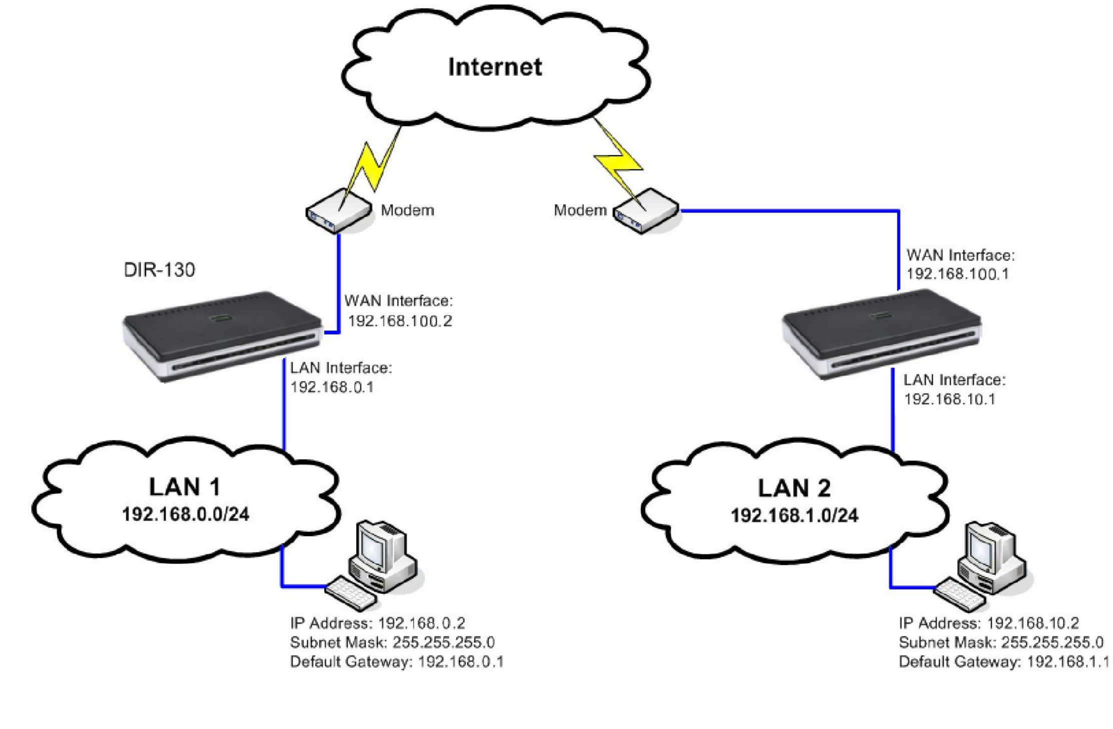
How to configure an IPSec VPN tunnel between two DIR-130's


Internet
Modem
Modem
DIR-130
WAN Interface: 192.168.100.2
LAN Interface: 192.168.0.1
WAN Interface: 192.168.100.1
LAN Interface: 192.168.10.1
LAN 1 192.168.0.0/24
LAN 2 192.168.1.0/24
IP Address: 192.168.0.2
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.0.1
IP Address: 192.168.10.2
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.1.1

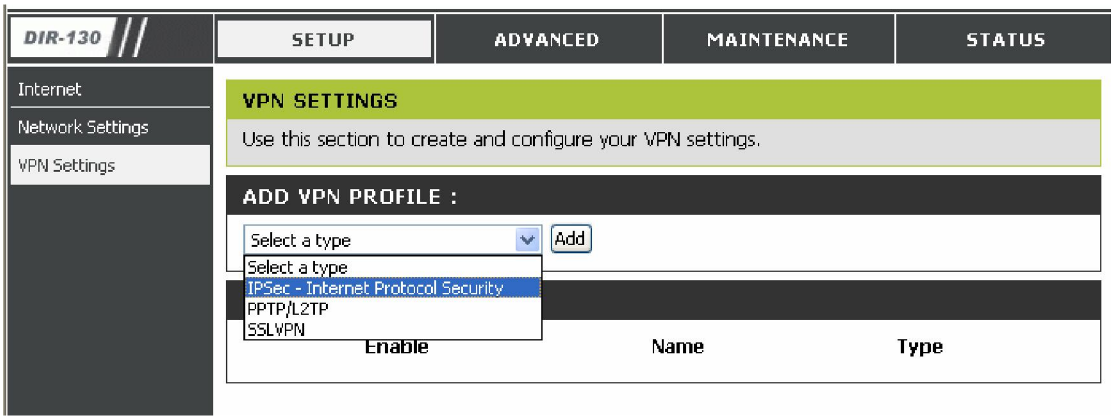
This example will demonstrate how to configure a LAN-to-LAN IPSec VPN tunnel between two DIR-130.

In this example:
LAN1 (Sydney) has the subnet of **192.168.0.0/24**
LAN2 (Melbourne) has the subnet of **192.168.10.0/24**

Configuration of Sydney VPN

Step 1: Open your web browser and type in the IP address of the router (192.168.0.1 by default). Enter the username (admin by default) and password (blank by default), and then click **OK**.

Step 2: Click on **SETUP** and select **VPN SETTINGS**. Choose **IPSec** from the **ADD VPN PROFILE** dropdown menu and click **Add**.



VPN SETTINGS

Use this section to create and configure your VPN settings.

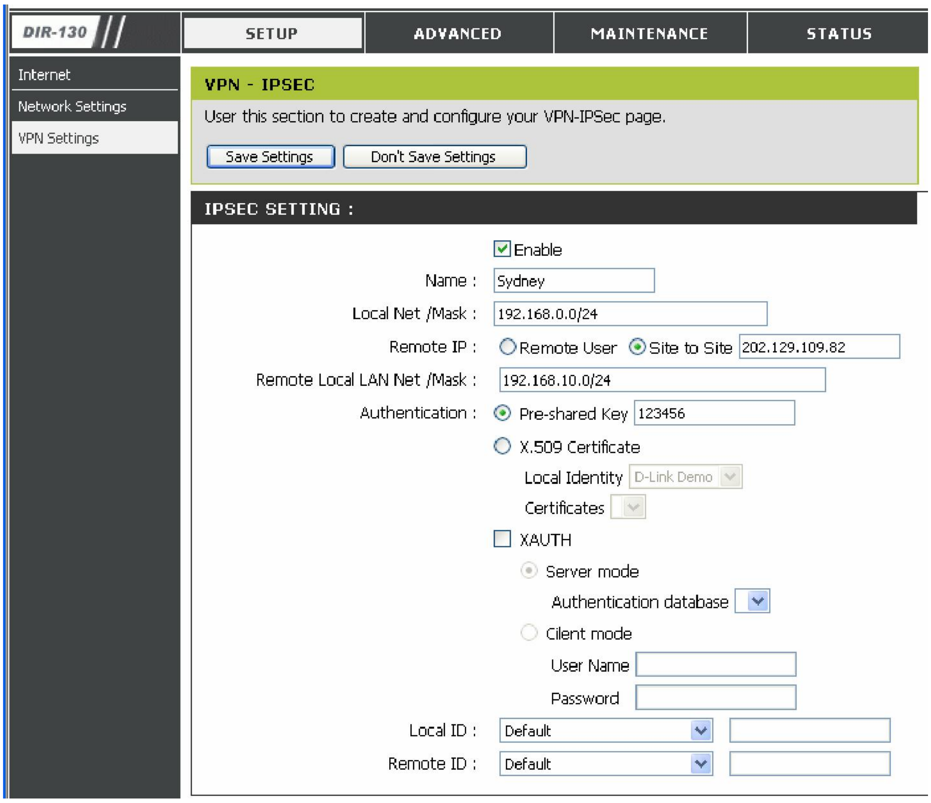
ADD VPN PROFILE :

Select a type

- Select a type
- IPSec - Internet Protocol Security
- PPTP/L2TP
- SSLVPN

Step 3: Configure the IPSec VPN as followed:
Enable Settings: check box to enable

Name: enter a name for the VPN
Encapsulation Mode: Tunnel
Remote IP: select Site to Site and enter the remote Gateway
Remote Local LAN Net /Mask: enter the remote LAN network and Subnet Mask
Authentication Protocol: enter a Pre-shared Key (must be the same as the Remote Side)
Phase 1 IKE Proposal List: leave as is
NAT-**T Enabled**: leave as is
PFS: check to enable
Phase 2 IPSec Proposal List: leave as is

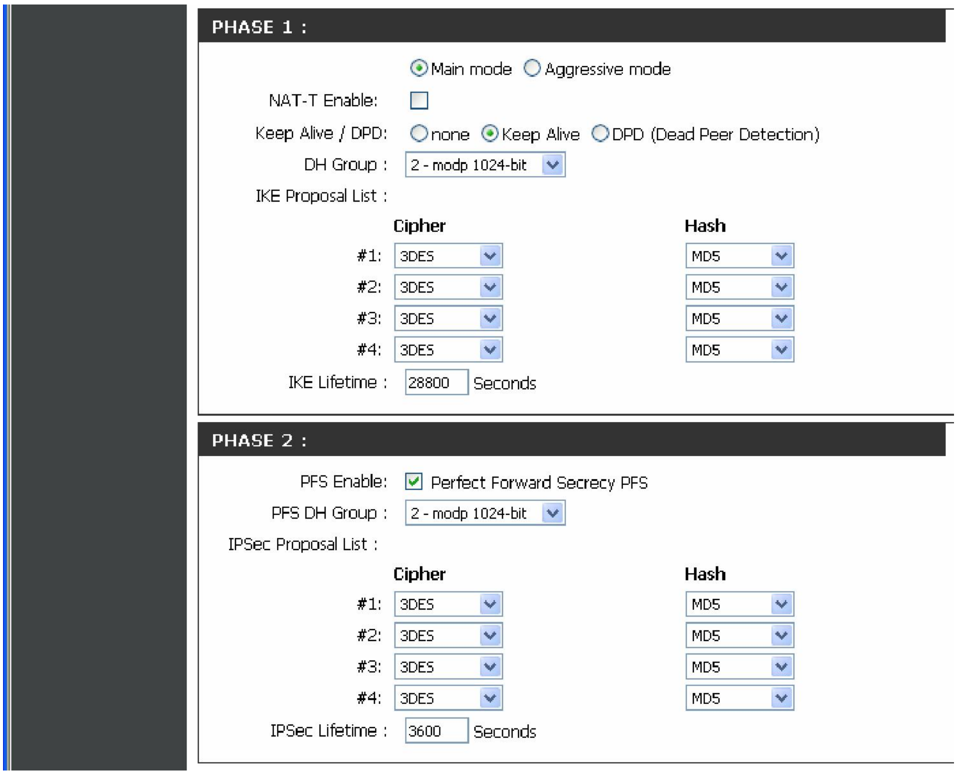


VPN - IPSEC

User this section to create and configure your VPN-IPSec page.

IPSEC SETTING :

☑ Enable
Name : Sydney
Local Net /Mask : 192.168.0.0/24
Remote IP : ○ Remote User ● Site to Site 202.129.109.82
Remote Local LAN Net /Mask : 192.168.10.0/24
Authentication : ● Pre-shared Key 123456
○ X.509 Certificate
Local Identity D-Link Demo
Certificates
□ XAUTH
● Server mode
Authentication database
○ Client mode
User Name
Password
Local ID : Default
Remote ID : Default



PHASE 1 :

● Main mode ○ Aggressive mode

NAT-T Enable: □

Keep Alive / DPD: ○ none ● Keep Alive ○ DPD (Dead Peer Detection)

DH Group : 2 - modp 1024-bit

IKE Proposal List :

	Cipher	Hash
#1:	3DES	MD5
#2:	3DES	MD5
#3:	3DES	MD5
#4:	3DES	MD5

IKE Lifetime : 28800 Seconds

PHASE 2 :

PFS Enable: ☑ Perfect Forward Secrecy PFS

PFS DH Group : 2 - modp 1024-bit

IPSec Proposal List :

	Cipher	Hash
#1:	3DES	MD5
#2:	3DES	MD5
#3:	3DES	MD5
#4:	3DES	MD5

IPSec Lifetime : 3600 Seconds

Step 4: Click Save Settings once done.

Configuration of Remote Network

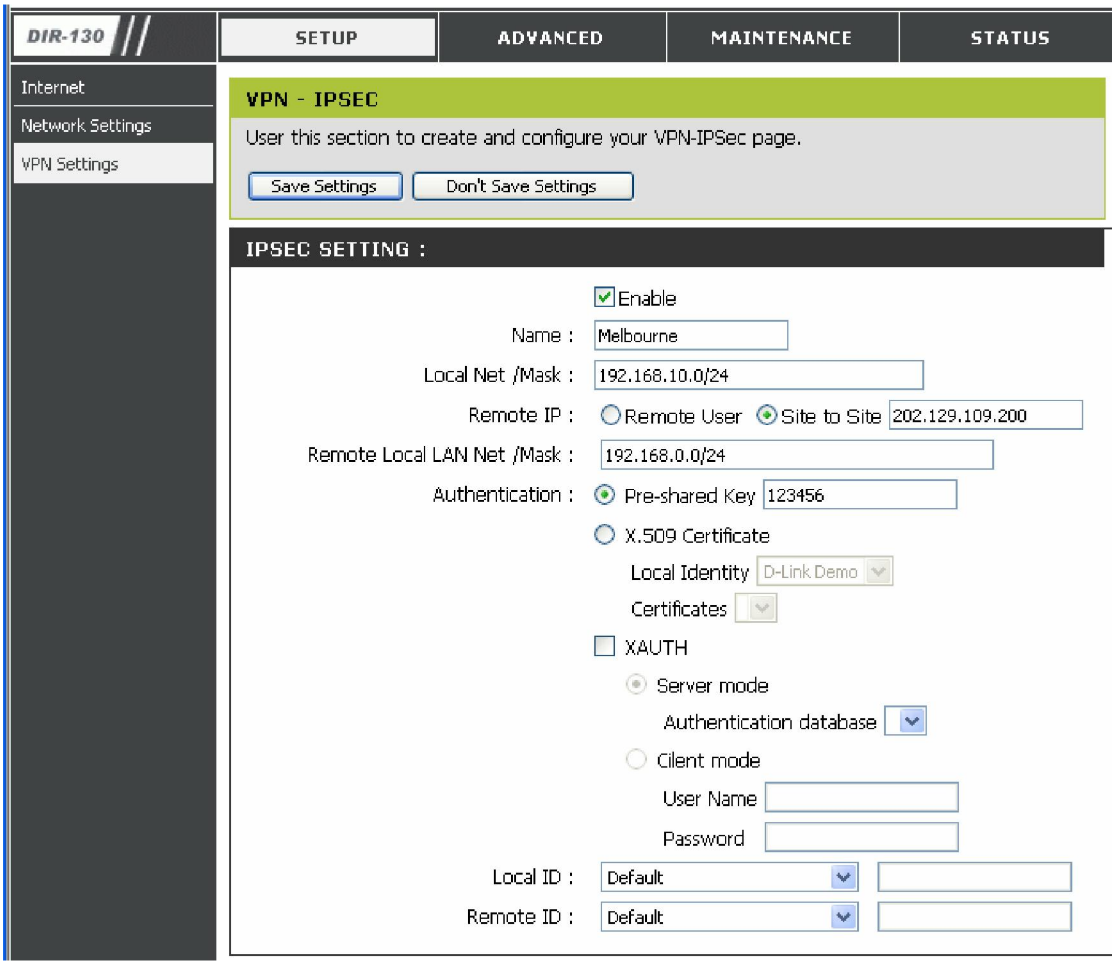
Note: Both sides cannot be on the same subnet.

Step 1: Open your web browser and type in the IP address of the router (192.168.10.1). Enter the username (admin by default) and password (blank by default), and then click **OK**.

Step 2: Click on **SETUP** and select **VPN SETTINGS**.
Choose **IPSec** from the **ADD VPN PROFILE** dropdown menu and click **Add**.

Step 3: Configure the IPSec VPN as followed:

Enable Settings: check box to enable
Name: enter a name for the VPN
Encapsulation Mode: Tunnel
Remote IP: select Site to Site and enter the remote Gateway
Remote Local LAN Net /Mask: enter the remote LAN network and Subnet Mask
Authentication Protocol: enter a Pre-shared Key (must be the same as the Remote Side)
Phase 1 IKE Proposal List: leave as is
NAT-T Enabled: leave as is
PFS: check to enable
Phase 2 IPSec Proposal List: leave as is

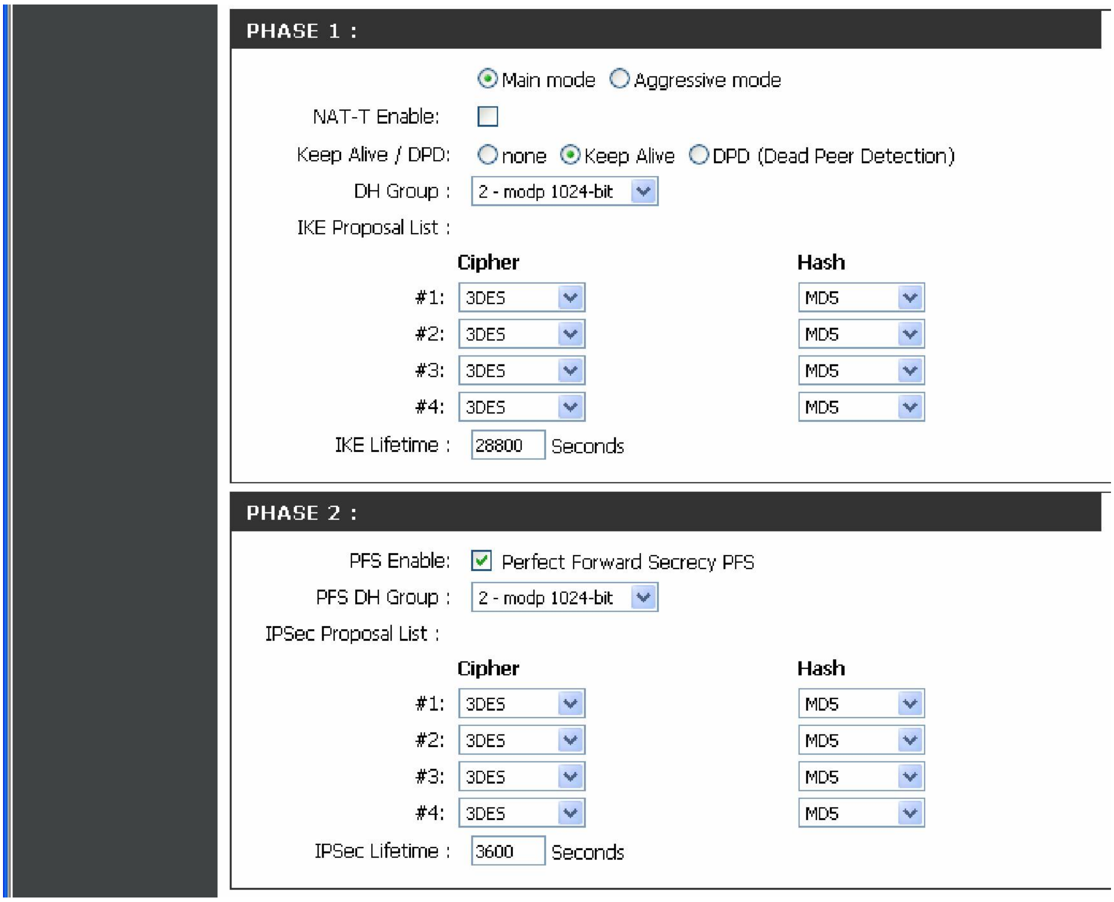


VPN - IPSEC

User this section to create and configure your VPN-IPSec page.

IPSEC SETTING :

☑ Enable
Name : Melbourne
Local Net /Mask : 192.168.10.0/24
Remote IP : ○ Remote User ● Site to Site 202.129.109.200
Remote Local LAN Net /Mask : 192.168.0.0/24
Authentication : ● Pre-shared Key 123456
○ X.509 Certificate
Local Identity D-Link Demo
Certificates
□ XAUTH
● Server mode
Authentication database
○ Cilent mode
User Name
Password
Local ID : Default
Remote ID : Default



PHASE 1 :

● Main mode ○ Aggressive mode

NAT-T Enable: □

Keep Alive / DPD: ○ none ● Keep Alive ○ DPD (Dead Peer Detection)

DH Group : 2 - modp 1024-bit

IKE Proposal List :

	Cipher	Hash
#1:	3DES	MD5
#2:	3DES	MD5
#3:	3DES	MD5
#4:	3DES	MD5

IKE Lifetime : 28800 Seconds

PHASE 2 :

PFS Enable: ☑ Perfect Forward Secrecy PFS

PFS DH Group : 2 - modp 1024-bit

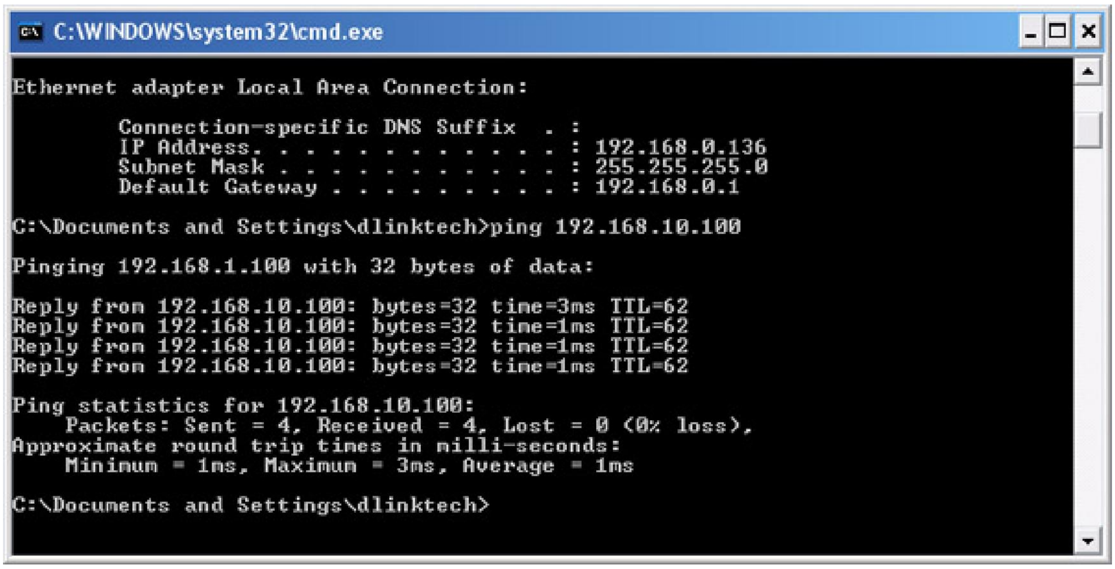
IPSec Proposal List :

	Cipher	Hash
#1:	3DES	MD5
#2:	3DES	MD5
#3:	3DES	MD5
#4:	3DES	MD5

IPSec Lifetime : 3600 Seconds

Step 4: Click Save Settings.

Step 5: The tunnel should be established. To verify connection, open a command prompt and ping to a client on the remote network.



C:\WINDOWS\system32\cmd.exe

```
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.0.136
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1

C:\Documents and Settings\dlinktech>ping 192.168.10.100

Pinging 192.168.1.100 with 32 bytes of data:

Reply from 192.168.10.100: bytes=32 time=3ms TTL=62
Reply from 192.168.10.100: bytes=32 time=1ms TTL=62
Reply from 192.168.10.100: bytes=32 time=1ms TTL=62
Reply from 192.168.10.100: bytes=32 time=1ms TTL=62

Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 1ms

C:\Documents and Settings\dlinktech>
```