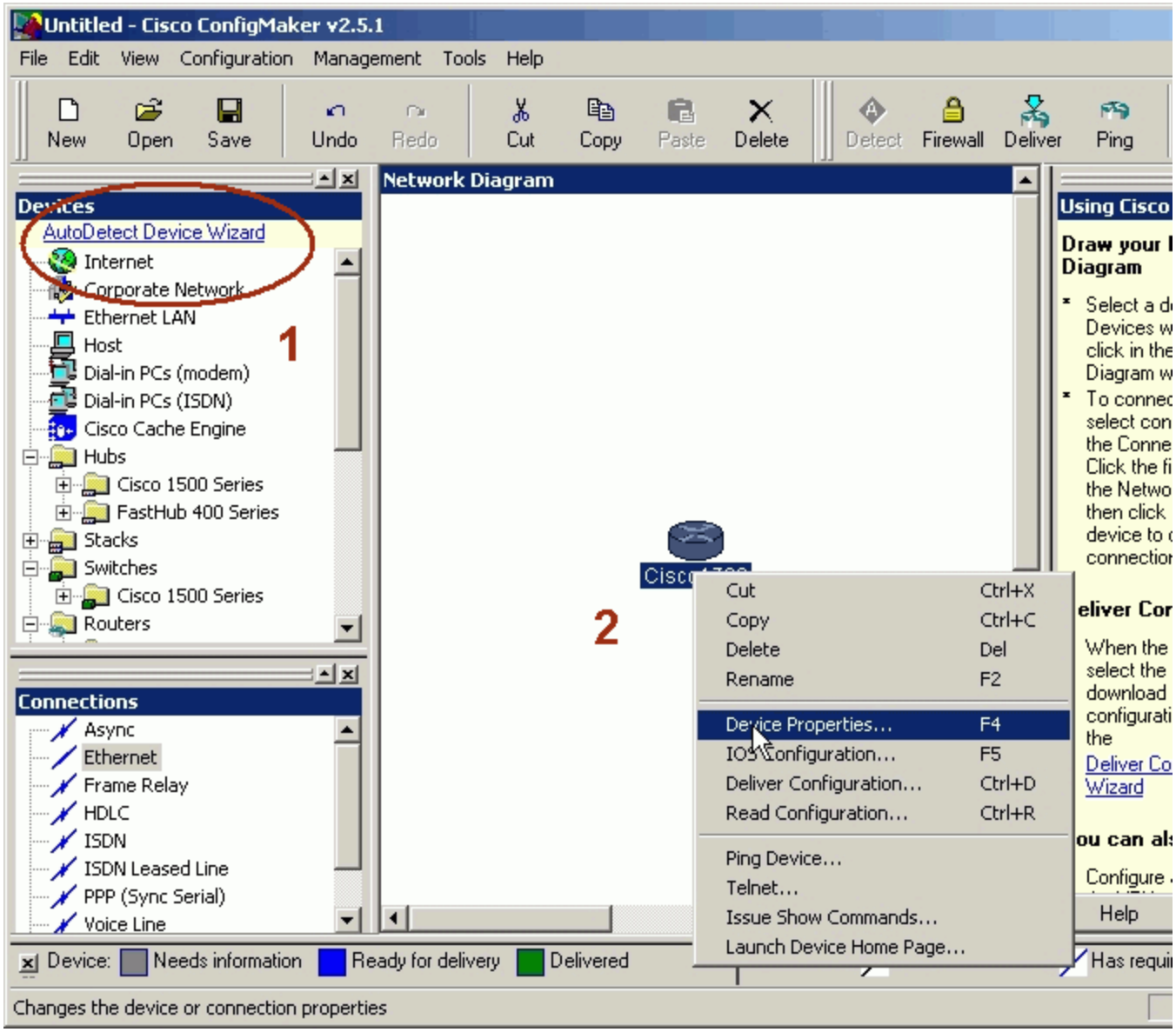
There are two ways to configure a Cisco VPN: using commands from theconsole or using the **Cisco ConfigMaker**. Cisco ConfigMaker is an easy-to-use Windows 98/Me/NT/2000 application that configures Cisco routers, switches, hubs, and other devices. We will guide you through how to setup IPSec by using Cisco ConfigMaker in Section 2.1. If you prefer to use commands from console, please go to Section 2.2.

2.1 Set Up Cisco Router via ConfigMaker

You can download Cisco ConfigMaker from
http://www.cisco.com/warp/public/cc/pd/nemnsw/cm/index.shtml.

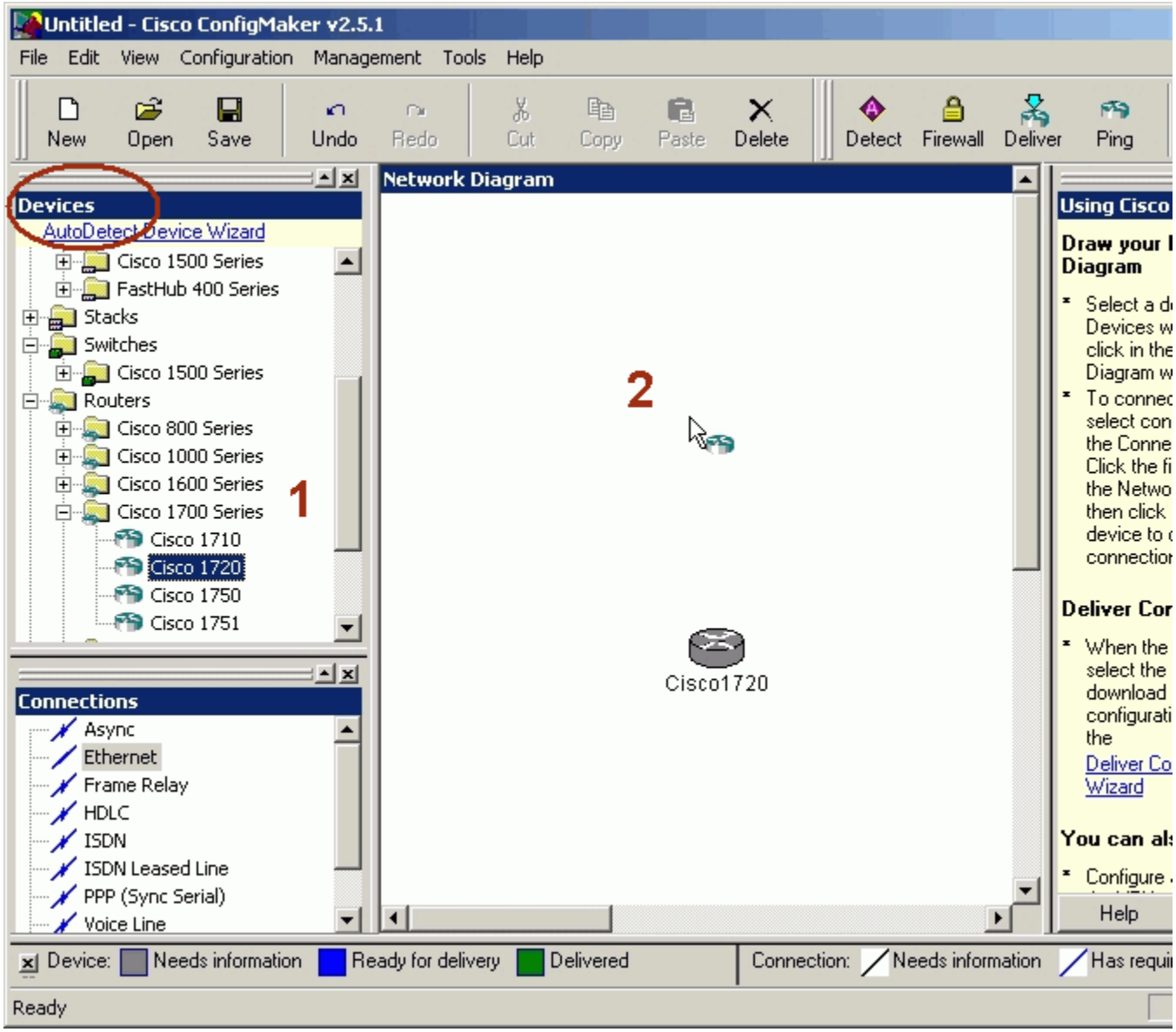
1. Select **AutoDetect device Wizard** in **Devices** window.
2. Make sure that the console has been connected to your PC. If the router is detected successfully, a Cisco router should appear in the Network Diagram Window.
3. Click the right button of the mouse, choose **Device Properties....** In **Passwords** tab, setup the passwords for this router.

See the screen shot:



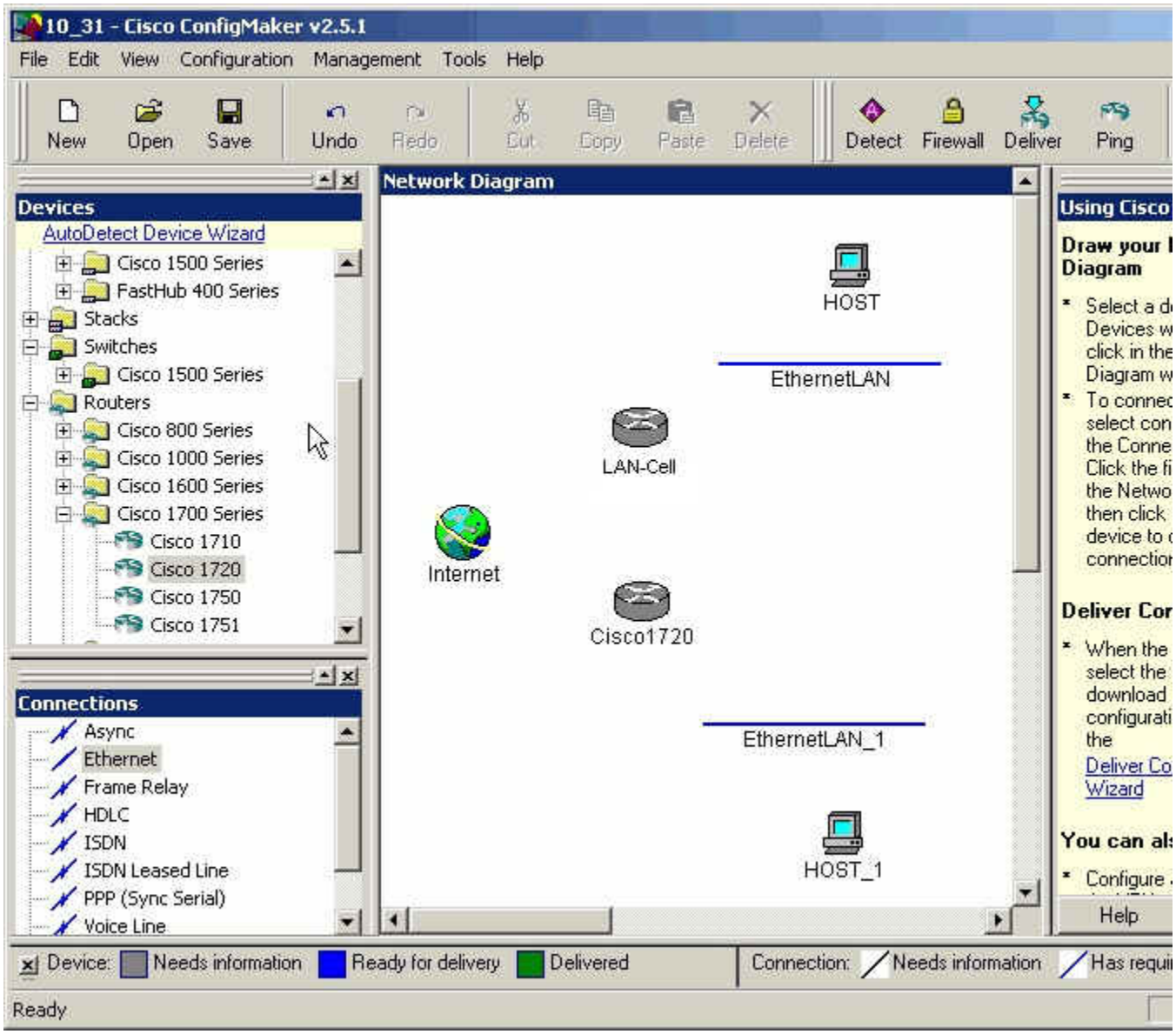
4. From **Devices window** choose a router, and add this router in **Network Diagram**. Rename it as "**LAN-Cell**". Assign passwords, choose **TCP/IP** as it's protocol, and then set the interface of WAN slot 0 as **1 Ethernet.**

See the screen shot:



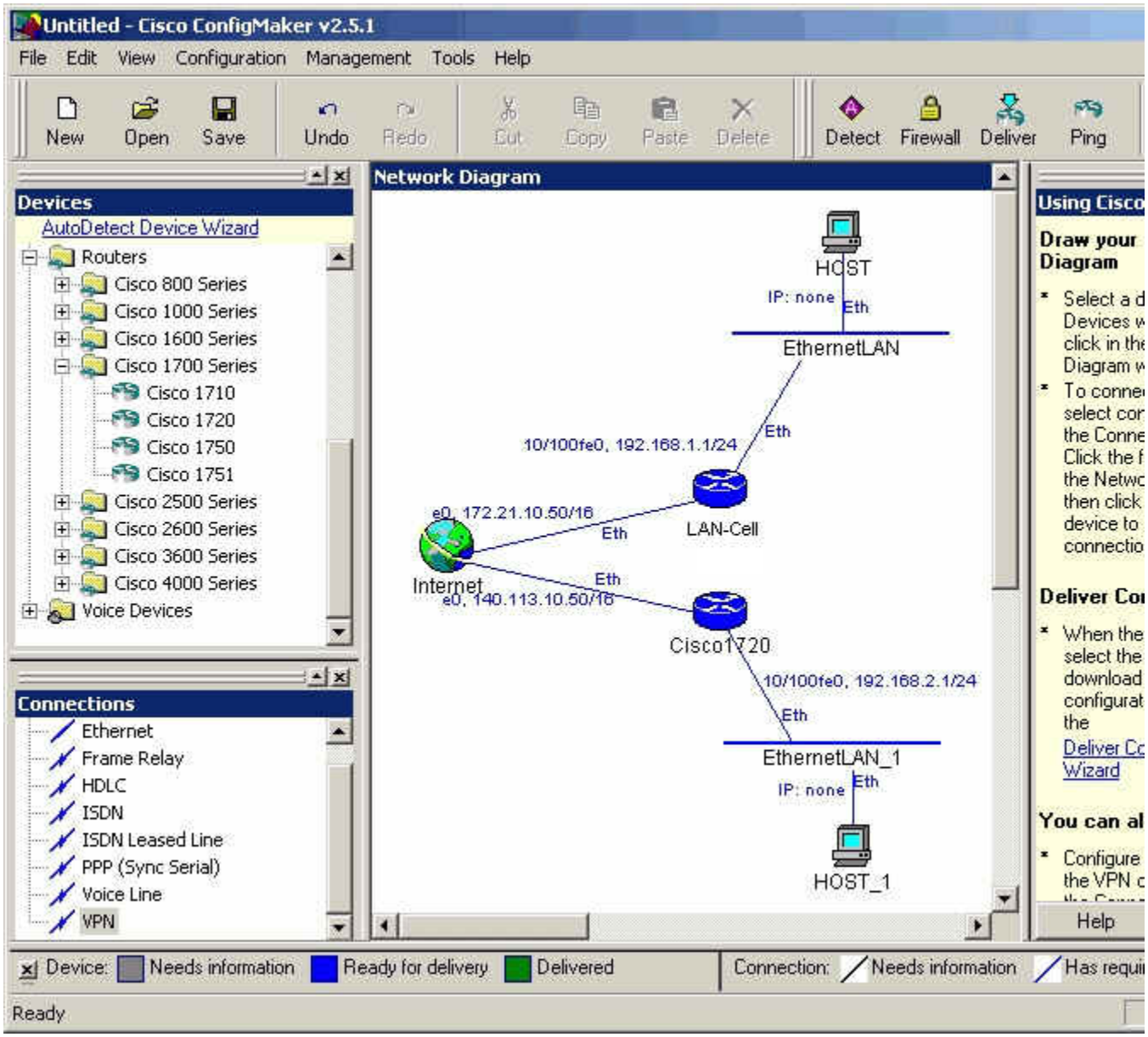
5. Layout your network topology in the Network Diagram as shown below. You may choose network components, such as **hosts, Internet, Ethernet LAN** from the **Devices** window.

See the screen shot:



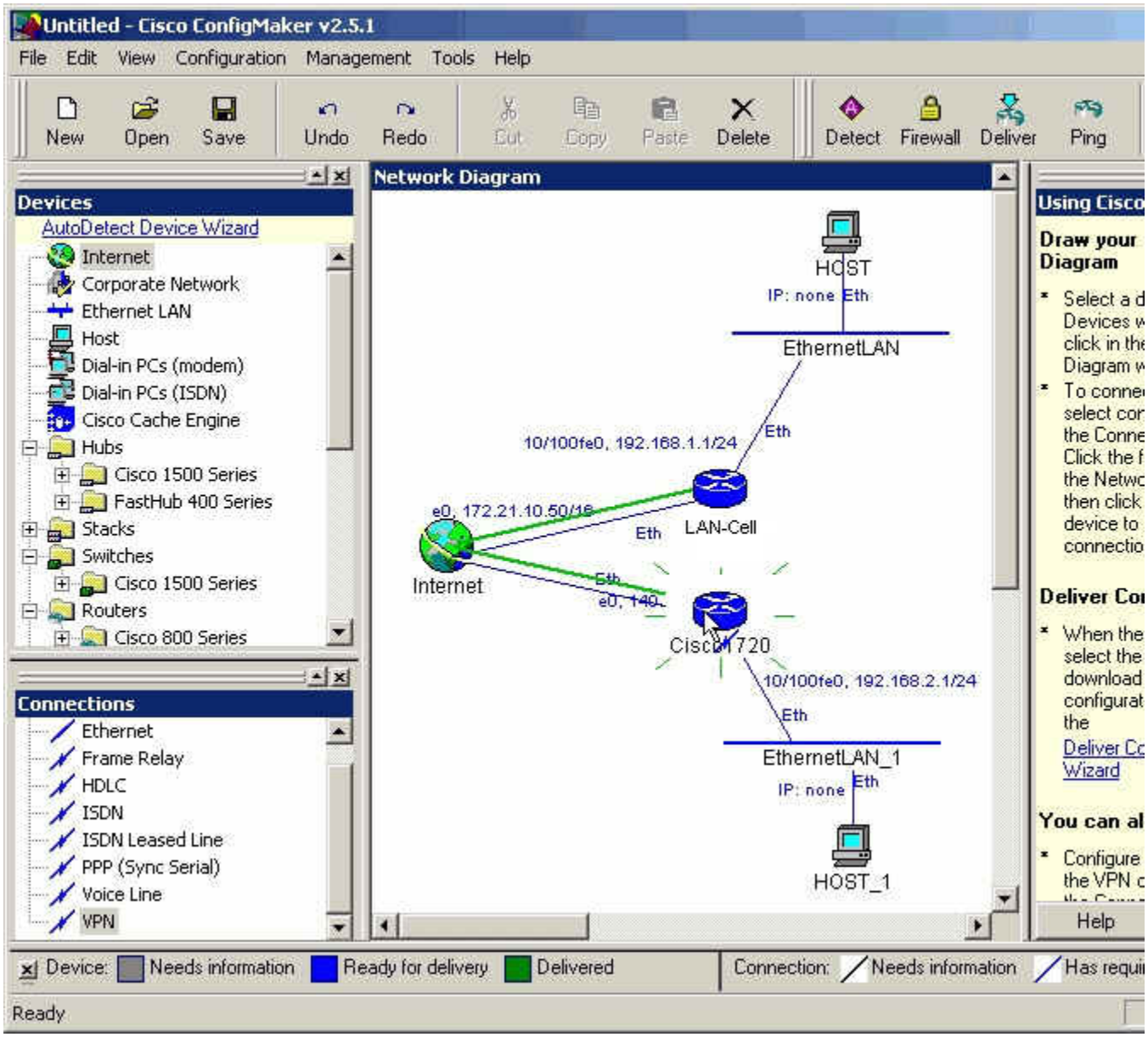
6. Connect the network components by **Ethernet** from the **Connections** window in the left bottom. Specify the WAN and LAN IP addresses of the LAN-Cell and Cisco.

See the screen shot:



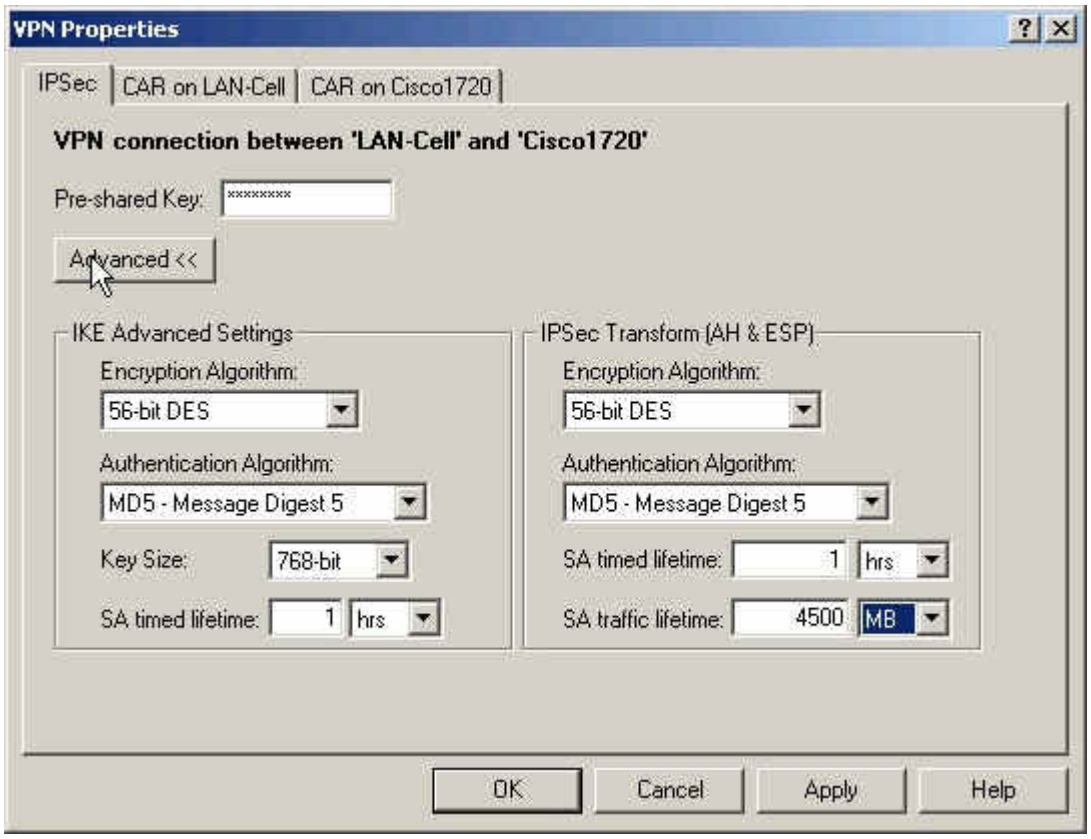
7. Select **VPN** from **Connections** window. During this stage, you have to enter the pre-shared key, "**12345678**".

See the screen shot:



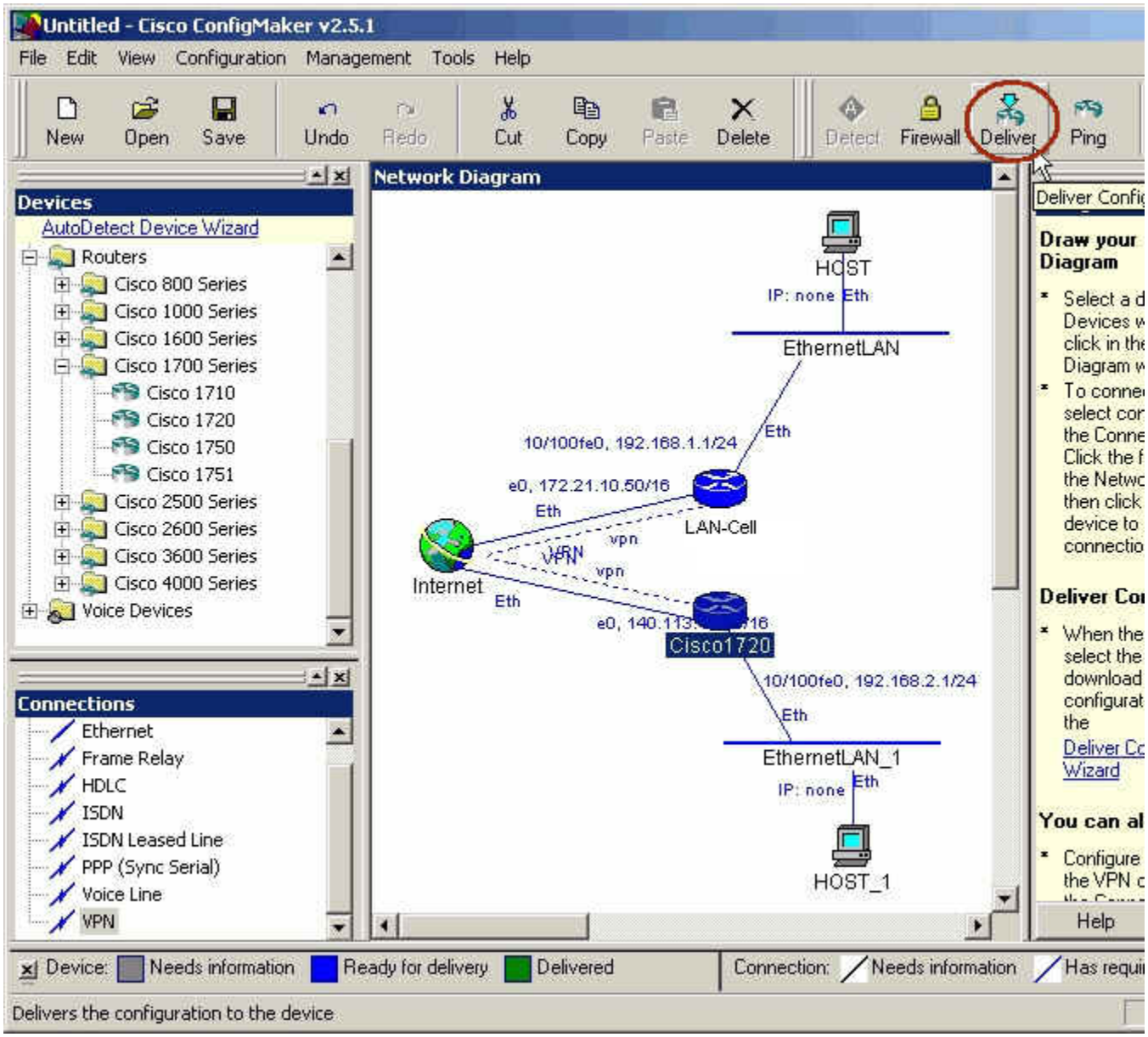
8. Select **VPN**, then click the right button of the mouse, and choose **Connection Properties...**. Setup IPSec parameters as shown below. Note that the parameters you set here should match settings in LAN-Cell. In **IKE Advanced Settings**, **Encryption Algorithm** is **56-bit DES**, **Authentication Algorithm** is **MD5** and the **SA lifetime** is **1 hr**. In IPSec Transform, **Encryption Algorithm** is **56-bit DES**, **Authentication Algorithm** is **MD5**, and **SA lifetime** is **1 hr**.

See the screen shot:



9. Choose the Cisco router, and click **Deliver** to save the settings.

See the screen shot:



10. Enter Cisco **commands mode** from console and check if Cisco can make a successful ping to the LAN-Cell. You might have to tune the configuration to accommodate your practical environment. For more detailed information, please go to http://www.cisco.com
11. In **config mode**, enter a command "**crypto ipsec transform-set cm-transformset-1 esp-des esp-md5-hmac**".
12. After all of the settings, if PC1 and PC2 can reach each other, then IPSec VPN has been established successfully. There is also an useful command to debug IPSec VPN, "**debug crypto ipsec**".

2.2 Set Up Cisco Router via Commands

Note that, in order to set up the Cisco router by commands, you have to connect your PC and Cisco

router by a console cable. Enter the following commands one per line.

Cisco1720#**config**
Cisco1720#<*start typing the commands below*>

```
!
version 12.2
no parser cache
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname Cisco1720
!
logging rate-limit console 10 except errors
enable password 7 1543595F50
!
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
no ip domain-lookup
!
ip dhcp pool 1
   network 192.168.2.0 255.255.255.0
   default-router 192.168.2.1
!
ip audit notify log
ip audit po max-events 100
ip ssh time-out 120
ip ssh authentication-retries 3
no ip dhcp-client network-discovery
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
 lifetime 3600
crypto isakmp key 12345678 address 172.21.10.50
!
!
crypto ipsec transform-set cm-transformset-1 esp-des esp-md5-hmac
crypto mib ipsec flowmib history tunnel size 200
crypto mib ipsec flowmib history failure size 200
!
crypto map cm-cryptomap local-address Ethernet0
crypto map cm-cryptomap 1 ipsec-isakmp
 set peer 172.21.10.50
 set transform-set cm-transformset-1
 match address 100
!
!
!
!
```

```
interface Ethernet0
 description connected to Internet
 ip address 140.113.10.50 255.255.0.0
 half-duplex
 crypto map cm-cryptomap
!
interface FastEthernet0
 description connected to EthernetLAN_1
 ip address 192.168.2.1 255.255.255.0
 speed auto
!
router rip
 version 1
 passive-interface Ethernet0
 network 140.113.0.0
 network 192.168.2.0
 no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet0
no ip http server
!
access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
!
!
snmp-server community public RO
!
line con 0
 exec-timeout 0 0
 password 7 06575D7218
 login
line aux 0
line vty 0 4
 password 7 11584B5643
 login
line vty 5 15
 login
!
no scheduler allocate
end
```

After all of the settings, if PC1 and PC2 can reach each other, then IPSec VPN has been established successfully. There is also a useful command to debug IPSec VPN, "**debug crypto ipsec**".