GRE/IPSec VPN for 3Com 5642 Router to 3Com X-family

Document Version:	1.2
Publication Date:	18 February 2009
Description:	Configuring site-to-site VPNs from 3Com 5642 Router to X-FAMILY
Product:	3Com X-FAMILY
3Com TOS Version:	2.5.0.6688 or later
3Com 5642 Router Software Version:	Extended_V2.41 (N.B. **Must** be extended version)

1 Overview

This technical note describes how to setup GRE/IPSec VPN tunnels between a 3Com X-FAMILY and the 3Com 5642 Router.

A GRE/IPSec tunnel has a number of benefits over a normal tunnel-mode IPSec VPN:
- it can carry dynamic unicast routing protocols such as RIP;
- it can carry multicast traffic securely;
- it can carry dynamic multicast routing protocols such as PIM-DM.

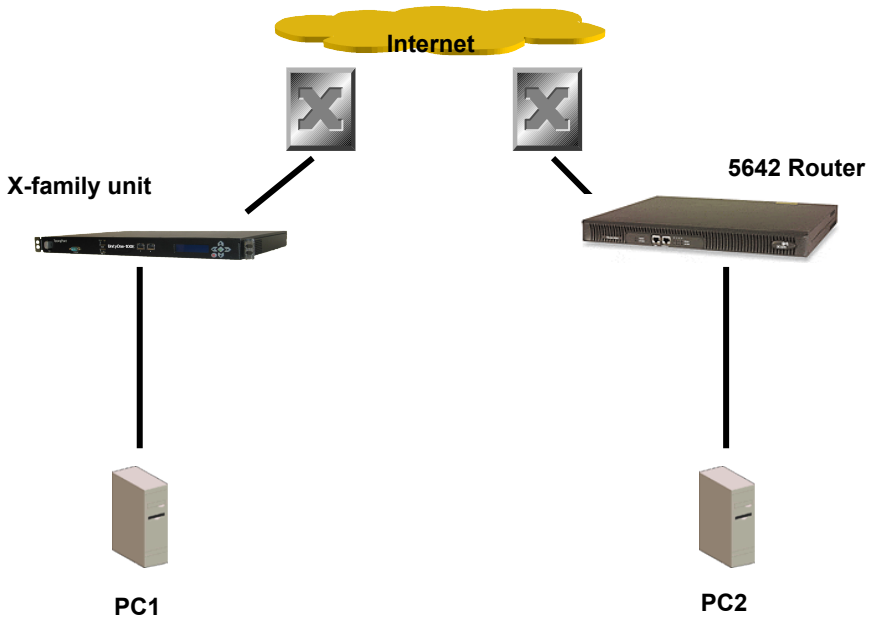
These benefits mean, for example, that a GRE/IPSec tunnel can carry 3COM NBX telephone data traffic securely, including the multicast traffic required for Conference Calls and Paging etc.

Both Main Mode and Aggressive Mode deployments are shown. Main Mode is more secure and hence is recommended when both sites have a static IP address. Aggressive mode can be used if one IP address is dynamic.

This document only describes "shared-secret/pre-shared-key" setup, not the alternative method using X.509 certificates.

2 Connection

This diagram shows the 3Com 5642 Router and an X-family unit connected via the Internet – actually a simple router in my configuration. Each device has a PC connected to its LAN interface – to be used both for configuration and for testing purposes.



Addresses are:

Device	Interface	Address	Mask	Gateway
Router	1 (to X-family)	10.10.20.1	255.255.255.0	
Router	2 (to 5642)	10.10.10.1	255.255.255.0	
X-family	external	10.10.20.147	255.255.255.0	10.10.20.1
X-family	GRE	100.100.100.1	255.255.255.255	
5642 Router	external	10.10.10.147	255.255.255.0	10.10.10.1
5642 Router	GRE	100.100.100.2	255.255.255.255	
PC1		192.168.1.100	255.255.255.0	192.168.1.254
PC2		192.168.22.100	255.255.255.0	192.168.22.254

3 Pre-Configuration before setting up GRE VPNs

3.1 3Com X-FAMILY Pre-Configuration

3.1.1 Initial Setup via the OBE

Setup the user account and then set the basic configuration as follows. The dialogue shown is the OBE ("Out of Box Experience") on the Command Line Interface – alternatively this could be set up using the OBE on the Graphical User Interface).

```
Your super-user account has been created.
You may continue initial configuration by logging into your device.
After logging in, you will be asked for additional information.

Login: topuser
Password: t0p--us3r

Entering Setup wizard...

Enter Host Name [myhostname]: 3KB_X_unit_1
Enter Host Location [room/rack]: Lab

            Host Name: 3KB_X_unit_1
        Host Location: Lab
Enter [A]ccept, [C]hange, or [E]xit without saving [C]: a

Timekeeping options allow you to set the time zone, enable or disable
daylight saving time, and configure or disable NTP.

Would you like to modify timekeeping options? <Y,[N]>:

The X-Series device may be configured into a number of well known
network deployments.

Would you like to modify the network deployment mode? <Y,[N]>:

Virtual interfaces define how this device integrates with the IP layer 3
network.  You must configure one virtual interface for every IP subnet
that is directly connected to the X-Series device.  For example, you
need
```

```
one for the WAN connection (external virtual interface) and one for
every
directly connected network subnet (internal virtual interfaces).

Would you like to modify virtual interfaces? <Y,[N]>:y

Virtual interfaces:
Id  Type      Mode    IP Address       Subnet Mask      NAT
 1  internal  static  192.168.1.254    255.255.255.0    external-ip
 2  external  dhcp                                     disable
 3  <empty>
 4  <empty>
 5  <empty>
 6  <empty>

Enter [A]ccept, [C]hange, [R]emove or [E]xit without saving [C]:
Enter the number of the entry you want to change []: 2
Mode (static, dhcp, pppoe, pptp, l2tp) [dhcp]: sta
IP address []: 10.10.20.147
Mask [255.255.255.0]:

Virtual interfaces:
Id  Type      Mode    IP Address       Subnet Mask      NAT
 1  internal  static  192.168.1.254    255.255.255.0    external-ip
 2  external  static  10.10.20.147     255.255.255.0    disable
 3  <empty>
 4  <empty>
 5  <empty>
 6  <empty>

Enter [A]ccept, [C]hange, [R]emove or [E]xit without saving [C]: a

You must configure a default gateway manually if external virtual
interface is static.

Would you like to modify default gateway? <Y,[N]>:y
Default Gateway [0.0.0.0]: 10.10.20.1

Security zones enable you to section your network logically into
security
domains.  As network traffic travels between zones, it is routed and
security-scanned by the firewall and IPS according to the policies you
define.  You need to create security zones that naturally map onto your
intended network security boundaries.  A security zone may or may not be
connected (mapped) to a virtual interface.

Would you like to modify security zones? <Y,[N]>:

Would you like to modify security zone to virtual interface mapping? <Y,
[N]>:

DNS (Domain Name Service) is a system which translates computer
hostnames
to IP addresses. The X-Series device requires DNS configuration in order
to perform web filtering.

Would you like to configure DNS? <Y,[N]>:
```

```
Firewall policy rules control the flow of network traffic between
security zones.  Firewall policy rules control traffic flow based
on source and destination security zones and network protocol.

Would you like to modify firewall policy rules? <Y,[N]>:

SMS-based configuration allows the device to retrieve the configuration
for a secure management VPN to the SMS system.  This ensures that
the device can be managed securely from the SMS

Would you like to enable SMS-based configuration? <Y,[N]>:

If you wish to run this wizard again, use the 'setup' command.

3KB_X_unit_1#
```

Notes:

Virtual Interfaces - There are two virtual interfaces (external and internal) set up as factory default. The only configuration required on them is to set the IP addresses. (In the example, I have kept the internal IP address as default and changed the external IP address).

Security Zones – The factory default configuration sets the LAN security zone to be on Port 1 and linked to the internal Virtual Interface. The WAN security zone is on the last port (Port 4 on an X505 or port 6 on the X506 and X5) and is linked to the external virtual interface. No change is needed to this.

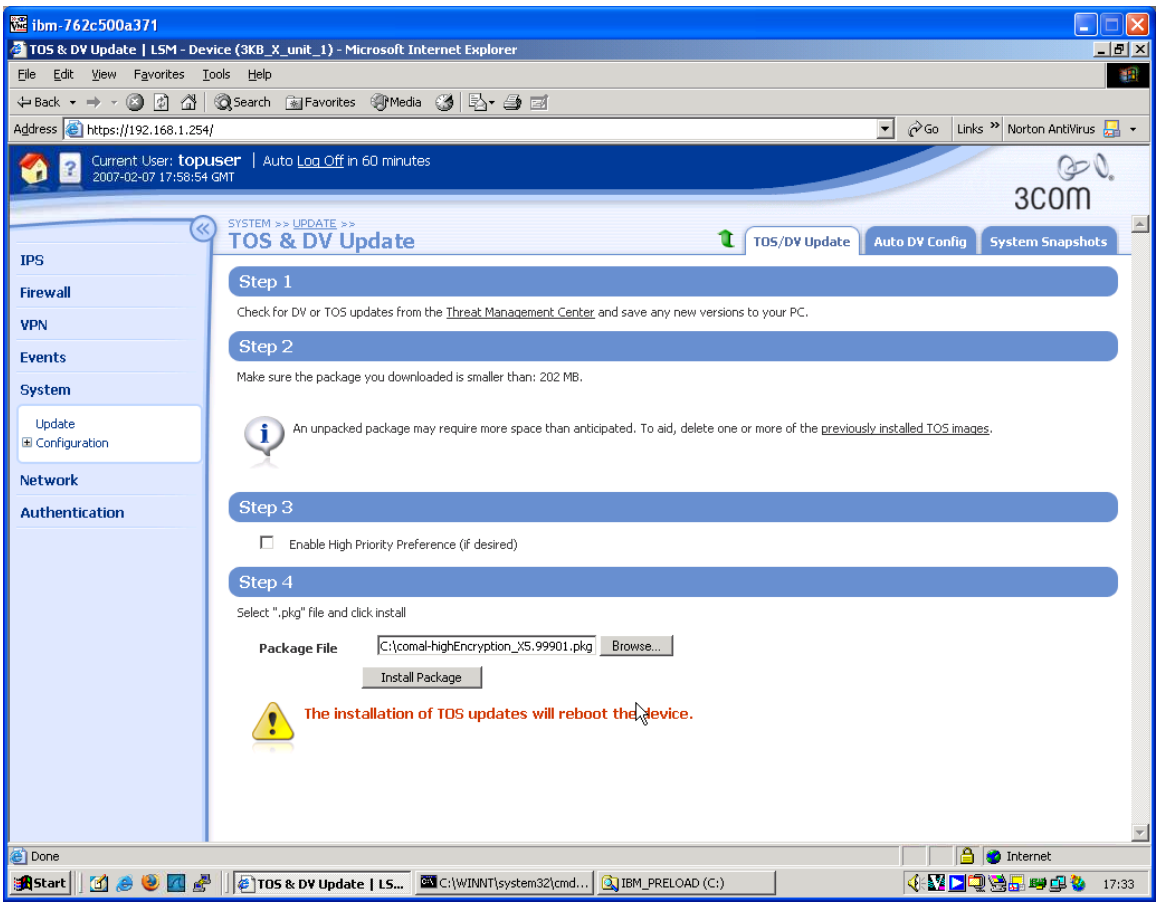
Firewall rules – the firewall rules in the factory default configuration will be sufficient – specifically this one:

2 permit WAN this-device vpn-protocols

3.1.2 Load the High Encryption Token

When delivered from the factory, the X-FAMILY devices are capable of encryption levels up to a key size of 64 bits (e.g. DES). To enable higher encryption key sizes to be used (e.g. 3DES, AES) a High Encryption "token" package must be loaded onto the device. This package is only available to approved end users in approved locations.

1. Acquire the High Encryption package from the TMC and load it onto PC1.
2. Open a browser on PC1, connect to https://192.168.1.254 and login as the user you set up during the OBE.
3. Navigate to System -> Update, open the "TOS/DV Update" tab and complete the form as shown below with the path of the High Encryption package on PC1. Click "Install Package".



4. The package will be installed and the X-FAMILY device will reboot. The X-FAMILY device is ready to set up the VPN when reboot has completed.

3.2 3Com 5642 Router Pre-Configuration

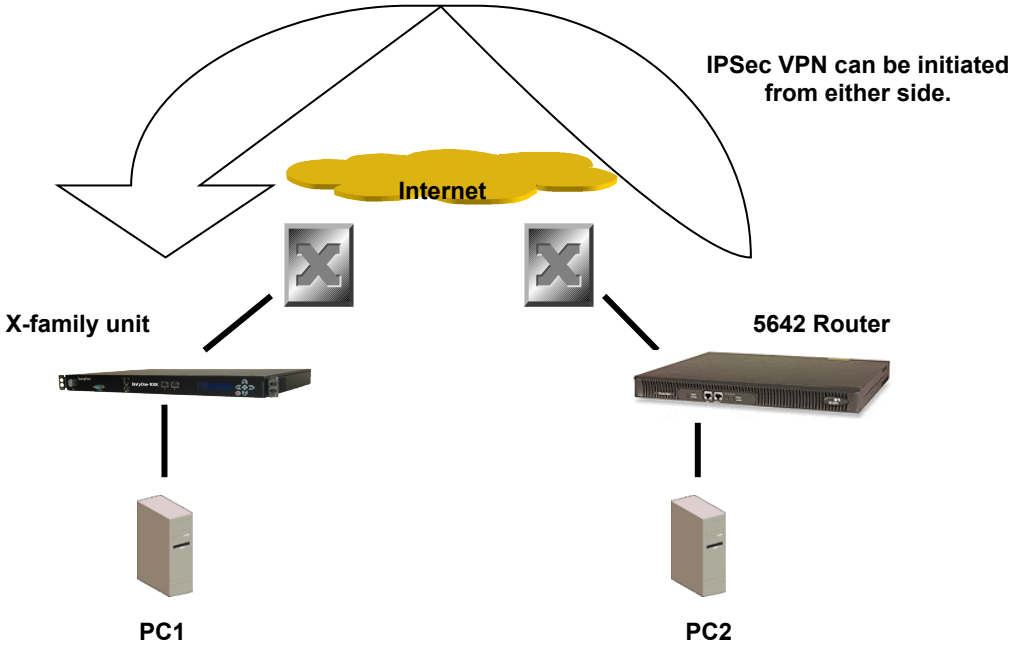
1. Unless the 5642 has a known IP address and can be accessed using Telnet or SSH, the initial setup must be started via a serial connection from PC2 to the Console port on the front of the Router.
2. Open a terminal emulator (e.g. Hyperterminal) on PC2 and set it to 9600 bps, 8 data bits, 1 stop bit, no parity and no flow control.
3. Hit <Return> on PC2 and login (if necessary).
4. You are now in user-view with an angle-bracket prompt like this:
   ```
   <3COM_ROUTER>
   ```
5. Type the following to get into system view
   ```
   system-view
   ```
6. You are now in system view with a square-bracket prompt:
   ```
   System View: return to User View with Ctrl+Z.
   [3COM_ROUTER]
   ```
7. We will use two Ethernet interfaces for the internal and external interfaces. First set up the internal interface by typing:
   ```
   interface Ethernet0/1
   ```
8. You are now in the view for this particular interface, prompt is:
   ```
   [3COM_ROUTER-Ethernet0/1]
   ```
9. Set the ip address by typing:
   ```
   ip address 192.168.22.254 255.255.255.0
   ```
   Then quit and do the same for the external interface:
   ```
   [3COM_ROUTER-Ethernet0/1]quit
   [3COM_ROUTER]interface Ethernet0/0
   [3COM_ROUTER-Ethernet0/0]ip address 10.10.10.147
   255.255.255.0
   [3COM_ROUTER-Ethernet0/0]quit
   [3COM_ROUTER]
   ```

Perform the following sequence of commands to save the configuration changes and to make the router load this configuration if it is rebooted or power cycled.

```
[3COM_ROUTER]save initial.cfg
The current configuration will be saved to flash:/initial.cfg
[Y/N]:y
Now saving current configuration to the device.
Saving configuration flash:/initial.cfg. Please wait...
.................
Current configuration has been saved to the device successfully.
[3COM_ROUTER]quit
<3COM_ROUTER>startup saved-configuration initial.cfg
Please wait ............. Done!
<3COM_ROUTER>
```

4 Configuring Main Mode GRE/IPSec Tunnel

This example shows how to configure a GRE/IPSec tunnel using Main Mode between the X-FAMILY and a 3Com 5642 Router. Main Mode is the recommended setting when both devices have static IP addresses that can be accessed from the public internet.

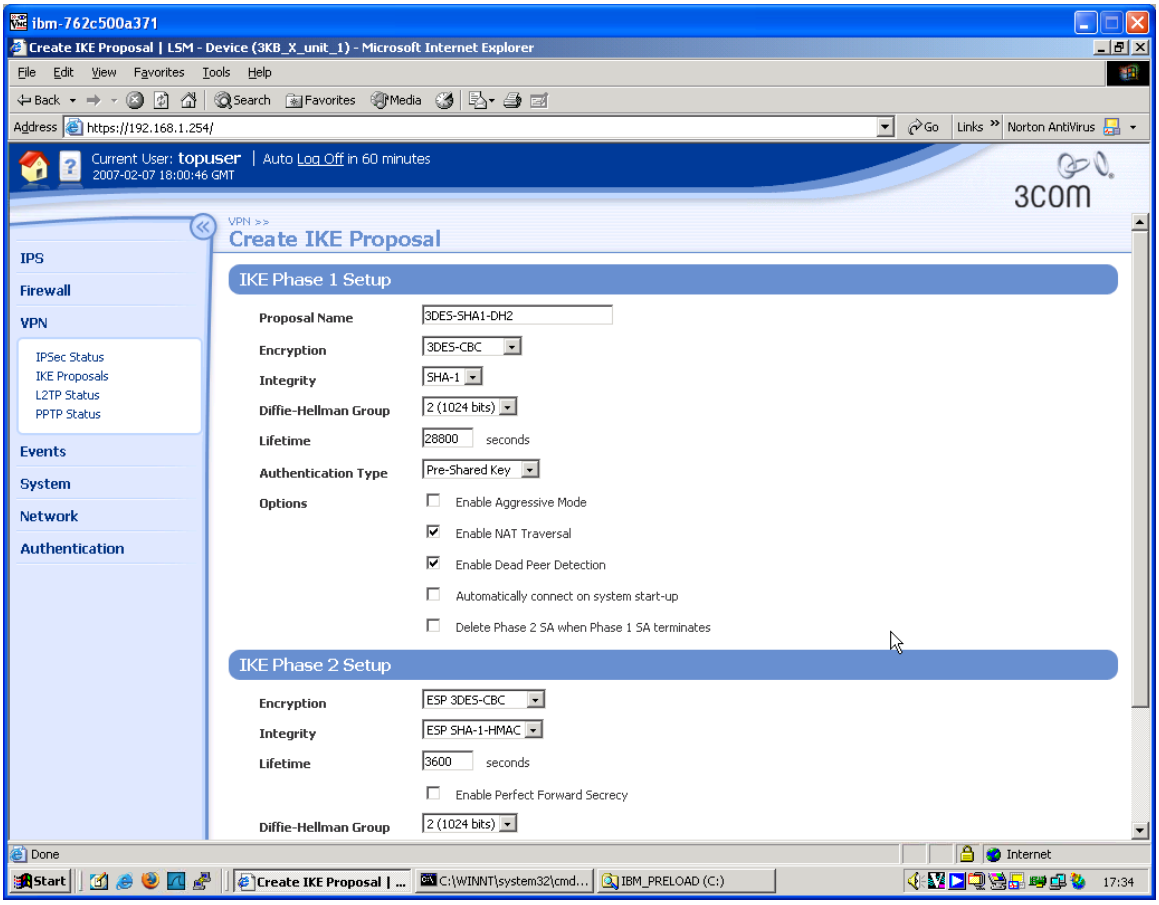


Key Setup Information

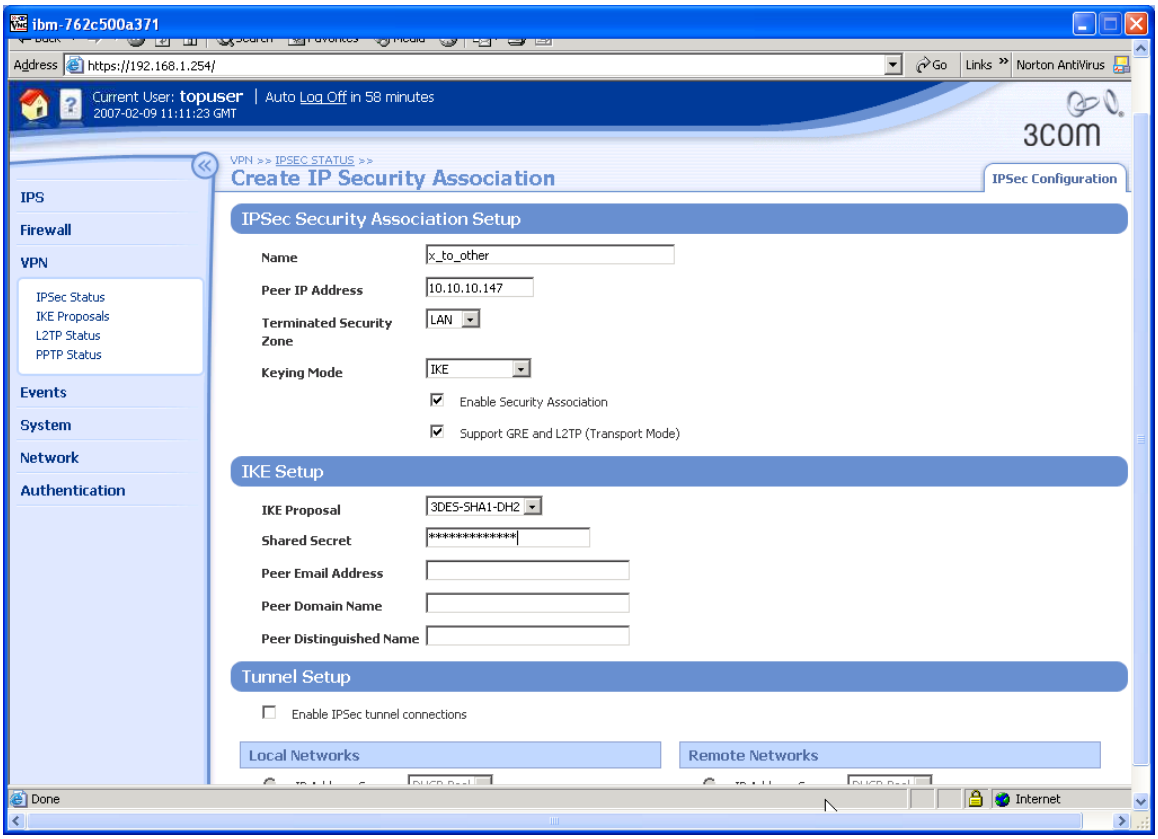
Keying Mode	IKE
IKE Mode	Main Mode
SA Authentication Method	Pre-shared Key
Keying Group DH	DH (Diffie Hellman) Group 2
Encryption and Data Integrity	3DES-SHA1

4.1 3Com X-FAMILY VPN Configuration

1. Open a browser on PC1, connect to https://192.168.1.254 and login as the user you set up during the OBE.
2. Navigate to VPN -> IKE Proposals. You will see one default proposal for DES-SHA1-PSK but we do not want to use this as it does not provide a suitably high level of security so click on the "Create IKE Proposal" button to create a new proposal. Complete the form that opens as shown below.

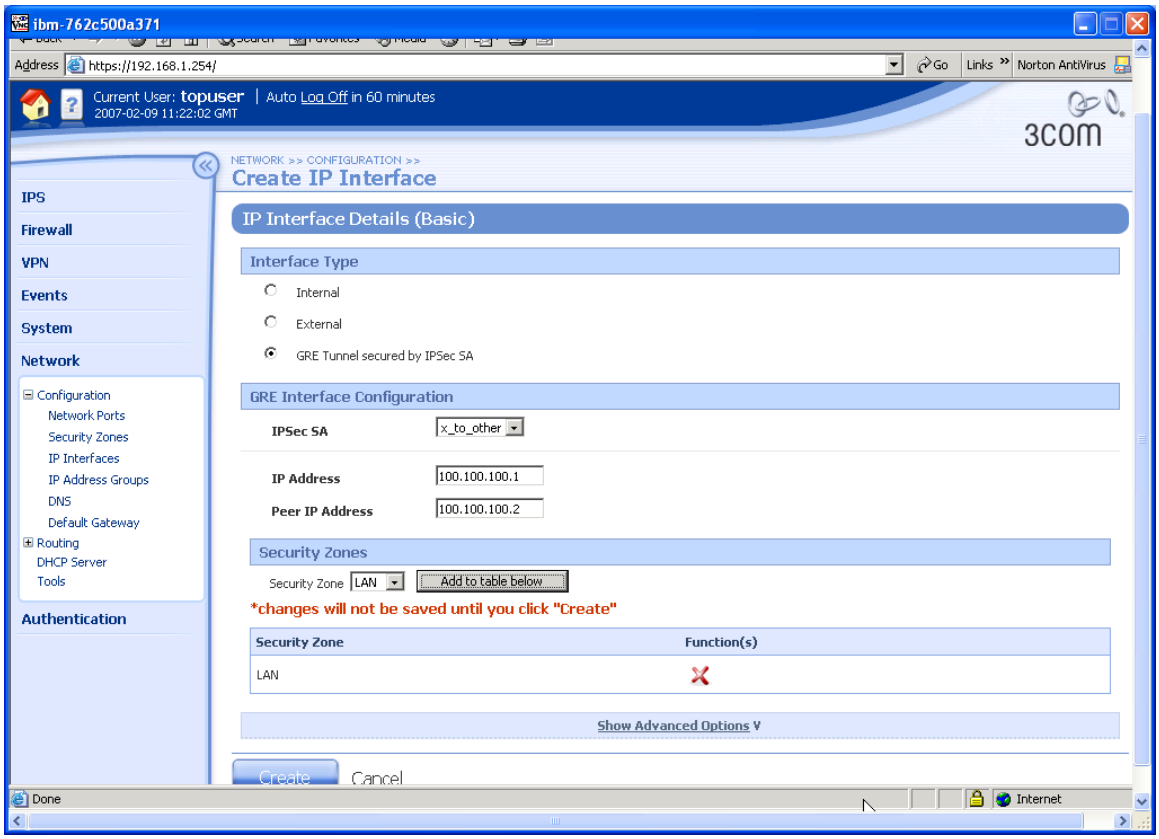


3. Click "Create" to save the new IKE Proposal.
4. Navigate to VPN -> IPSEC Status and click on the "IPSEC Configuration" tab.
5. Click the Enable IPSEC Global VPNs checkbox and click the Apply button.
6. On the IPSEC Configuration screen you will see one Security Association called "Default" displayed but we will not be using this as it is mainly used with IPSec clients on remote PCs, so click the Create IPSec Association button to create a new Security Association. Complete the form that opens as shown below. Note that this is a **transport** mode SA, and so the "Tunnel Setup" section of the screen is not applicable. Note also that the "Shared Secret" string entered here must be at least 8 characters and must be exactly the same as the shared secret entered on the peer device.

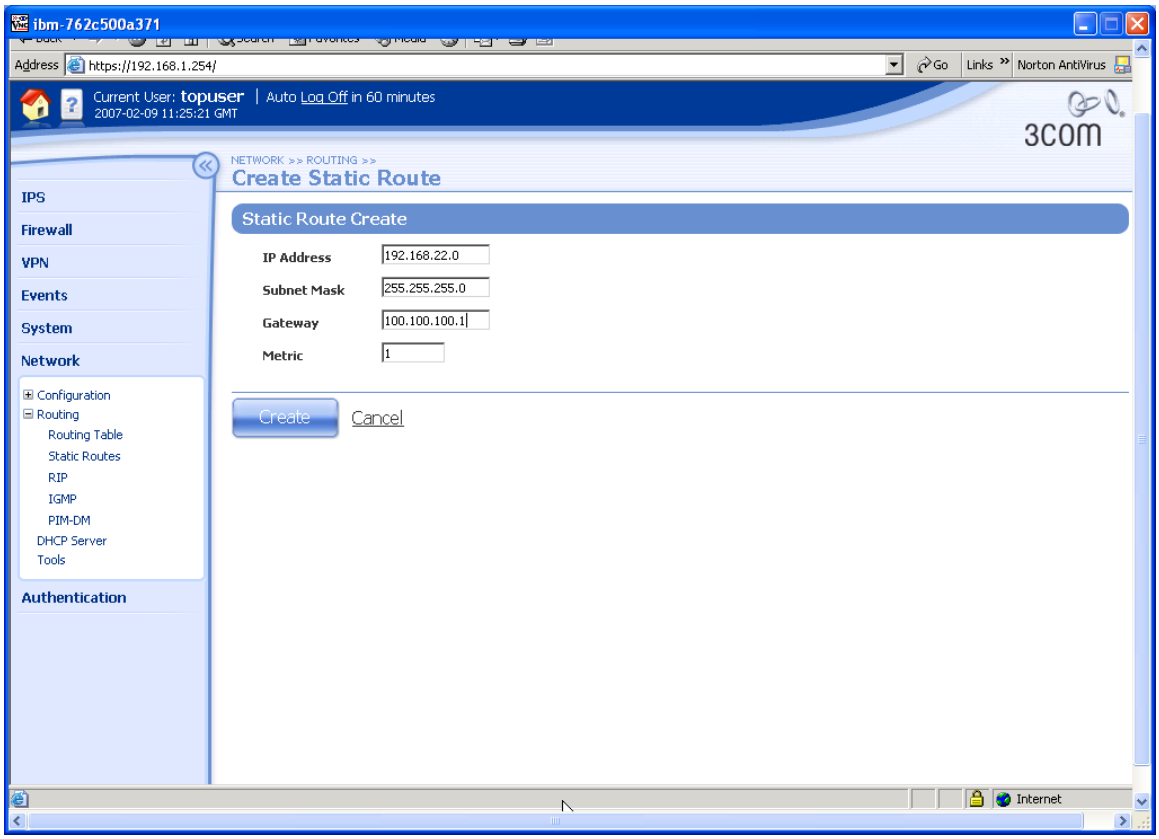


7. Click "Create" to save the new Security Association.
8. To create the GRE interface, navigate to Network->Configuration->IP Interfaces, click the button "Create IP Interface" and complete the form as shown below.
   Note that the "IP Address" and Peer "IP Address" are the addresses for the local and remote ends of the GRE tunnel respectively and they must:
   - be single host addresses (i.e. have an assumed mask of 255.255.255.255);
   - be different from each other;
   - not be used anywhere else in the wider routed network (as they will be used for routing and may appear in RIP/OSPF updates).

   The addresses must be reversed at the other end of the tunnel.



9. Click "Create" to create the new GRE Virtual Interface.
10. Now add a static route to 192.168.22.0/24 pointing down the GRE tunnel. Navigate to Network->Routing->Static Routes, click the button "Add Static Route" and complete the form as shown below.



11. Click the "Create" button to create the route.

4.2 3Com 5642 Router Configuration

We first need to set up an acl (Access Control List) to select the source and destination addresses that will communicate plus a default route and a static route to make sure that traffic gets sent over the correct interfaces. (Note that the subnet mask bits in the ACL rule are reversed – e.g. 0.0.0.255 instead of 255.255.255.0 for a Class C subnet).

1. Using direct console port connection, telnet or SSH, login to the 5642 Command Line Interface and perform the sequence of commands shown below:

```
<3COM_ROUTER>system-view
System View: return to User View with Ctrl+Z.
[3COM_ROUTER]acl number 3101
[3COM_ROUTER-acl-adv-3101]rule 1 permit ip source 10.10.10.147
0.0.0.0 destination 10.10.20.147 0.0.0.0
[3COM_ROUTER-acl-adv-3101]quit
[3COM_ROUTER]ip route-static 0.0.0.0 0.0.0.0 10.10.10.1 preference
60
[3COM_ROUTER]ip route-static 192.168.1.0 255.255.255.0 Tunnel 0
preference 20
[3COM_ROUTER]
```

Next we must create an ike (i.e. Phase 1) proposal.

2. Continue from 1 above and perform the following sequence of commands.

```
[3COM_ROUTER]ike proposal 1
[3COM_ROUTER-ike-proposal-1]encryption-algorithm 3des-cbc
[3COM_ROUTER-ike-proposal-1]dh group2
[3COM_ROUTER-ike-proposal-1]quit
[3COM_ROUTER]
```

Now an IPSec (Phase 2) proposal (N.B. transport mode).

3. Continue from 2 above and perform the following sequence of commands.

```
[3COM_ROUTER]ipsec proposal 3des-sha1
[3COM_ROUTER-ipsec-proposal-3des-sha1]encapsulation-mode transport
[3COM_ROUTER-ipsec-proposal-3des-sha1]esp authentication-algorithm
sha1
[3COM_ROUTER-ipsec-proposal-3des-sha1]esp encryption-algorithm
3des
[3COM_ROUTER-ipsec-proposal-3des-sha1]quit
[3COM_ROUTER]
```

Now an ike peer.

4. Continue from 3 above and perform the following sequence of commands.

```
[3COM_ROUTER]ike peer X
[3COM_ROUTER-ike-peer-X]exchange-mode main
[3COM_ROUTER-ike-peer-X]id-type ip
[3COM_ROUTER-ike-peer-X]pre-shared-key <shared-secret> * See Note
[3COM_ROUTER-ike-peer-X]remote-address 10.10.20.147
[3COM_ROUTER-ike-peer-X]local-address 10.10.10.147
[3COM_ROUTER-ike-peer-X]remote-name 10.10.20.147
```

```
[3COM_ROUTER-ike-peer-X]quit
[3COM_ROUTER]
```

* Note that the <shared-secret> string entered here must be at least 8 characters and must be exactly the same as the shared secret entered on the peer device.

Now we link them all together with an IPSec Policy…

5. Continue from 4 above and perform the following sequence of commands.

```
[3COM_ROUTER]ipsec policy test 1 isakmp
[3COM_ROUTER-ipsec-policy-isakmp-test-1]ike-peer X
[3COM_ROUTER-ipsec-policy-isakmp-test-1]proposal 3des-sha1
[3COM_ROUTER-ipsec-policy-isakmp-test-1]quit
[3COM_ROUTER]
```

…and attach the IPSec Policy to the external Ethernet interface…

6. Continue from 5 above and perform the following sequence of commands.

```
[3COM_ROUTER]interface Ethernet0/0
[3COM_ROUTER-Ethernet0/0]ipsec policy test
[3COM_ROUTER-Ethernet0/0]quit
[3COM_ROUTER]
```

…and add a GRE tunnel interface…

7. Continue from 6 above and perform the following sequence of commands.

```
[3COM_ROUTER]interface Tunnel 0
[3COM_ROUTER-Tunnel0]tunnel-protocol gre
[3COM_ROUTER-Tunnel0]destination 10.10.20.147
[3COM_ROUTER-Tunnel0]source 10.10.10.147
[3COM_ROUTER-Tunnel0]ip address 100.100.100.2 24
[3COM_ROUTER-Tunnel0]quit
[3COM_ROUTER]
```

…and add a static route to send traffic to 192.168.1.0 through the GRE tunnel

8. Continue from 7 above and perform the following command.

```
[3COM_ROUTER] ip route-static 192.168.1.0 255.255.255.0 Tunnel 0
preference 20
[3COM_ROUTER]
```

Finally save the configuration and make it load as default if the router is rebooted or power cycled. (Note we need to quit out of system-view into user-view to use the startup command).

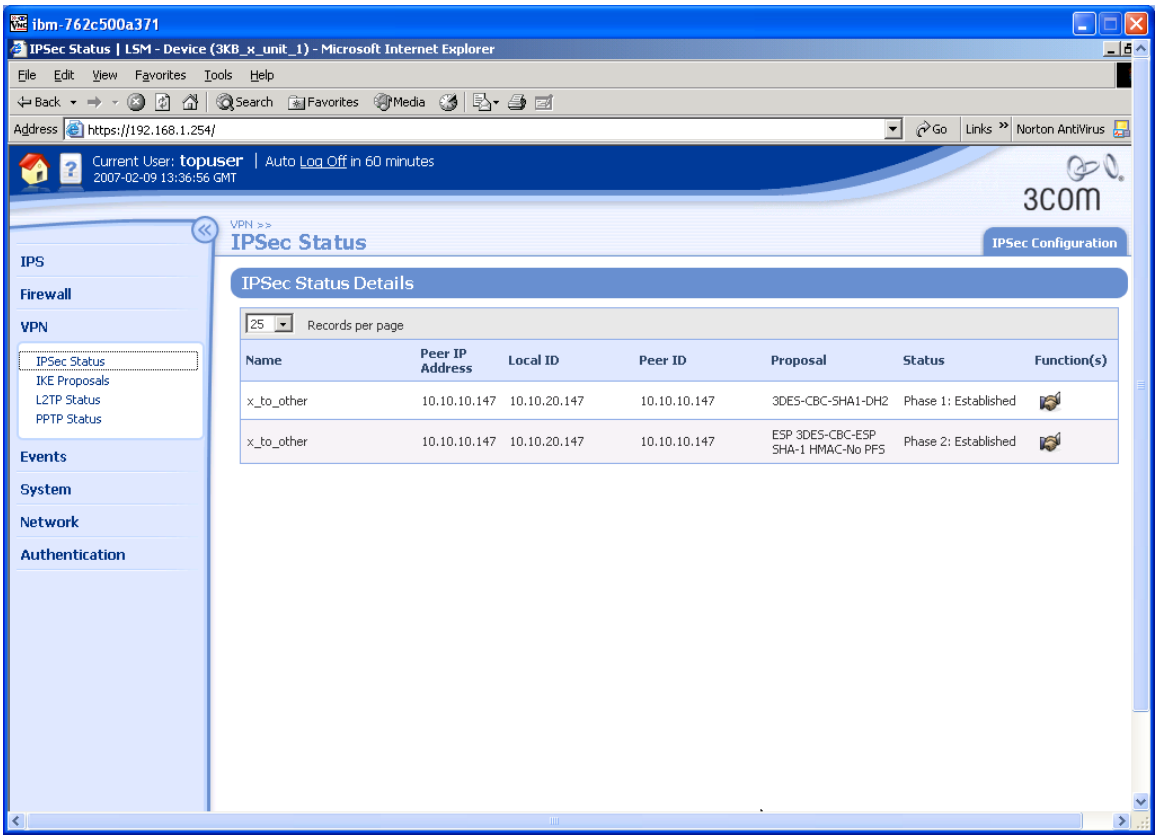
9. Continue from 5 above and perform the following sequence of commands.

```
[3COM_ROUTER]save main_gre.cfg
The current configuration will be saved to flash:/main_gre.cfg [Y/
N]:y
Now saving current configuration to the device.
Saving configuration flash:/main_gre.cfg. Please wait...
.................
Current configuration has been saved to the device successfully.
[3COM_ROUTER]quit
<3COM_ROUTER>startup saved-configuration main_gre.cfg
```

```
Please wait ............. Done!
<3COM_ROUTER>
```

4.3 Testing the VPN with data

1. Ping from PC1 to PC2 - this will bring up the IPSec SA which should look like this on the IPSec Status screen of the X-FAMILY device. One or two pings may be lost while the tunnel establishes but then all subsequent pings should be successful.



2. An additional check – to confirm that the traffic is actually going over the GRE tunnel – can be performed at the 5642 Router.Using direct console port connection, telnet or SSH, login to the 5642 Command Line Interface and perform the sequence of commands shown below:

```
<3COM_ROUTER>display interface Tunnel0
Tunnel0 current state :UP
Line protocol current state :UP
Description : Tunnel0 Interface
The Maximum Transmit Unit is 64000
Internet Address is 100.100.100.2/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.10.10.147, destination 10.10.20.147
Tunnel keepalive disable
Tunnel protocol/transport GRE/IP, key disabled
Checksumming of packets disabled
Output queue : (Urgent queuing : Size/Length/Discards)  0/50/0
Output queue : (Protocol queuing : Size/Length/Discards) 0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
```

```
    Last 300 seconds input:  1.12 bytes/sec, 0.01 packets/sec
    Last 300 seconds output:  1.12 bytes/sec, 0.01 packets/sec
    12 packets input,  1008 bytes
    0 input error
    18 packets output,  1512 bytes
    0 output error
```

3. Now ping PC1 from PC2 (or PC2 from PC1) and then rerun the above command. Both the "packets input" and "packets output" statistics should have incremented by the number of pings.

```
<3COM_ROUTER>display interface Tunnel0
Tunnel0 current state :UP
Line protocol current state :UP
Description : Tunnel0 Interface
The Maximum Transmit Unit is 64000
Internet Address is 100.100.100.2/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.10.10.147, destination 10.10.20.147
Tunnel keepalive disable
Tunnel protocol/transport GRE/IP, key disabled
Checksumming of packets disabled
Output queue : (Urgent queuing : Size/Length/Discards)  0/50/0
Output queue : (Protocol queuing : Size/Length/Discards) 0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
    Last 300 seconds input:  1.12 bytes/sec, 0.01 packets/sec
    Last 300 seconds output:  1.12 bytes/sec, 0.01 packets/sec
    16 packets input,  1344 bytes
    0 input error
    22 packets output,  1848 bytes
    0 output error
```

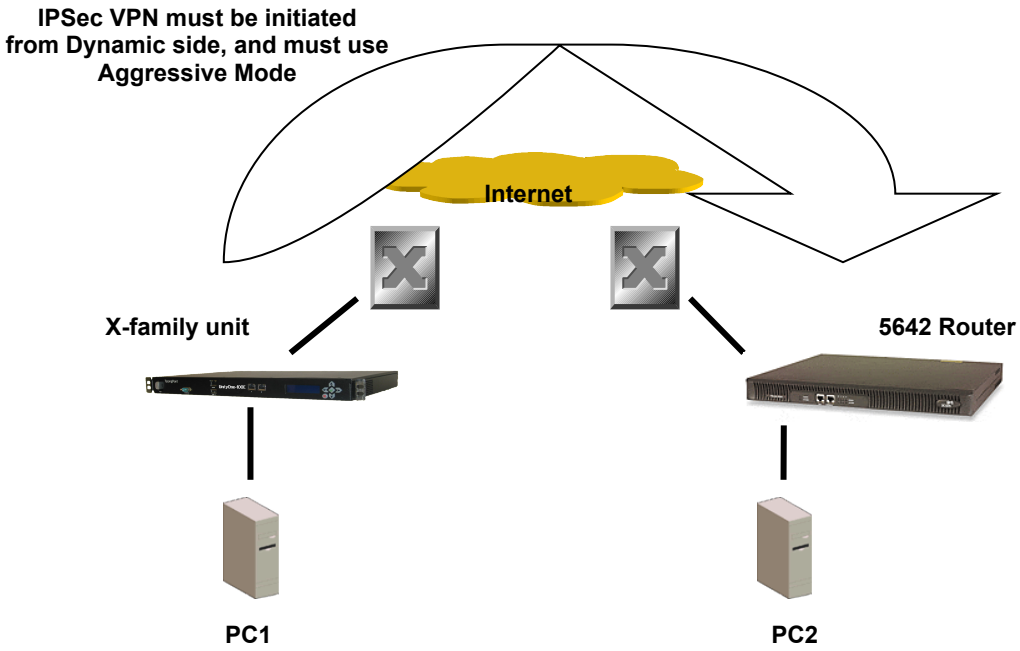
5 Aggressive Mode Tunnel

This example shows how to configure an IPSec tunnel using Aggressive Mode between the X-FAMILY and a 3Com 5642 Router. Aggressive Mode must be used when one side of the VPN tunnel has a variable (dynamic) WAN IP address. While Aggressive Mode can be used even if both sides have a Static WAN IP address, Main Mode is recommended as the tunnel will be more secure.

The X-family receives a dynamic IP address (through PPPoE, PPTP, DHCP or L2TP) from the Internet Service Provider. The x-family must initiate the VPN back to the 3Com Router, and the tunnel must use Aggressive Mode IKE.

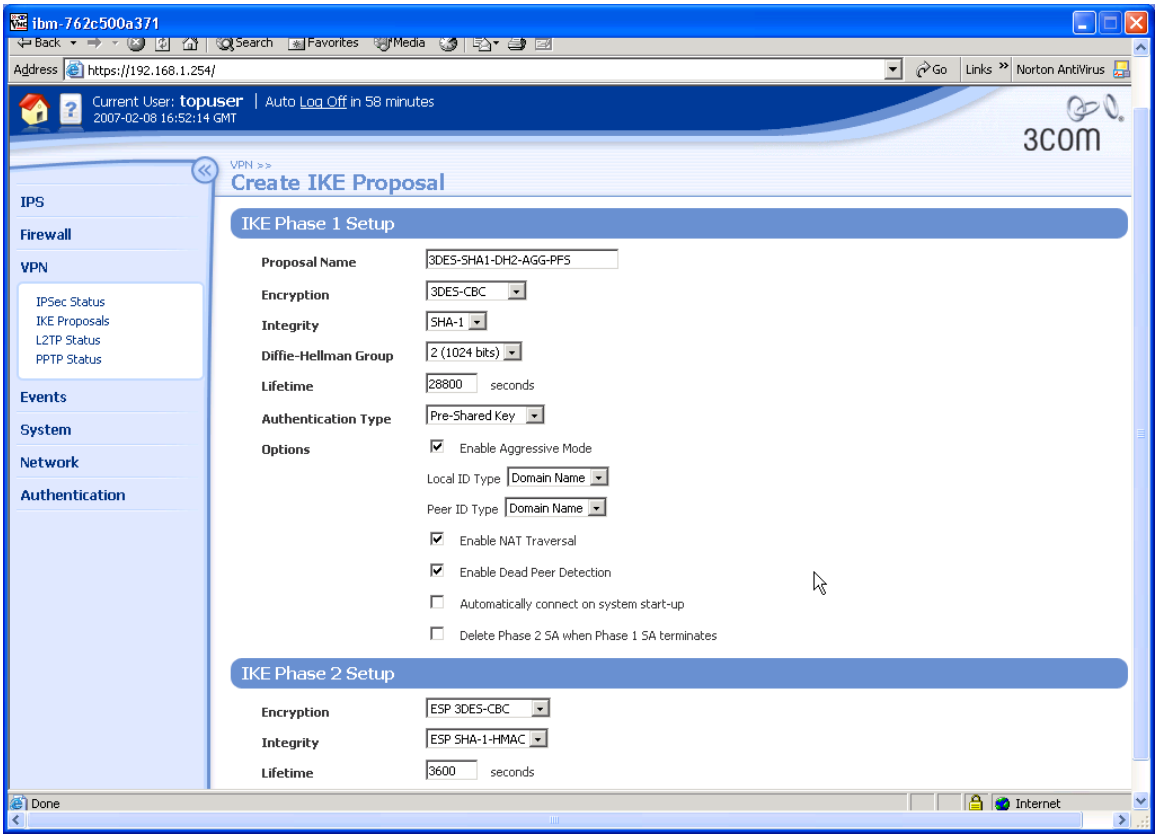
Key Setup Information

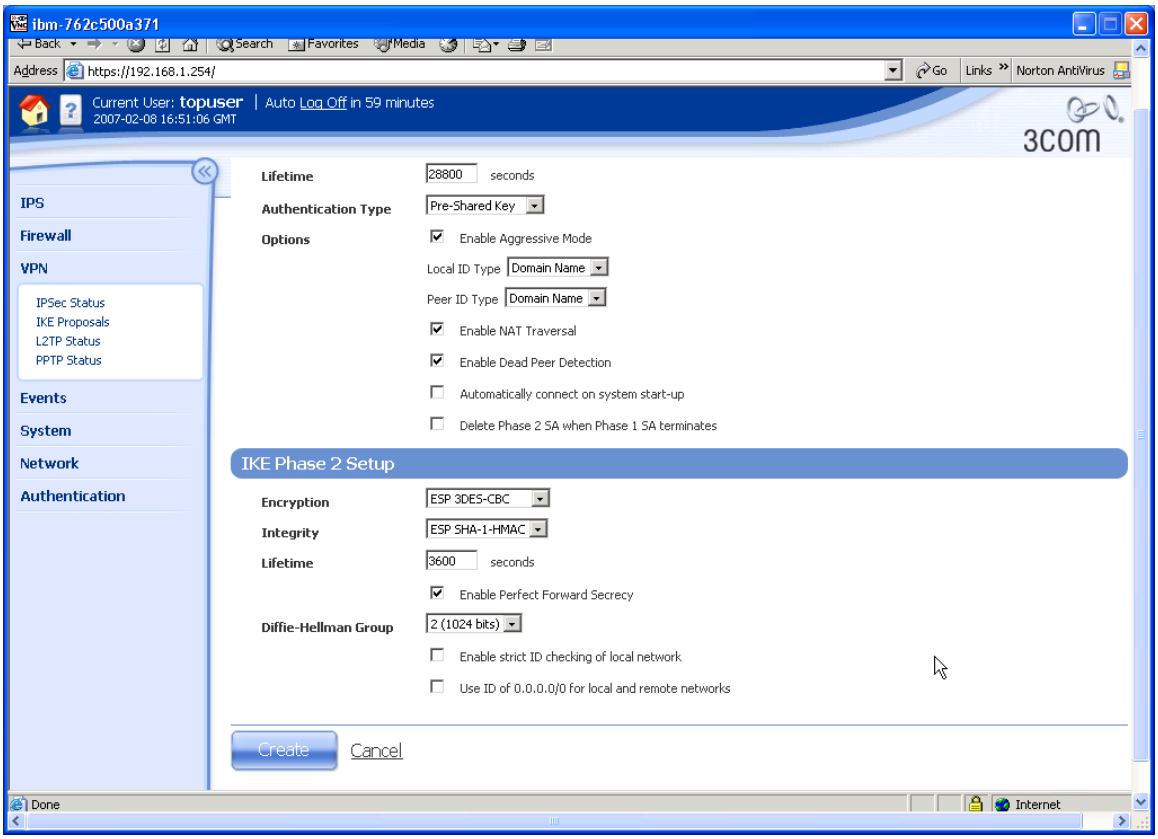
Keying Mode	IKE
IKE Mode	Aggressive Mode with Perfect Forward Secrecy
SA Authentication Method	Pre-shared Key
Keying Group DH	DH (Diffie Hellman) Group 2
Encryption and Data Integrity	3DES-SHA1



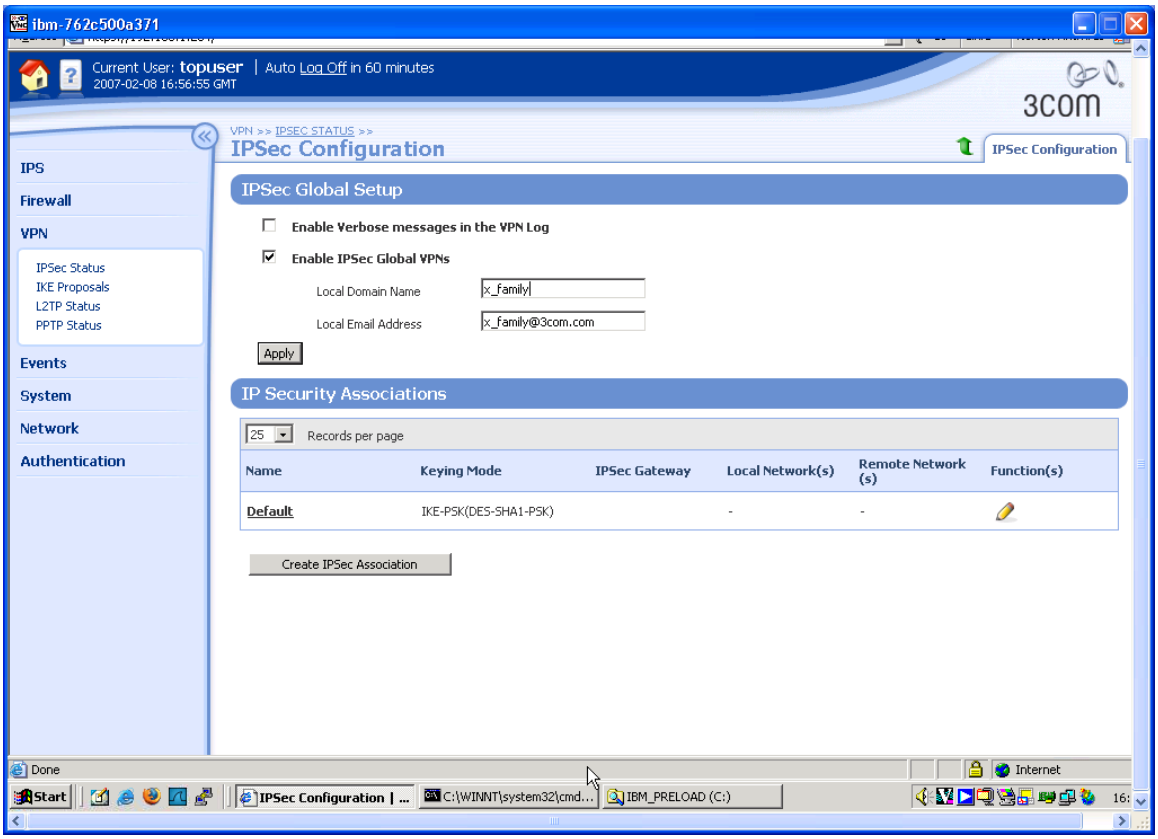
5.1 3Com X-FAMILY Configuration

1. Open a browser on PC1, connect to https://192.168.1.254 and login as the user you set up during the OBE.
2. Navigate to VPN -> IKE Proposals. You will see one default proposal for DES-SHA1-PSK but we do not want to use this as it does not provide a suitably high level of security so click on the "Create IKE Proposal" button to create a new proposal. Complete the form that opens as shown below. (There are two screenshots as the form is too large to fit on a single screen).

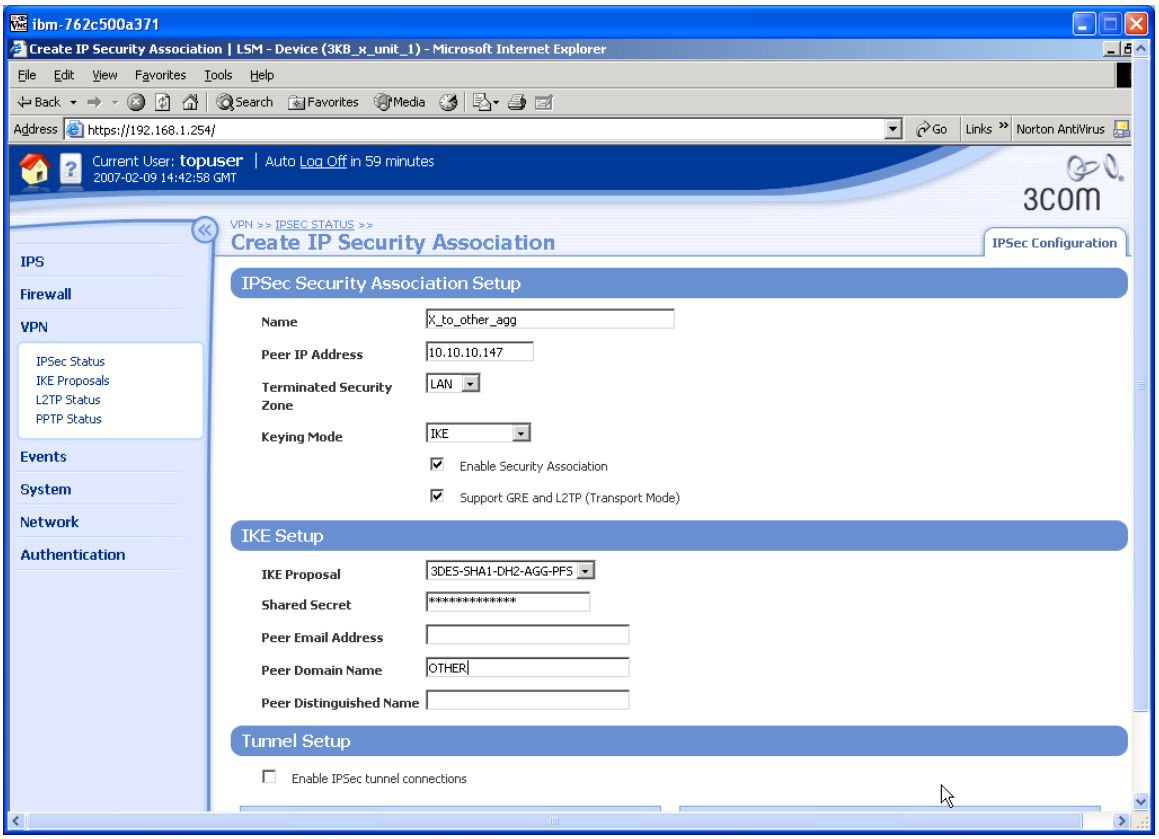




3. Click “Create” to save the new IKE Proposal.
4. Navigate to VPN -> IPSEC Status and click on the “IPSEC Configuration” tab.
5. Configure the upper part of the screen as shown below.

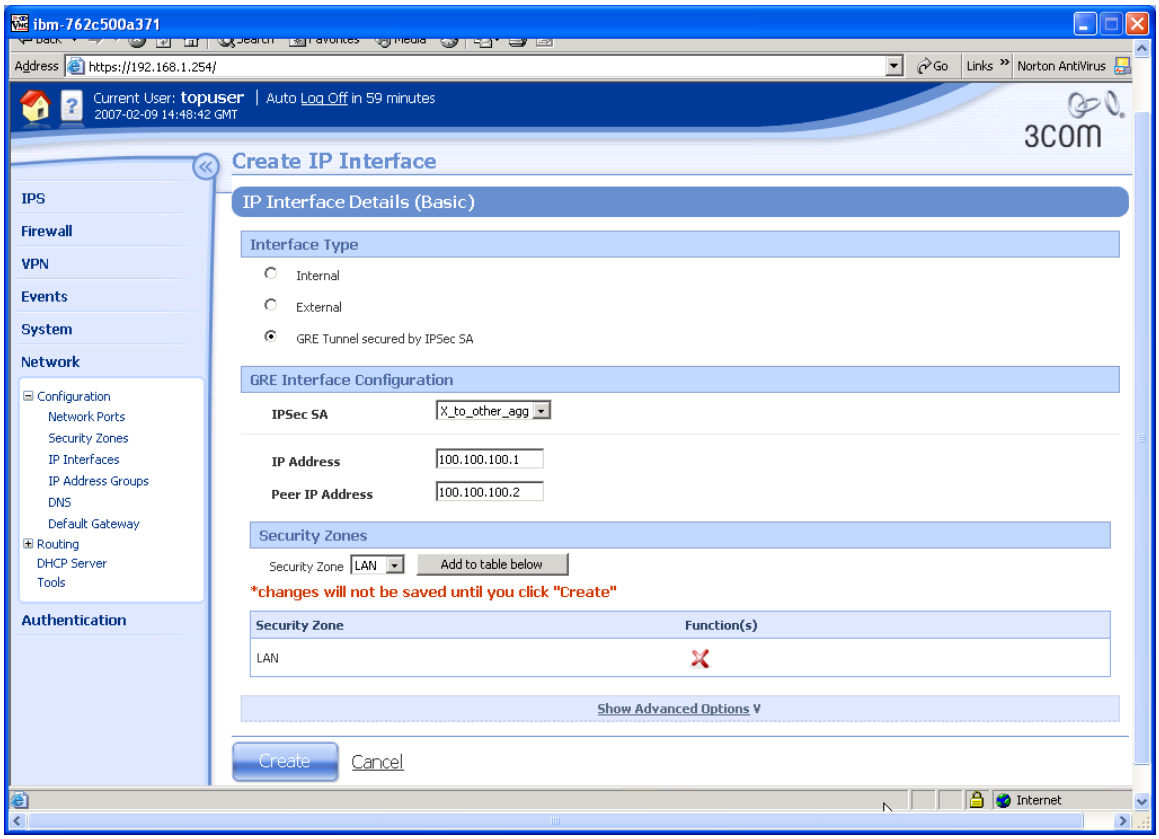


6. Click the Apply button to save the changes.
7. On the IPSEC Configuration screen you will see one Security Association called "Default" displayed but we will not be using this as it is mainly used with IPSec clients on remote PCs, so click the Create IPSec Association button to create a new Security Association. Complete the form that opens as shown below. Note that this is a transport mode SA so the "Tunnel Setup" part of the form is not applicable. Note also that the "Shared Secret" string entered here must be at least 8 characters and must be exactly the same as the shared secret entered on the peer device.

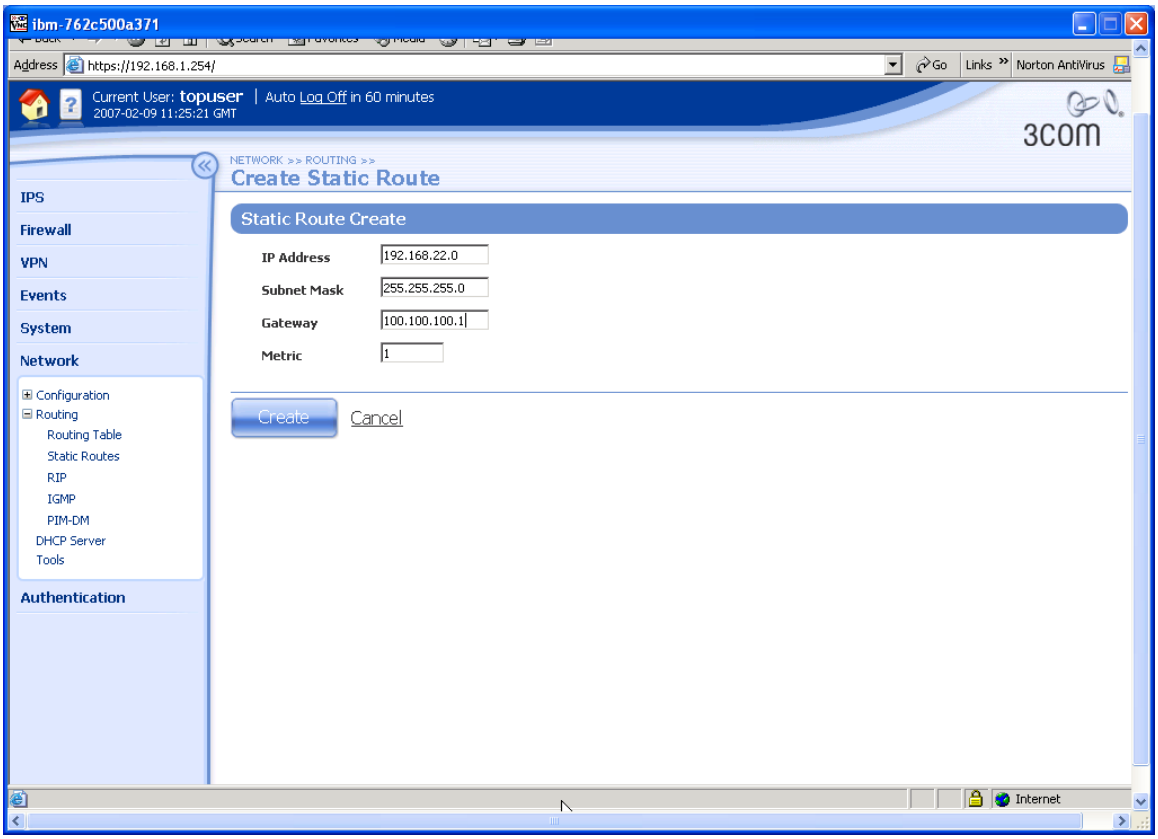


8. Click "Create" to create the Security Association.
9. To create the GRE interface, navigate to Network->Configuration->IP Interfaces, click the button "Create IP Interface" and complete the form as shown below.
   Note that the "IP Address" and Peer "IP Address" are the addresses for the local and remote ends of the GRE tunnel respectively and they must:
   - be single host addresses (i.e. have an assumed mask of 255.255.255.255);
   - be different from each other;
   - not be used anywhere else in the wider routed network (as they will be used for routing and may appear in RIP/OSPF updates).

   The addresses must be reversed at the other end of the tunnel.



10. Click “Create” to create the new GRE Virtual Interface.
11. Now add a static route to 192.168.22.0/24 pointing down the GRE tunnel. Navigate to Network->Routing->Static Routes, click the button “Add Static Route” and complete the form as shown below



12. Click the "Create" button to create the route.

5.2 3Com 5642 Router Configuration

We first need to set up an acl (Access Control List) to select the source and destination addresses that will communicate plus a default route to make sure that traffic gets sent over the correct interface. (Note that the subnet mask bits in the ACL rule are reversed – e.g. 0.0.0.255 instead of 255.255.255.0 for a Class C subnet).

1. Using direct console port connection, telnet or SSH, login to the 5642 Command Line Interface and perform the sequence of commands shown below:

```
<3COM_ROUTER>system-view
System View: return to User View with Ctrl+Z.
[3COM_ROUTER]acl number 3101
[3COM_ROUTER-acl-adv-3101]rule 1 permit ip source 10.10.10.147
0.0.0.0 destination 10.10.20.147 0.0.0.0
[3COM_ROUTER-acl-adv-3101]quit
[3COM_ROUTER]ip route-static 0.0.0.0 0.0.0.0 10.10.10.1 preference
60
[3COM_ROUTER]
```

Next we must create an ike (i.e. Phase 1) proposal.

2. Continue from 1 above and perform the following sequence of commands.

```
[3COM_ROUTER]ike proposal 1
[3COM_ROUTER-ike-proposal-1]encryption-algorithm 3des-cbc
[3COM_ROUTER-ike-proposal-1]dh group2
[3COM_ROUTER-ike-proposal-1]quit
[3COM_ROUTER]
```

Now an IPSec (Phase 2) proposal (N.B. transport mode).

3. Continue from 2 above and perform the following sequence of commands.

```
[3COM_ROUTER]ipsec proposal 3des-sha1
[3COM_ROUTER-ipsec-proposal-3des-sha1]encapsulation-mode transport
[3COM_ROUTER-ipsec-proposal-3des-sha1]esp authentication-algorithm
sha1
[3COM_ROUTER-ipsec-proposal-3des-sha1]esp encryption-algorithm
3des
[3COM_ROUTER-ipsec-proposal-3des-sha1]quit
[3COM_ROUTER]
```

Now an ike peer.

4. Continue from 3 above and perform the following sequence of commands.

```
[3COM_ROUTER]ike peer X
[3COM_ROUTER-ike-peer-X]exchange-mode aggressive
[3COM_ROUTER-ike-peer-X]id-type name
[3COM_ROUTER-ike-peer-X]remote-name x-family
[3COM_ROUTER-ike-peer-X]pre-shared-key <shared-secret> * See Note
(1)
[3COM_ROUTER-ike-peer-X]undo remote-address * See Note (2)
[3COM_ROUTER-ike-peer-X]local-address 10.10.10.147
[3COM_ROUTER-ike-peer-X]quit
[3COM_ROUTER]
```

Note (1) that the <shared-secret> string entered here must be at least 8 characters and must be exactly the same as the shared secret entered on the peer device.
Note (2) This command will only be required if a remote-address has been entered for this ike peer before (i.e. if the main mode configuration in the first part of this document is being amended into an aggressive mode configuration).

…and a sysname that will be used as domain name for this end of the tunnel.

5. Continue from 4 above and perform the following sequence of commands.

```
[3COM_ROUTER]sysname OTHER
[OTHER]
```

Now we link them all together with an IPSec Policy and set PFS…

6. Continue from 5 above and perform the following sequence of commands.

```
[OTHER]ipsec policy test 1 isakmp
[OTHER-ipsec-policy-isakmp-test-1]security acl 3101
[OTHER-ipsec-policy-isakmp-test-1]ike-peer X
[OTHER-ipsec-policy-isakmp-test-1]proposal 3des-sha1
[OTHER-ipsec-policy-isakmp-test-1]pfs dh-group2
[OTHER-ipsec-policy-isakmp-test-1]quit
[OTHER]
```

…and attach the IPSec Policy to the external interface.

7. Continue from 6 above and perform the following sequence of commands.

```
[OTHER]interface Ethernet0/0
[OTHER-Ethernet0/0]ipsec policy test
[OTHER-Ethernet0/0]quit
[OTHER]
```

…and add a GRE tunnel interface…

8. Continue from 7 above and perform the following sequence of commands.

```
[OTHER]interface Tunnel 0
[OTHER-Tunnel0]tunnel-protocol gre
[OTHER-Tunnel0]destination 10.0.0.146
[OTHER-Tunnel0]source 10.0.0.147
[OTHER-Tunnel0]ip address 100.100.100.2 24
[OTHER-Tunnel0]quit
[OTHER]
```

…and add a static route to send traffic to 192.168.1.0 through the GRE tunnel

9. Continue from 7 above and perform the following command.

```
[OTHER] ip route-static 192.168.1.0 255.255.255.0 Tunnel 0
preference 20
[OTHER]
```

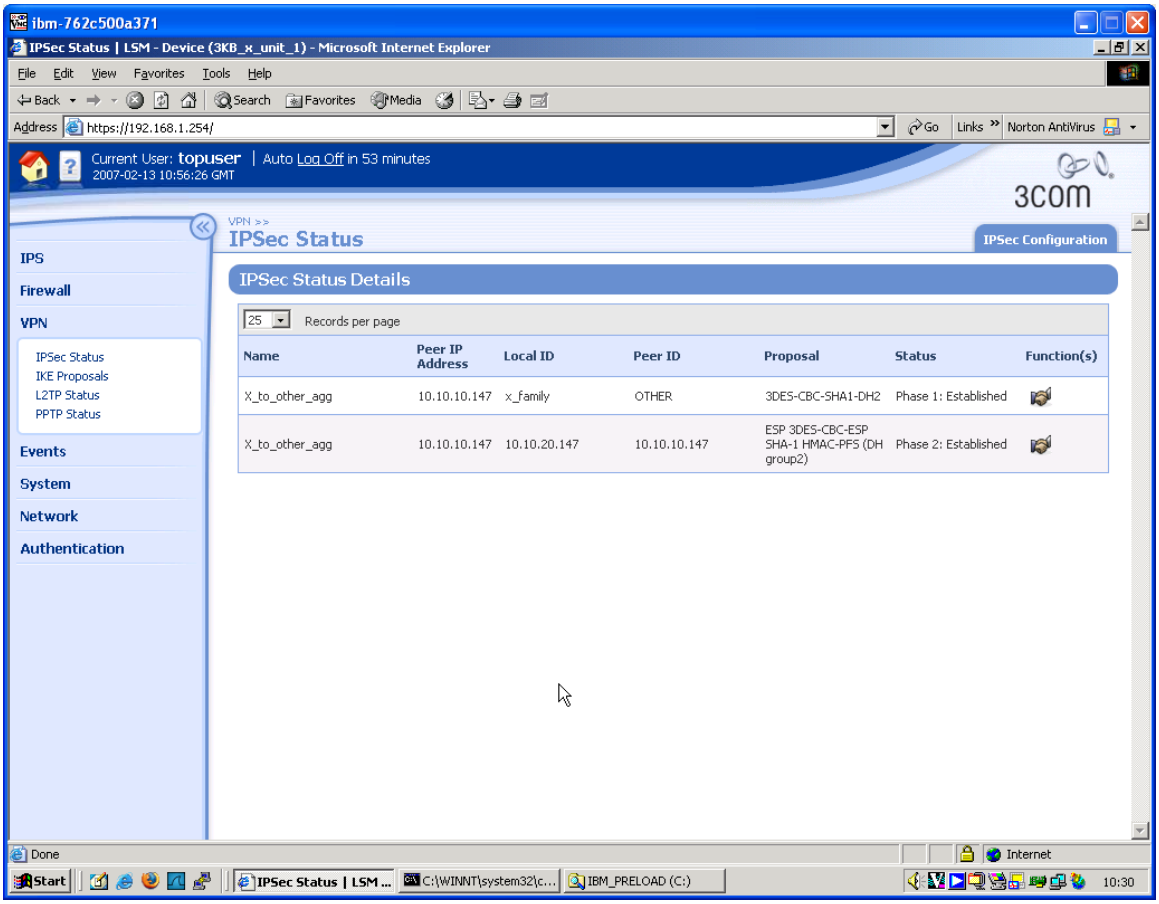
Finally save the configuration and make it load as default if the router is rebooted or power cycled. (Note we need to quit out of system-view into user-view to use the startup command).

10. Continue from 6 above and perform the following sequence of commands.

```
[OTHER]save agg_gre.cfg
The current configuration will be saved to flash:/agg_gre.cfg
[Y/N]:y
Now saving current configuration to the device.
Saving configuration flash:/agg_gre.cfg. Please wait...
..................
Current configuration has been saved to the device successfully.
[OTHER]quit
<OTHER>startup saved-configuration agg_gre.cfg
Please wait ............. Done!
<OTHER>
```

5.3 Testing the VPN with data

1. Ping from PC1 to PC2 - this will bring up the tunnel which should look like this on the IPSec Status screen of the X-FAMILY device. One or two pings may be lost while the tunnel establishes but then all subsequent pings should be successful. N.B. The direction of the initial ping (PC1 to PC2) is important as the X-family must be the initiator of the VPN connection. This is because the IP address of the X-family is not known to the 3Com Router device.



2. An additional check – to confirm that the traffic is actually going over the GRE tunnel – can be performed at the 5642 Router.

Using direct console port connection, telnet or SSH, login to the 5642 Command Line Interface and perform the sequence of commands shown below:

```
<OTHER>display interface Tunnel 0
Tunnel0 current state :UP
Line protocol current state :UP
Description : Tunnel0 Interface
The Maximum Transmit Unit is 64000
Internet Address is 100.100.100.2/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.10.10.147, destination 10.10.20.147
Tunnel keepalive disable
```

```
Tunnel protocol/transport GRE/IP, key disabled
Checksumming of packets disabled
Output queue : (Urgent queuing : Size/Length/Discards)  0/50/0
Output queue : (Protocol queuing : Size/Length/Discards) 0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
   Last 300 seconds input:  0.00 bytes/sec, 0.00 packets/sec
   Last 300 seconds output:  0.00 bytes/sec, 0.00 packets/sec
   18 packets input,  1512 bytes
   0 input error
   24 packets output,  2016 bytes
   0 output error
```

3. Now ping PC1 from PC2 (or PC2 from PC1) and then rerun the above command. Both the "packets input" and "packets output" statistics should have incremented by the number of pings.

```
<OTHER>display interface Tunnel 0
Tunnel0 current state :UP
Line protocol current state :UP
Description : Tunnel0 Interface
The Maximum Transmit Unit is 64000
Internet Address is 100.100.100.2/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.10.10.147, destination 10.10.20.147
Tunnel keepalive disable
Tunnel protocol/transport GRE/IP, key disabled
Checksumming of packets disabled
Output queue : (Urgent queuing : Size/Length/Discards)  0/50/0
Output queue : (Protocol queuing : Size/Length/Discards) 0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
   Last 300 seconds input:  0.00 bytes/sec, 0.00 packets/sec
   Last 300 seconds output:  0.00 bytes/sec, 0.00 packets/sec
   22 packets input,  1848 bytes
   0 input error
   28 packets output,  2352 bytes
   0 output error

<OTHER>
```

6 Appendix – Configuration Files

Here are textual configuration files for both devices for reference purposes.

6.1 Main Mode

6.1.1 "show conf" file for X-family device

```
3KB_x_unit_1# show conf
interface ethernet 3 1
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface ethernet 3 2
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface ethernet 3 3
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface ethernet 3 4
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface ethernet 3 5
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface ethernet 3 6
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface settings poll-interval 2000
interface settings detect-mdi enable
interface settings mdi-mode mdix
host name "3KB_x_unit_1"
host location "Lab"
host ip-filter permit any icmp
host ip-filter permit any ip
no autodv
user options max-attempts   5
user options expire-period  90
```

```
user options expire-action  expire
user options lockout-period 5
user options attempt-action lockout
user options security-level 2
high-availability disable
high-availability heartbeat 4 100 2
high-availability id 4098
clock timezone GMT
clock dst
log audit select general
log audit select login
log audit select logout
log audit select user
log audit select time
log audit select policy
log audit select update
log audit select boot
log audit select report
log audit select host
log audit select configuration
log audit select oam
log audit select sms
log audit select server
log audit select segment
log audit select high-availability
log audit select monitor
log audit select ip-filter
log audit select conn-table
log audit select host-communication
log audit select tse
category-settings -profile "Default Security Profile" vulnerabilities
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" exploits
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" security-policy
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" reconnaissance
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" virus
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" spyware
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" identity-theft
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" traffic-normal
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" network-equipment
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" p2p
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" im
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" streaming-media
enable - action-set "Recommended"
notify-contact "Management Console" 1
notify-contact "Remote System Log" 1
default-alert-sink period 1
```

```
server ssh
server no http
server https
server browser-check
monitor threshold memory      -major  90 -critical  95
monitor threshold disk        -major  90 -critical  95
monitor threshold temperature -major  92 -critical  94
monitor disable power-supply
no service-access
tse adaptive-filter mode automatic
tse afc-severity warning
tse connection-table timeout 1800
tse logging-mode conditional -threshold 1.0 -period 600
tse quarantine duration 60
email-rate-limit 10
zone update LAN vlan-id 1
zone update LAN port 3/1
zone update LAN mtu 1500
zone update LAN addresses disable
zone update LAN vpn-tunnel-access enable
zone update VPN vlan-id 4
zone update VPN port none
zone update VPN mtu 1500
zone update VPN addresses disable
zone update VPN vpn-tunnel-access enable
zone update WAN vlan-id 3
zone update WAN port 3/6
zone update WAN mtu 1500
zone update WAN addresses disable
zone update WAN vpn-tunnel-access enable
address-groups update DHCP-Pool range 192.168.1.1 192.168.1.20
authentication privilege-groups update Allow_VPN_access vpn-client-
access
authentication privilege-groups update RADIUS
authentication radius default-privilege-group RADIUS
authentication radius server primary 0.0.0.0 port 1812 shared-secret
******** auth-method chap
authentication radius server secondary none
authentication radius disable
authentication radius user-authentication enable
authentication radius vpn-clients enable
authentication radius retries 3
authentication radius timeout 2
web-filtering default-rule block
web-filtering filter-action block-and-log
web-filtering filter-service cache expiry 24
web-filtering filter-service cache size 2097152
web-filtering filter-service block adult
web-filtering filter-service block gambling
web-filtering filter-service block violence
web-filtering filter-service block criminal
web-filtering filter-service block hacking
web-filtering filter-service block weapons
web-filtering filter-service block drugs
web-filtering filter-service block hate
web-filtering filter-service permit advertisement
web-filtering filter-service permit computing
```

```
web-filtering filter-service permit food
web-filtering filter-service permit politics
web-filtering filter-service permit hosting
web-filtering filter-service permit lifestyle
web-filtering filter-service permit dating
web-filtering filter-service permit reference
web-filtering filter-service permit sex-education
web-filtering filter-service permit sports
web-filtering filter-service permit usenet
web-filtering filter-service permit arts
web-filtering filter-service permit education
web-filtering filter-service permit games
web-filtering filter-service permit health
web-filtering filter-service permit careers
web-filtering filter-service permit vehicles
web-filtering filter-service permit photos
web-filtering filter-service permit religion
web-filtering filter-service permit search
web-filtering filter-service permit streaming-media
web-filtering filter-service permit email
web-filtering filter-service permit chat
web-filtering filter-service permit finance
web-filtering filter-service permit glamour
web-filtering filter-service permit hobbies
web-filtering filter-service permit kids
web-filtering filter-service permit news
web-filtering filter-service permit real-estate
web-filtering filter-service permit proxies
web-filtering filter-service permit shopping
web-filtering filter-service permit travel
web-filtering filter-service disable
web-filtering manual-filter disable
dhcp-server addresses group DHCP-Pool
dhcp-server enable
dhcp-server bootp disable
dhcp-server lease-duration 60
dhcp-server dns default
dhcp-server wins primary 0.0.0.0
dhcp-server wins secondary 0.0.0.0
dhcp-server nbx 0.0.0.0
dhcp-server relay disable
dns use-external-dns enable
interface virtual add 1 internal
interface virtual internal 1 ip 192.168.1.254 netmask 255.255.255.0
interface virtual internal 1 ha-mgmt-ip 0.0.0.0
interface virtual internal 1 nat external-ip
interface virtual internal 1 rip disable
interface virtual internal 1 rip send-mode v2-multicast
interface virtual internal 1 rip receive-mode all
interface virtual internal 1 rip auth disable
interface virtual internal 1 rip split-horizon enable
interface virtual internal 1 rip poison-reverse enable
interface virtual internal 1 rip advertise-routes enable
interface virtual internal 1 igmp disable
interface virtual internal 1 pim-dm disable
interface virtual internal 1 zone add LAN
interface virtual internal 1 zone add VPN
```

```
interface virtual add 2 external
interface virtual external 2 type static 10.10.20.147 netmask
255.255.255.0
interface virtual external 2 ha-mgmt-ip 0.0.0.0
interface virtual external 2 rip disable
interface virtual external 2 rip send-mode v2-multicast
interface virtual external 2 rip receive-mode all
interface virtual external 2 rip auth disable
interface virtual external 2 rip split-horizon enable
interface virtual external 2 rip poison-reverse enable
interface virtual external 2 rip advertise-routes disable
interface virtual external 2 igmp disable
interface virtual external 2 pim-dm disable
interface virtual external 2 zone add WAN
interface virtual add 3 gre
interface virtual gre 3 local-ip 100.100.100.1
interface virtual gre 3 peer-ip 100.100.100.2
interface virtual gre 3 sa x_to_other
interface virtual gre 3 rip disable
interface virtual gre 3 rip send-mode disable
interface virtual gre 3 rip receive-mode disable
interface virtual gre 3 rip auth disable
interface virtual gre 3 rip split-horizon disable
interface virtual gre 3 rip poison-reverse disable
interface virtual gre 3 rip advertise-routes enable
interface virtual gre 3 igmp disable
interface virtual gre 3 pim-dm disable
interface virtual gre 3 zone add LAN
default-gateway 10.10.20.1
firewall schedule update working-day days -mtwtf- from 0800 to 1800
firewall service update 3com-nbx udp port 2093 to 2096
firewall service update audio-call-control tcp port 1731
firewall service update dhcp-client udp port 68
firewall service update dhcp-server udp port 67
firewall service update dns-tcp tcp port 53
firewall service update dns-udp udp port 53
firewall service update finger-tcp tcp port 79
firewall service update ftp tcp port 21
firewall service update gopher-tcp tcp port 70
firewall service update gre gre
firewall service update h323 tcp port 1720
firewall service update http tcp port 80
firewall service update https tcp port 443
firewall service update igmp igmp
firewall service update ike udp port 500
firewall service update imap tcp port 143
firewall service update imapv3 tcp port 220
firewall service update ipsec-ah ah
firewall service update ipsec-esp esp
firewall service update kerberos-tcp tcp port 88
firewall service update kerberos-udp udp port 88
firewall service update l2tp udp port 1701
firewall service update ldap-tcp tcp port 389
firewall service update ldap-udp udp port 389
firewall service update lotus-notes-domino tcp port 1352
firewall service update lpr tcp port 515
firewall service update nat-t-ipsec udp port 4500
```

```
firewall service update nbname tcp port 137
firewall service update netbios-tcp tcp port 137 to 139
firewall service update netbios-udp udp port 137 to 139
firewall service update netmeeting tcp port 1720
firewall service update nfsd-tcp tcp port 2049
firewall service update nfsd-udp udp port 2049
firewall service update nntp tcp port 119
firewall service update ntp udp port 123
firewall service update pim-dm pim
firewall service update ping icmp port 8
firewall service update pop3 tcp port 110
firewall service update portmapper-tcp tcp port 111
firewall service update portmapper-udp udp port 111
firewall service update pptp-tcp tcp port 1723
firewall service update radius-accounting udp port 1813
firewall service update radius-auth udp port 1812
firewall service update rexec tcp port 512
firewall service update rip udp port 520
firewall service update rlogin tcp port 513
firewall service update rsh tcp port 514
firewall service update rtsp tcp port 554
firewall service update sip-tcp tcp port 5060
firewall service update sip-udp udp port 5060
firewall service update smb tcp port 445
firewall service update sms-client tcp port 10042
firewall service update sms-trap tcp port 8162 to 8163
firewall service update smtp tcp port 25
firewall service update snmp-request udp port 161
firewall service update snmp-trap udp port 162
firewall service update ssh tcp port 22
firewall service update syslog udp port 514
firewall service update t120 tcp port 1503
firewall service update telnet tcp port 23
firewall service update tftp udp port 69
firewall service update traceroute icmp port 8
firewall service update uucp udp port 540
firewall service update vnc-browser tcp port 5800
firewall service update vnc-viewer tcp port 5900
firewall service update x-windows tcp port 6000 to 6063
firewall service-group update dns dns-tcp dns-udp
firewall service-group update email pop3 smtp imap imapv3
firewall service-group update ipsec ike ipsec-ah ipsec-esp
firewall service-group update ldap ldap-udp ldap-tcp
firewall service-group update management https ssh ping snmp-request
firewall service-group update netmeeting h323 audio-call-control t120
firewall service-group update network-protocols dns-tcp dns-udp dhcp-
server
firewall service-group update nfs portmapper-tcp portmapper-udp nfsd-tcp
nfsd-udp
firewall service-group update pptp pptp-tcp gre
firewall service-group update secure-management https ssh
firewall service-group update sip sip-tcp sip-udp
firewall service-group update sms-config http https sms-client snmp-
request ssh
firewall service-group update sms-get ntp sms-trap
firewall service-group update snmp snmp-request snmp-trap
firewall service-group update vnc vnc-browser vnc-viewer
```

```
firewall service-group update voice 3com-nbx sip-tcp sip-udp
firewall service-group update vpn-protocols pptp-tcp l2tp gre ike nat-t-
ipsec
firewall rule update 1 permit LAN WAN ANY
firewall rule update 1 schedule always timeout 30 logging disable
firewall rule update 1 src-addr all
firewall rule update 1 dst-addr all
firewall rule update 1 bandwidth disable
firewall rule update 1 authentication disable
firewall rule update 1 position 1
firewall rule update 1 comment "Allow LAN unrestricted access to WAN"
firewall rule update 1 remote-logging disable
firewall rule enable 1
firewall rule update 2 permit WAN this-device vpn-protocols
firewall rule update 2 schedule always timeout 30 logging disable
firewall rule update 2 src-addr all
firewall rule update 2 dst-addr all
firewall rule update 2 bandwidth disable
firewall rule update 2 authentication disable
firewall rule update 2 position 2
firewall rule update 2 comment "Allow VPN termination"
firewall rule update 2 remote-logging disable
firewall rule enable 2
firewall rule update 3 permit LAN this-device management
firewall rule update 3 schedule always timeout 30 logging disable
firewall rule update 3 src-addr all
firewall rule update 3 dst-addr all
firewall rule update 3 bandwidth disable
firewall rule update 3 authentication disable
firewall rule update 3 position 3
firewall rule update 3 comment "Allow management access from LAN"
firewall rule update 3 remote-logging disable
firewall rule enable 3
firewall rule update 4 permit LAN this-device network-protocols
firewall rule update 4 schedule always timeout 30 logging disable
firewall rule update 4 src-addr all
firewall rule update 4 dst-addr all
firewall rule update 4 bandwidth disable
firewall rule update 4 authentication disable
firewall rule update 4 position 4
firewall rule update 4 comment "Allow DNS and DHCP from LAN"
firewall rule update 4 remote-logging disable
firewall rule enable 4
firewall alg sip services ANY
firewall alg sip sdp-port-range ANY
routing rip disable update-timer 30
routing static add 192.168.22.0 netmask 255.255.255.0 gw 100.100.100.1
metric 1
routing multicast igmp disable
routing multicast pim-dm disable query-interval 30 prune-timeout 180
vpn ike local-id email x_family@3com.com
vpn ike local-id domain x_family
vpn ike add DES-SHA1-PSK
vpn ike proposal DES-SHA1-PSK phase1-encryption des-cbc
vpn ike proposal DES-SHA1-PSK phase1-integrity sha1
vpn ike proposal DES-SHA1-PSK phase1-dh-group 1
vpn ike proposal DES-SHA1-PSK phase1-lifetime 28800
```

```
vpn ike proposal DES-SHA1-PSK auth-type psk
vpn ike proposal DES-SHA1-PSK aggressive-mode disable
vpn ike proposal DES-SHA1-PSK local-id-type ip
vpn ike proposal DES-SHA1-PSK peer-id-type ip
vpn ike proposal DES-SHA1-PSK ca-cert ANY
vpn ike proposal DES-SHA1-PSK nat-t disable
vpn ike proposal DES-SHA1-PSK dpd enable
vpn ike proposal DES-SHA1-PSK auto-connect disable
vpn ike proposal DES-SHA1-PSK tight-phase2-control enable
vpn ike proposal DES-SHA1-PSK phase2-encryption des-cbc
vpn ike proposal DES-SHA1-PSK phase2-integrity esp-sha1-hmac
vpn ike proposal DES-SHA1-PSK phase2-lifetime 3600
vpn ike proposal DES-SHA1-PSK pfs disable
vpn ike proposal DES-SHA1-PSK phase2-dh-group 1
vpn ike proposal DES-SHA1-PSK phase2-zero-id disable
vpn ike proposal DES-SHA1-PSK phase2-strict-id-check disable
vpn ike add 3DES-SHA1-DH2
vpn ike proposal 3DES-SHA1-DH2 phase1-encryption 3des-cbc
vpn ike proposal 3DES-SHA1-DH2 phase1-integrity sha1
vpn ike proposal 3DES-SHA1-DH2 phase1-dh-group 2
vpn ike proposal 3DES-SHA1-DH2 phase1-lifetime 28800
vpn ike proposal 3DES-SHA1-DH2 auth-type psk
vpn ike proposal 3DES-SHA1-DH2 aggressive-mode disable
vpn ike proposal 3DES-SHA1-DH2 local-id-type ip
vpn ike proposal 3DES-SHA1-DH2 peer-id-type ip
vpn ike proposal 3DES-SHA1-DH2 ca-cert ANY
vpn ike proposal 3DES-SHA1-DH2 nat-t enable
vpn ike proposal 3DES-SHA1-DH2 dpd enable
vpn ike proposal 3DES-SHA1-DH2 auto-connect disable
vpn ike proposal 3DES-SHA1-DH2 tight-phase2-control disable
vpn ike proposal 3DES-SHA1-DH2 phase2-encryption 3des-cbc
vpn ike proposal 3DES-SHA1-DH2 phase2-integrity esp-sha1-hmac
vpn ike proposal 3DES-SHA1-DH2 phase2-lifetime 3600
vpn ike proposal 3DES-SHA1-DH2 pfs disable
vpn ike proposal 3DES-SHA1-DH2 phase2-dh-group 2
vpn ike proposal 3DES-SHA1-DH2 phase2-zero-id disable
vpn ike proposal 3DES-SHA1-DH2 phase2-strict-id-check disable
vpn ipsec enable
vpn ipsec add Default
vpn ipsec sa Default disable
vpn ipsec sa Default key ike proposal DES-SHA1-PSK shared-secret
********
vpn ipsec sa Default transport enable
vpn ipsec sa Default peer 0.0.0.0
vpn ipsec sa Default zone LAN
vpn ipsec sa Default tunnel enable
vpn ipsec add x_to_other
vpn ipsec sa x_to_other key ike proposal 3DES-SHA1-DH2 shared-secret
********
vpn ipsec sa x_to_other transport enable
vpn ipsec sa x_to_other peer 10.10.10.147
vpn ipsec sa x_to_other zone LAN
vpn ipsec sa x_to_other tunnel remote range 0.0.0.0 0.0.0.0
vpn ipsec sa x_to_other tunnel local range 0.0.0.0 0.0.0.0
vpn ipsec sa x_to_other tunnel nat disable
vpn ipsec sa x_to_other tunnel disable
vpn ipsec sa x_to_other enable
```

```
vpn l2tp addresses none
vpn l2tp zone LAN
vpn l2tp dns relay
vpn l2tp encryption enable
vpn l2tp disable
vpn pptp addresses none
vpn pptp zone LAN
vpn pptp dns relay
vpn pptp encryption enable
vpn pptp disable
ntp peer
ntp server 161.71.52.200:123
ntp duration 5
ntp offset 1
ntp fast enable
ntp enable
ramdisk sync-interval sys 30
ramdisk sync-interval audit 30
ramdisk sync-interval block -1
ramdisk sync-interval alert -1
ramdisk sync-interval firewallsession -1
ramdisk sync-interval firewallblock -1
ramdisk sync-interval vpn -1
sms v2
sms no must-be-ip
no sms
sms no remote-deploy
session timeout 20 -persist
3KB_x_unit_1#
```

6.1.2 3Com 5642 Router configuration file

```
<3COM_ROUTER>display current-configuration
#
#3Com Router Software Extended_V2.41
#
 sysname 3COM_ROUTER
#
 configure-user count  1
#
radius scheme system
#
domain system
#
local-user admin
 password simple topuser
 service-type ssh telnet terminal
 level 3
 service-type ftp
 service-type ppp
#
ike proposal 1
 encryption-algorithm 3des-cbc
 dh group2
#
```

```
ike peer x
 pre-shared-key shared-secret
 remote-name 10.10.20.147
 remote-address 10.10.20.147
 local-address 10.10.10.147
#
ipsec proposal 3des-sha1
 encapsulation-mode transport
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
#
ipsec policy test 1 isakmp
 security acl 3101
 ike-peer x
 proposal 3des-sha1
#
acl number 3101
 rule 1 permit ip source 10.10.10.147 0 destination 10.10.20.147 0
#
controller T3 1/0
 t1 1 channel-set 0 timeslot-list 5-10
 t1 2 unframed
 t1 27 unframed
#
interface Aux0
 async mode flow
#
interface Ethernet0/0
 ip address 10.10.10.147 255.255.255.0
 ipsec policy test
#
interface Ethernet0/1
 ip address 192.168.22.254 255.255.255.0
#
interface Serial1/0/1:0
 link-protocol ppp
#
interface Serial1/0/2:0
 link-protocol ppp
#
interface Serial1/0/27:0
 link-protocol ppp
#
interface Tunnel0
 ip address 100.100.100.2 255.255.255.0
 source 10.10.10.147
 destination 10.10.20.147
#
interface NULL0
#
hwping-agent enable
#
 ip route-static 0.0.0.0 0.0.0.0 10.10.10.1 preference 60
```

```
 ip route-static 192.168.1.0 255.255.255.0 Tunnel 0 preference 20
#
 snmp-agent
 snmp-agent local-engineid 000007DB7F000001000070BC
 snmp-agent community read public
 snmp-agent community write private
 snmp-agent sys-info contact topman
 snmp-agent sys-info location Lab
 snmp-agent sys-info version v1 v3
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
 user privilege level 3
 set authentication password simple toppass
#
return
<3COM_ROUTER>
```

6.2 Aggressive Mode

6.2.1 "show conf" file for X-family device

```
3KB_x_unit_1# show conf
interface ethernet 3 1
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface ethernet 3 2
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface ethernet 3 3
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface ethernet 3 4
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface ethernet 3 5
    negotiate
    duplex full
    linespeed 100
    no shutdown
```

```
    exit
interface ethernet 3 6
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface settings poll-interval 2000
interface settings detect-mdi enable
interface settings mdi-mode mdix
host name "3KB_x_unit_1"
host location "Lab"
host ip-filter permit any icmp

host ip-filter permit any ip

no autodv
user options max-attempts   5
user options expire-period  90
user options expire-action  expire
user options lockout-period 5
 --More--

user options attempt-action lockout
user options security-level 2
high-availability disable

high-availability heartbeat 4 100 2

high-availability id 4098

clock timezone GMT
clock dst
log audit select general
log audit select login
log audit select logout
log audit select user
log audit select time
log audit select policy
log audit select update
log audit select boot
log audit select report
log audit select host
log audit select configuration
log audit select oam
log audit select sms
log audit select server
log audit select segment
log audit select high-availability
log audit select monitor
log audit select ip-filter
log audit select conn-table
log audit select host-communication
log audit select tse
category-settings -profile "Default Security Profile" vulnerabilities
enable - action-set "Recommended"
```

```
category-settings -profile "Default Security Profile" exploits
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" security-policy
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" reconnaissance
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" virus
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" spyware
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" identity-theft
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" traffic-normal
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" network-equipment
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" p2p
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" im
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" streaming-media
enable - action-set "Recommended"
notify-contact "Management Console" 1
notify-contact "Remote System Log" 1
default-alert-sink period 1
server ssh
server no http
server https
server browser-check
monitor threshold memory      -major  90 -critical  95
monitor threshold disk        -major  90 -critical  95
monitor threshold temperature -major  92 -critical  94
monitor disable power-supply
no service-access
tse adaptive-filter mode automatic
tse afc-severity warning
tse connection-table timeout 1800
tse logging-mode conditional -threshold 1.0 -period 600
tse quarantine duration 60
email-rate-limit 10
zone update LAN vlan-id 1
zone update LAN port 3/1
zone update LAN mtu 1500
zone update LAN addresses disable
zone update LAN vpn-tunnel-access enable
zone update VPN vlan-id 4
zone update VPN port none
zone update VPN mtu 1500
zone update VPN addresses disable
zone update VPN vpn-tunnel-access enable
zone update WAN vlan-id 3
zone update WAN port 3/6
zone update WAN mtu 1500
zone update WAN addresses disable
zone update WAN vpn-tunnel-access enable
address-groups update DHCP-Pool range 192.168.1.1 192.168.1.20
```

```
authentication privilege-groups update Allow_VPN_access vpn-client-
access
authentication privilege-groups update RADIUS
authentication radius default-privilege-group RADIUS
authentication radius server primary 0.0.0.0 port 1812 shared-secret
******** au
th-method chap
authentication radius server secondary none
authentication radius disable
authentication radius user-authentication enable
authentication radius vpn-clients enable
authentication radius retries 3
authentication radius timeout 2
web-filtering default-rule block
web-filtering filter-action block-and-log
web-filtering filter-service cache expiry 24
web-filtering filter-service cache size 2097152
web-filtering filter-service block adult
web-filtering filter-service block gambling
web-filtering filter-service block violence
web-filtering filter-service block criminal
web-filtering filter-service block hacking
web-filtering filter-service block weapons
web-filtering filter-service block drugs
web-filtering filter-service block hate
web-filtering filter-service permit advertisement
web-filtering filter-service permit computing
web-filtering filter-service permit food
web-filtering filter-service permit politics
web-filtering filter-service permit hosting
web-filtering filter-service permit lifestyle
web-filtering filter-service permit dating
web-filtering filter-service permit reference
web-filtering filter-service permit sex-education
web-filtering filter-service permit sports
web-filtering filter-service permit usenet
web-filtering filter-service permit arts
web-filtering filter-service permit education
web-filtering filter-service permit games
web-filtering filter-service permit health
web-filtering filter-service permit careers
web-filtering filter-service permit vehicles
web-filtering filter-service permit photos
web-filtering filter-service permit religion
web-filtering filter-service permit search
web-filtering filter-service permit streaming-media
web-filtering filter-service permit email
web-filtering filter-service permit chat
web-filtering filter-service permit finance
web-filtering filter-service permit glamour
web-filtering filter-service permit hobbies
web-filtering filter-service permit kids
web-filtering filter-service permit news
web-filtering filter-service permit real-estate
web-filtering filter-service permit proxies
web-filtering filter-service permit shopping
web-filtering filter-service permit travel
```

```
web-filtering filter-service disable
web-filtering manual-filter disable
dhcp-server addresses group DHCP-Pool
dhcp-server enable
dhcp-server bootp disable
dhcp-server lease-duration 60
dhcp-server dns default
dhcp-server wins primary 0.0.0.0
dhcp-server wins secondary 0.0.0.0
dhcp-server nbx 0.0.0.0
dhcp-server relay disable
dns use-external-dns enable
interface virtual add 1 internal
interface virtual internal 1 ip 192.168.1.254 netmask 255.255.255.0
interface virtual internal 1 ha-mgmt-ip 0.0.0.0
interface virtual internal 1 nat external-ip
interface virtual internal 1 rip disable
interface virtual internal 1 rip send-mode v2-multicast
interface virtual internal 1 rip receive-mode all
interface virtual internal 1 rip auth disable
interface virtual internal 1 rip split-horizon enable
interface virtual internal 1 rip poison-reverse enable
interface virtual internal 1 rip advertise-routes enable
interface virtual internal 1 igmp disable
interface virtual internal 1 pim-dm disable
interface virtual internal 1 zone add LAN
interface virtual internal 1 zone add VPN
interface virtual add 2 external
interface virtual external 2 type static 10.10.20.147 netmask
255.255.255.0
interface virtual external 2 ha-mgmt-ip 0.0.0.0
interface virtual external 2 rip disable
interface virtual external 2 rip send-mode v2-multicast
interface virtual external 2 rip receive-mode all
interface virtual external 2 rip auth disable
interface virtual external 2 rip split-horizon enable
interface virtual external 2 rip poison-reverse enable
interface virtual external 2 rip advertise-routes disable
interface virtual external 2 igmp disable
interface virtual external 2 pim-dm disable
interface virtual external 2 zone add WAN
interface virtual add 3 gre
interface virtual gre 3 local-ip 100.100.100.1
interface virtual gre 3 peer-ip 100.100.100.2
interface virtual gre 3 sa X_to_other_agg
interface virtual gre 3 rip disable
interface virtual gre 3 rip send-mode disable
interface virtual gre 3 rip receive-mode disable
interface virtual gre 3 rip auth disable
interface virtual gre 3 rip split-horizon disable
interface virtual gre 3 rip poison-reverse disable
interface virtual gre 3 rip advertise-routes enable
interface virtual gre 3 igmp disable
interface virtual gre 3 pim-dm disable
interface virtual gre 3 zone add LAN
default-gateway 10.10.20.1
firewall schedule update working-day days -mtwtf- from 0800 to 1800
```

```
firewall service update 3com-nbx udp port 2093 to 2096
firewall service update audio-call-control tcp port 1731
firewall service update dhcp-client udp port 68
firewall service update dhcp-server udp port 67
firewall service update dns-tcp tcp port 53
firewall service update dns-udp udp port 53
firewall service update finger-tcp tcp port 79
firewall service update ftp tcp port 21
firewall service update gopher-tcp tcp port 70
firewall service update gre gre
firewall service update h323 tcp port 1720
firewall service update http tcp port 80
firewall service update https tcp port 443
firewall service update igmp igmp
firewall service update ike udp port 500
firewall service update imap tcp port 143
firewall service update imapv3 tcp port 220
firewall service update ipsec-ah ah
firewall service update ipsec-esp esp
firewall service update kerberos-tcp tcp port 88
firewall service update kerberos-udp udp port 88
firewall service update l2tp udp port 1701
firewall service update ldap-tcp tcp port 389
firewall service update ldap-udp udp port 389
firewall service update lotus-notes-domino tcp port 1352
firewall service update lpr tcp port 515
firewall service update nat-t-ipsec udp port 4500
firewall service update nbname tcp port 137
firewall service update netbios-tcp tcp port 137 to 139
firewall service update netbios-udp udp port 137 to 139
firewall service update netmeeting tcp port 1720
firewall service update nfsd-tcp tcp port 2049
firewall service update nfsd-udp udp port 2049
firewall service update nntp tcp port 119
firewall service update ntp udp port 123
firewall service update pim-dm pim
firewall service update ping icmp port 8
firewall service update pop3 tcp port 110
firewall service update portmapper-tcp tcp port 111
firewall service update portmapper-udp udp port 111
firewall service update pptp-tcp tcp port 1723
firewall service update radius-accounting udp port 1813
firewall service update radius-auth udp port 1812
firewall service update rexec tcp port 512
firewall service update rip udp port 520
firewall service update rlogin tcp port 513
firewall service update rsh tcp port 514
firewall service update rtsp tcp port 554
firewall service update sip-tcp tcp port 5060
firewall service update sip-udp udp port 5060
firewall service update smb tcp port 445
firewall service update sms-client tcp port 10042
firewall service update sms-trap tcp port 8162 to 8163
firewall service update smtp tcp port 25
firewall service update snmp-request udp port 161
firewall service update snmp-trap udp port 162
firewall service update ssh tcp port 22
```

```
firewall service update syslog udp port 514
firewall service update t120 tcp port 1503
firewall service update telnet tcp port 23
firewall service update tftp udp port 69
firewall service update traceroute icmp port 8
firewall service update uucp udp port 540
firewall service update vnc-browser tcp port 5800
firewall service update vnc-viewer tcp port 5900
firewall service update x-windows tcp port 6000 to 6063
firewall service-group update dns dns-tcp dns-udp
firewall service-group update email pop3 smtp imap imapv3
firewall service-group update ipsec ike ipsec-ah ipsec-esp
firewall service-group update ldap ldap-udp ldap-tcp
firewall service-group update management https ssh ping snmp-request
firewall service-group update netmeeting h323 audio-call-control t120
firewall service-group update network-protocols dns-tcp dns-udp dhcp-
server
firewall service-group update nfs portmapper-tcp portmapper-udp nfsd-tcp
nfsd-udp
firewall service-group update pptp pptp-tcp gre
firewall service-group update secure-management https ssh
firewall service-group update sip sip-tcp sip-udp
firewall service-group update sms-config http https sms-client snmp-
request ssh
firewall service-group update sms-get ntp sms-trap
firewall service-group update snmp snmp-request snmp-trap
firewall service-group update vnc vnc-browser vnc-viewer
firewall service-group update voice 3com-nbx sip-tcp sip-udp
firewall service-group update vpn-protocols pptp-tcp l2tp gre ike nat-t-
ipsec
firewall rule update 1 permit LAN WAN ANY
firewall rule update 1 schedule always timeout 30 logging disable
firewall rule update 1 src-addr all
firewall rule update 1 dst-addr all
firewall rule update 1 bandwidth disable
firewall rule update 1 authentication disable
firewall rule update 1 position 1
firewall rule update 1 comment "Allow LAN unrestricted access to WAN"
firewall rule update 1 remote-logging disable
firewall rule enable 1
firewall rule update 2 permit WAN this-device vpn-protocols
firewall rule update 2 schedule always timeout 30 logging disable
firewall rule update 2 src-addr all
firewall rule update 2 dst-addr all
firewall rule update 2 bandwidth disable
firewall rule update 2 authentication disable
firewall rule update 2 position 2
firewall rule update 2 comment "Allow VPN termination"
firewall rule update 2 remote-logging disable
firewall rule enable 2
firewall rule update 3 permit LAN this-device management
firewall rule update 3 schedule always timeout 30 logging disable
firewall rule update 3 src-addr all
firewall rule update 3 dst-addr all
firewall rule update 3 bandwidth disable
firewall rule update 3 authentication disable
firewall rule update 3 position 3
```

```
firewall rule update 3 comment "Allow management access from LAN"
firewall rule update 3 remote-logging disable
firewall rule enable 3
firewall rule update 4 permit LAN this-device network-protocols
firewall rule update 4 schedule always timeout 30 logging disable
firewall rule update 4 src-addr all
firewall rule update 4 dst-addr all
firewall rule update 4 bandwidth disable
firewall rule update 4 authentication disable
firewall rule update 4 position 4
firewall rule update 4 comment "Allow DNS and DHCP from LAN"
firewall rule update 4 remote-logging disable
firewall rule enable 4
firewall alg sip services ANY
firewall alg sip sdp-port-range ANY
routing rip disable update-timer 30
routing static add 192.168.22.0 netmask 255.255.255.0 gw 100.100.100.1
metric 1
routing multicast igmp disable
routing multicast pim-dm disable query-interval 30 prune-timeout 180
vpn ike local-id email x_family@3com.com
vpn ike local-id domain x_family
vpn ike add DES-SHA1-PSK
vpn ike proposal DES-SHA1-PSK phase1-encryption des-cbc
vpn ike proposal DES-SHA1-PSK phase1-integrity sha1
vpn ike proposal DES-SHA1-PSK phase1-dh-group 1
vpn ike proposal DES-SHA1-PSK phase1-lifetime 28800
vpn ike proposal DES-SHA1-PSK auth-type psk
vpn ike proposal DES-SHA1-PSK aggressive-mode disable
vpn ike proposal DES-SHA1-PSK local-id-type ip
vpn ike proposal DES-SHA1-PSK peer-id-type ip
vpn ike proposal DES-SHA1-PSK ca-cert ANY
vpn ike proposal DES-SHA1-PSK nat-t disable
vpn ike proposal DES-SHA1-PSK dpd enable
vpn ike proposal DES-SHA1-PSK auto-connect disable
vpn ike proposal DES-SHA1-PSK tight-phase2-control enable
vpn ike proposal DES-SHA1-PSK phase2-encryption des-cbc
vpn ike proposal DES-SHA1-PSK phase2-integrity esp-sha1-hmac
vpn ike proposal DES-SHA1-PSK phase2-lifetime 3600
vpn ike proposal DES-SHA1-PSK pfs disable
vpn ike proposal DES-SHA1-PSK phase2-dh-group 1
vpn ike proposal DES-SHA1-PSK phase2-zero-id disable
vpn ike proposal DES-SHA1-PSK phase2-strict-id-check disable
vpn ike add 3DES-SHA1-DH2
vpn ike proposal 3DES-SHA1-DH2 phase1-encryption 3des-cbc
vpn ike proposal 3DES-SHA1-DH2 phase1-integrity sha1
vpn ike proposal 3DES-SHA1-DH2 phase1-dh-group 2
vpn ike proposal 3DES-SHA1-DH2 phase1-lifetime 28800
vpn ike proposal 3DES-SHA1-DH2 auth-type psk
vpn ike proposal 3DES-SHA1-DH2 aggressive-mode disable
vpn ike proposal 3DES-SHA1-DH2 local-id-type ip
vpn ike proposal 3DES-SHA1-DH2 peer-id-type ip
vpn ike proposal 3DES-SHA1-DH2 ca-cert ANY
vpn ike proposal 3DES-SHA1-DH2 nat-t enable
vpn ike proposal 3DES-SHA1-DH2 dpd enable
vpn ike proposal 3DES-SHA1-DH2 auto-connect disable
vpn ike proposal 3DES-SHA1-DH2 tight-phase2-control disable
```

```
vpn ike proposal 3DES-SHA1-DH2 phase2-encryption 3des-cbc
vpn ike proposal 3DES-SHA1-DH2 phase2-integrity esp-sha1-hmac
vpn ike proposal 3DES-SHA1-DH2 phase2-lifetime 3600
vpn ike proposal 3DES-SHA1-DH2 pfs disable
vpn ike proposal 3DES-SHA1-DH2 phase2-dh-group 2
vpn ike proposal 3DES-SHA1-DH2 phase2-zero-id disable
vpn ike proposal 3DES-SHA1-DH2 phase2-strict-id-check disable
vpn ike add 3DES-SHA1-DH2-AGG-PFS
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS phase1-encryption 3des-cbc
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS phase1-integrity sha1
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS phase1-dh-group 2
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS phase1-lifetime 28800
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS auth-type psk
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS aggressive-mode enable
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS local-id-type domain
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS peer-id-type domain
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS ca-cert ANY
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS nat-t enable
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS dpd enable
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS auto-connect disable
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS tight-phase2-control disable
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS phase2-encryption 3des-cbc
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS phase2-integrity esp-sha1-hmac
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS phase2-lifetime 3600
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS pfs enable
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS phase2-dh-group 2
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS phase2-zero-id disable
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS phase2-strict-id-check disable
vpn ipsec enable
vpn ipsec add Default
vpn ipsec sa Default disable
vpn ipsec sa Default key ike proposal DES-SHA1-PSK shared-secret
********
vpn ipsec sa Default transport enable
vpn ipsec sa Default peer 0.0.0.0
vpn ipsec sa Default zone LAN
vpn ipsec sa Default tunnel enable
vpn ipsec add X_to_other_agg
vpn ipsec sa X_to_other_agg key ike proposal 3DES-SHA1-DH2-AGG-PFS
shared-secret
 ******** peer-id OTHER
vpn ipsec sa X_to_other_agg transport enable
vpn ipsec sa X_to_other_agg peer 10.10.10.147
vpn ipsec sa X_to_other_agg zone LAN
vpn ipsec sa X_to_other_agg tunnel remote range 0.0.0.0 0.0.0.0
vpn ipsec sa X_to_other_agg tunnel local range 0.0.0.0 0.0.0.0
vpn ipsec sa X_to_other_agg tunnel nat disable
vpn ipsec sa X_to_other_agg tunnel disable
vpn ipsec sa X_to_other_agg enable
vpn l2tp addresses none
vpn l2tp zone LAN
vpn l2tp dns relay
vpn l2tp encryption enable
vpn l2tp disable
vpn pptp addresses none
vpn pptp zone LAN
vpn pptp dns relay
```

```
vpn pptp encryption enable
vpn pptp disable
ntp peer
ntp server 161.71.52.200:123
ntp duration 5
ntp offset 1
ntp fast enable
ntp enable
ramdisk sync-interval sys 30
ramdisk sync-interval audit 30
ramdisk sync-interval block -1
ramdisk sync-interval alert -1
ramdisk sync-interval firewallsession -1
ramdisk sync-interval firewallblock -1
ramdisk sync-interval vpn -1
sms v2
sms no must-be-ip
no sms
sms no remote-deploy
session timeout 20 -persist
3KB_x_unit_1#
```

6.2.2 3Com 5642 Router configuration file

```
<OTHER>display current-configuration
#
#3Com Router Software Extended_V2.41
#
 sysname OTHER
#
 configure-user count  1
#
radius scheme system
#
domain system
#
local-user admin
 password simple breakit
 service-type ssh telnet terminal
 level 3
 service-type ftp
 service-type ppp
#
ike proposal 1
 encryption-algorithm 3des-cbc
 dh group2
#
ike peer x
 exchange-mode aggressive
 pre-shared-key shared-secret
 id-type name
 remote-name x_family
 local-address 10.10.10.147
```

```
#
ipsec proposal 3des-sha1
 encapsulation-mode transport
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
#
ipsec policy test 1 isakmp
 security acl 3101
 pfs dh-group2
 ike-peer x
 proposal 3des-sha1
#
acl number 3101
 rule 1 permit ip source 10.10.10.147 0 destination 10.10.20.147 0
#
controller T3 1/0
 t1 1 channel-set 0 timeslot-list 5-10
 t1 2 unframed
 t1 27 unframed
#
interface Aux0
 async mode flow
#
interface Ethernet0/0
 ip address 10.10.10.147 255.255.255.0
 ipsec policy test
#
interface Ethernet0/1
 ip address 192.168.22.254 255.255.255.0
#
interface Serial1/0/1:0
 link-protocol ppp
#
interface Serial1/0/2:0
 link-protocol ppp
#
interface Serial1/0/27:0
 link-protocol ppp
#
interface Tunnel0
 ip address 100.100.100.2 255.255.255.0
 source 10.10.10.147
 destination 10.10.20.147
#
interface NULL0
#
hwping-agent enable
#
 ip route-static 0.0.0.0 0.0.0.0 10.10.10.1 preference 60
 ip route-static 192.168.1.0 255.255.255.0 Tunnel 0 preference 20
#
 snmp-agent
 snmp-agent local-engineid 000007DB7F000001000070BC
```

```
 snmp-agent community read public
 snmp-agent community write private
 snmp-agent sys-info contact NetMan
 snmp-agent sys-info location Hemel Test Lab
 snmp-agent sys-info version v1 v3
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
 user privilege level 3
 set authentication password simple breakit
#
return
<OTHER>
```

7 Dynamic Routing Addendum

The preceding GRE tunnel configurations rely on static routes to route the test traffic over the GRE tunnel.

However, both the X-FAMILY and 5642 Router also support dynamic routing over the GRE tunnel. This comprises:

- RIP (Routing Information Protocol) for unicast dynamic routing and
- PIM-DM (Protocol Independent Multicast – Dense Mode) for multicast dynamic routing.

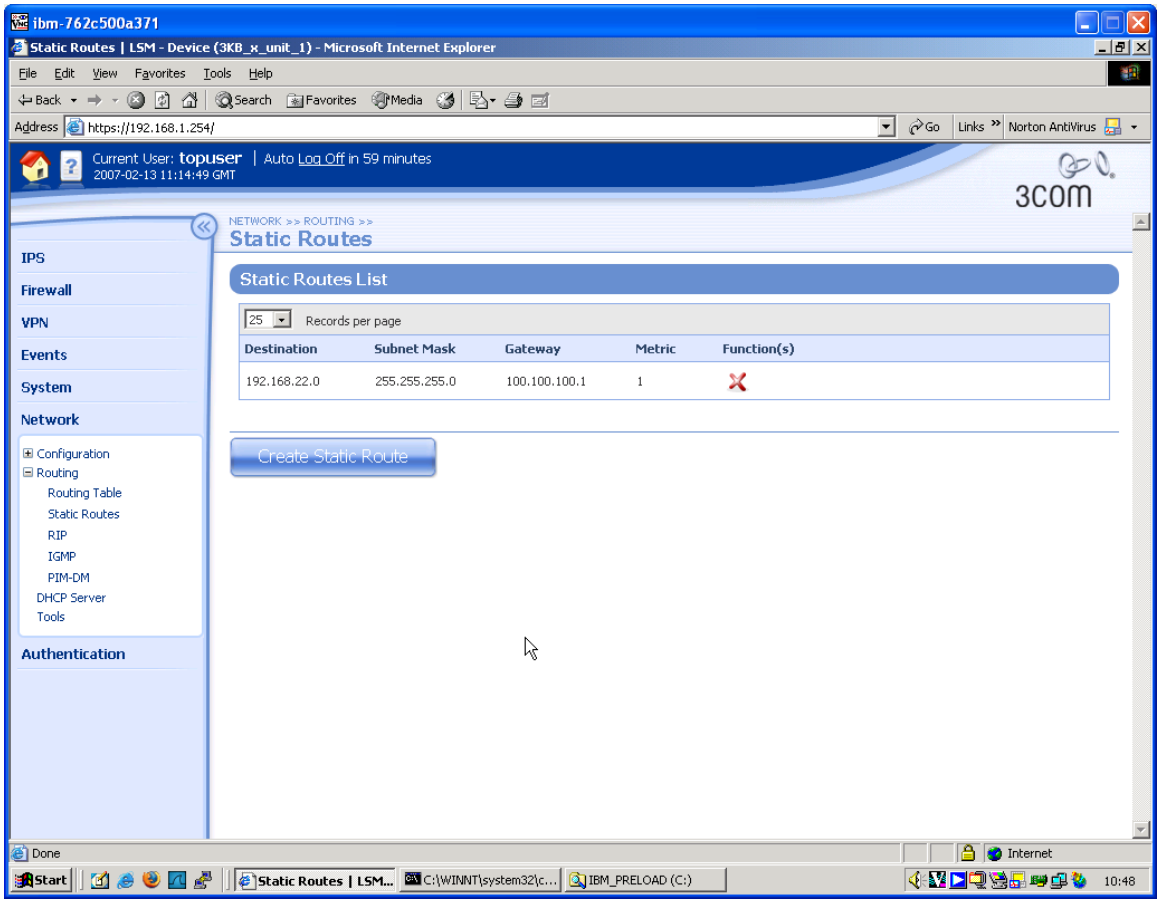
Both devices also support IGMP (Internet Group Management Protocol) – which is used to manage multicast group membership.

This addendum uses the previous – static-routed – configurations as a starting point and adds dynamic routing stage by stage.

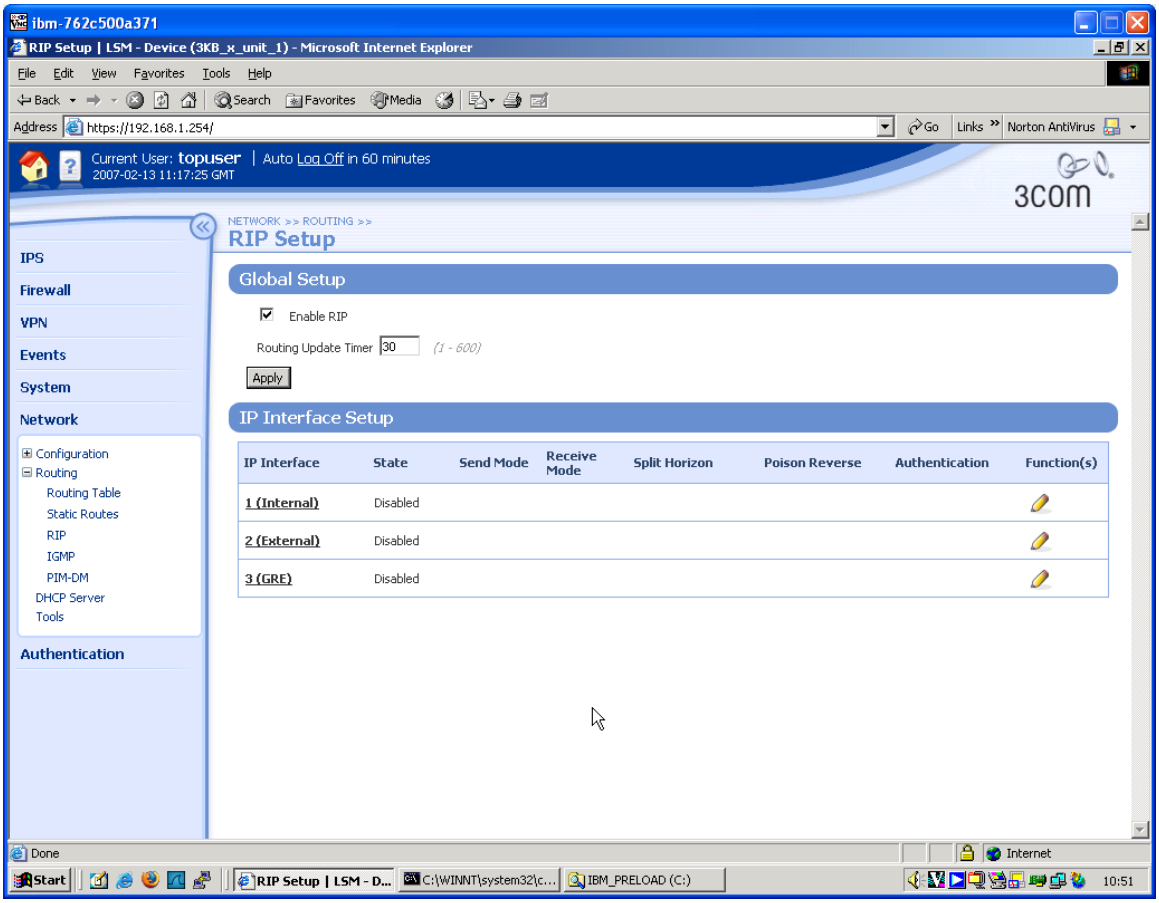
7.1 Adding Unicast Dynamic Routing Using RIP

7.1.1 Configuring X-FAMILY Device

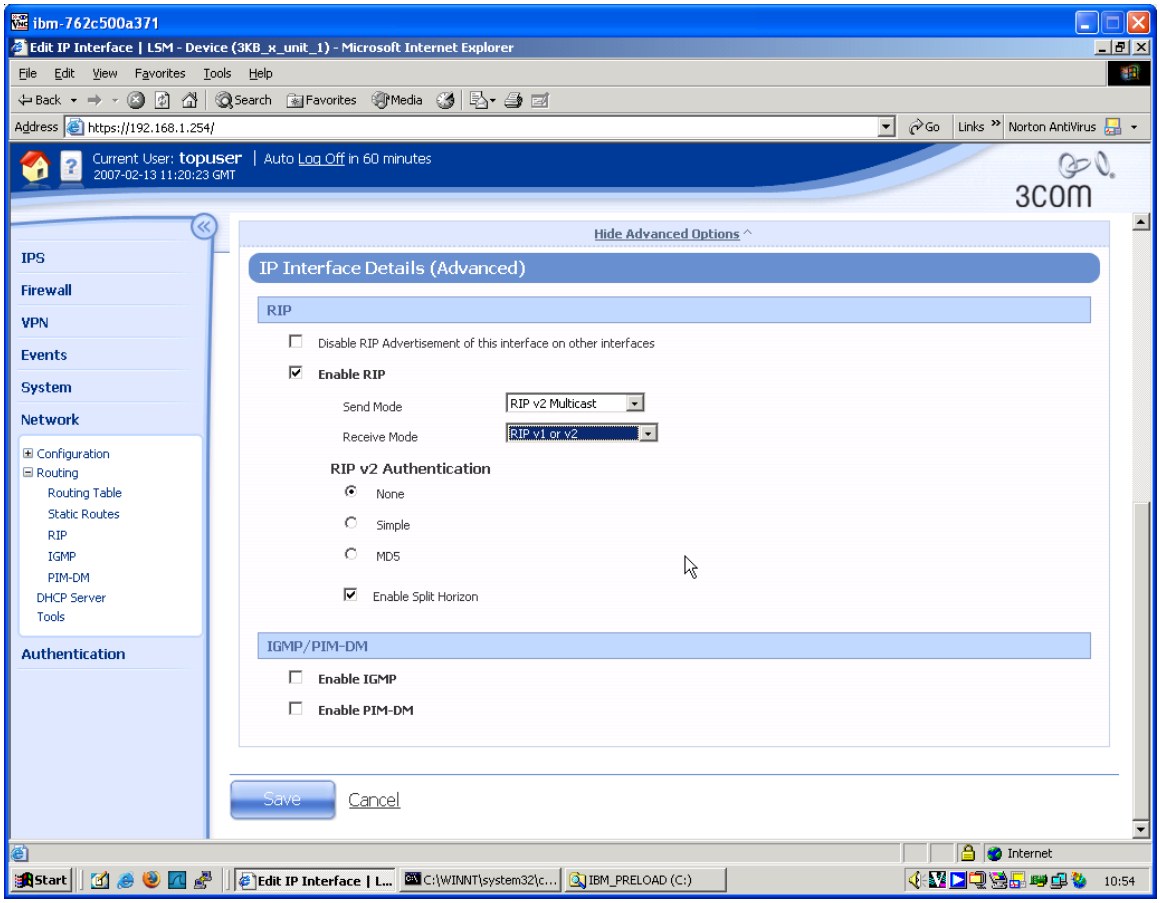
1. First delete the static route from the previous configuration. Navigate to Network->Routing->Static Routes and click the cross next to the single entry in the table to delete it.



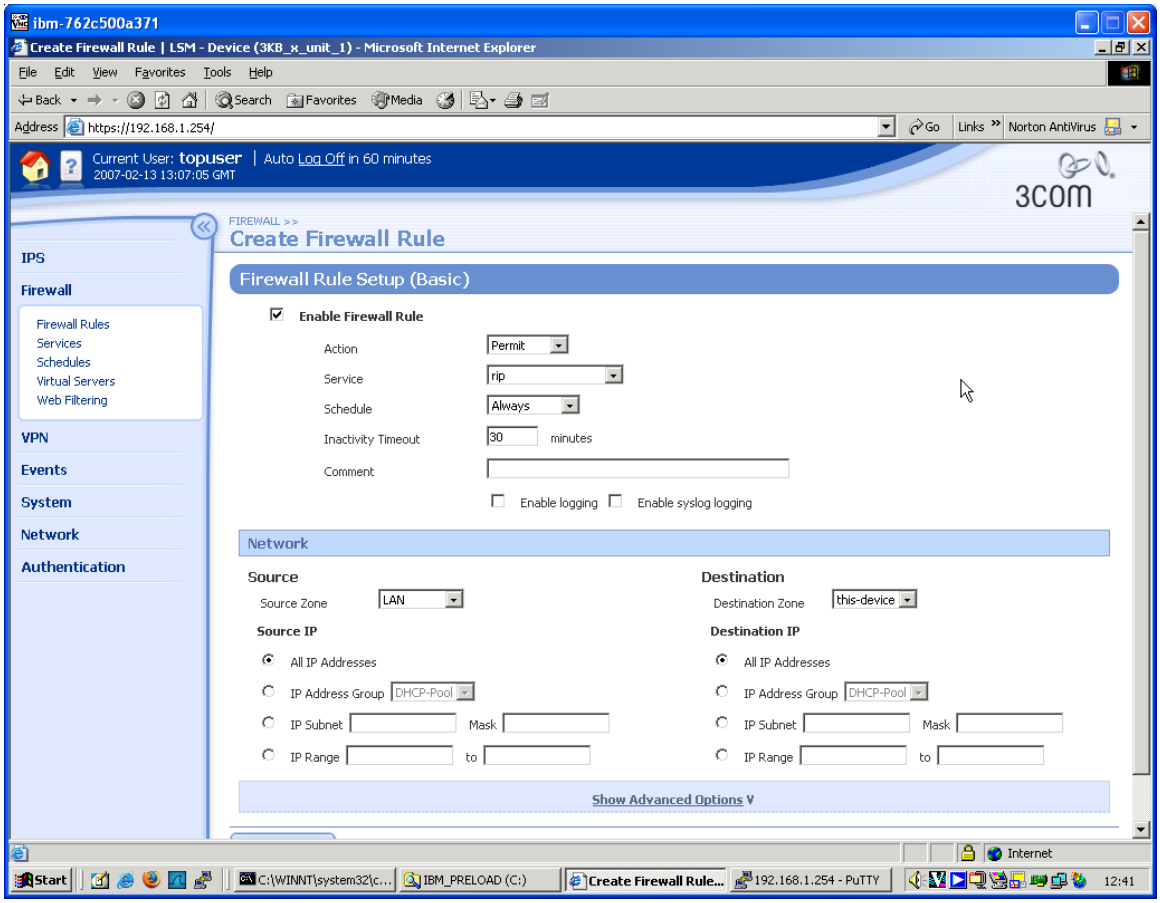
2. Now globally enable RIP on the Network->Routing->RIP page by checking the "Enable RIP" checkbox and clicking "Apply".



3. Then, on the same page, click on the GRE interface and complete the form as shown below. You will need to click the "Show Advanced Options" hyperlink to access these parameters. The RIP parameters are hidden until the "Enable RIP" checkbox is checked.



4. Click Save to save the changes.
5. Finally create a firewall rule to permit the RIP updates into the X-FAMILY device from the GRE tunnel (which, remember, terminates on the LAN zone). Navigate to Firewall->Firewall Rules, click on "Create Firewall Rule" and complete the form as follows.



6. Click the "Create" button to create the rule.

7.1.2 Configuring the 3Com 5642 Router.

7. First remove the static route set up previously.
   Using direct console port connection, telnet or SSH, login to the 5642 Command Line Interface and perform the sequence of commands shown below:

```
<OTHER>system-view
System View: return to User View with Ctrl+Z.
[ROUTER_5642]undo ip route-static 192.168.1.0 255.255.255.0
[OTHER]
```

8. Then enable RIP on the relevant networks and on the GRE Tunnel interface by performing the following sequence of commands.

```
[OTHER]rip
[OTHER-rip]network 192.168.22.0
[OTHER-rip]network 100.100.100.2
[OTHER-rip]quit
[OTHER]interface Tunnel 0
[OTHER-Tunnel0]rip work
[OTHER-Tunnel0]rip version 2 multicast
[OTHER-Tunnel0]quit
[OTHER]
```

7.1.3 Testing

1. The dynamic routing can be tested in two ways:
   - by ping traffic between PC1 and PC2 as normal (and checking the tunnel statistics on the 5642 Router as described earlier);
   - by looking in the routing table at each end for RIP entries for the network at the other end. For example, on the 5642 Router:

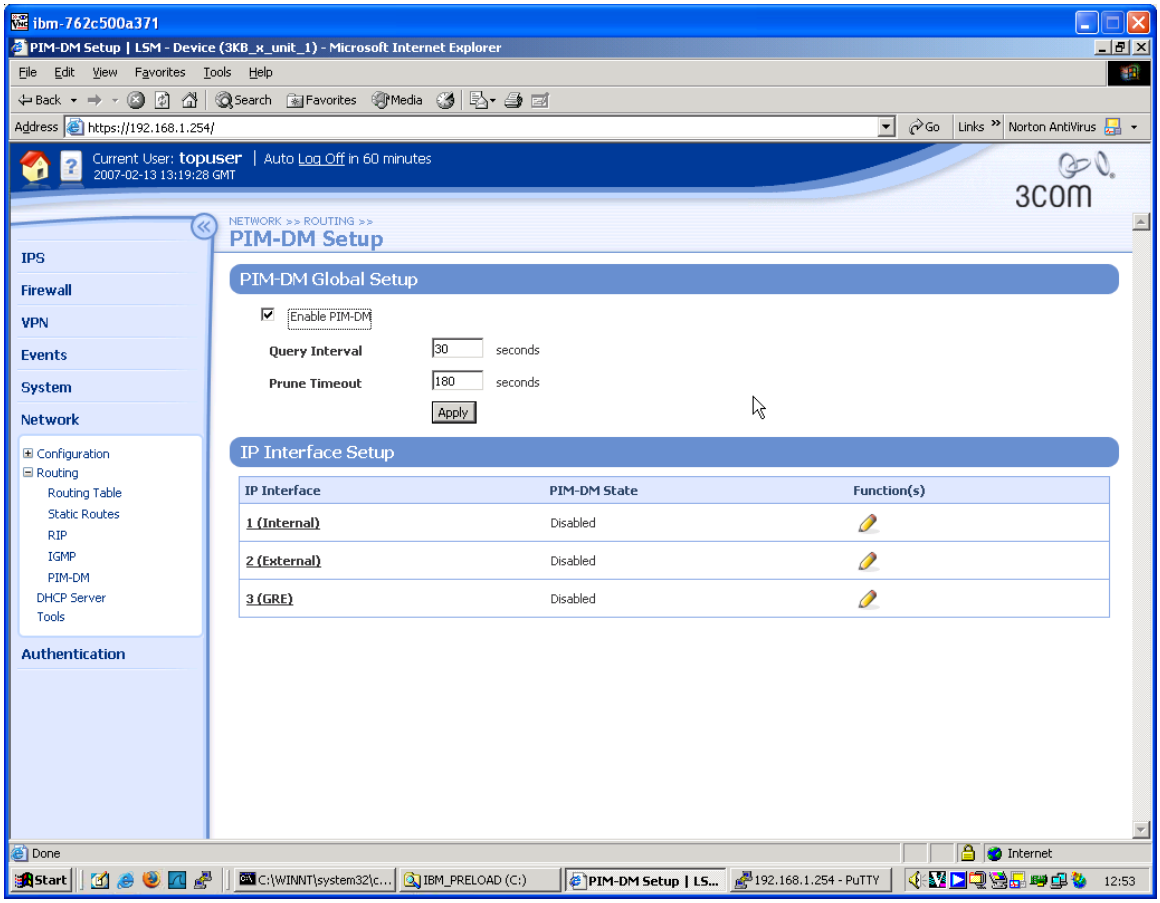
```
[OTHER]display ip routing-table
 Routing Table: public net
Destination/Mask    Protocol Pre  Cost        Nexthop         Interface
0.0.0.0/0           STATIC   60   0           10.10.10.1      Ethernet0/0
10.10.10.0/24       DIRECT   0    0           10.10.10.147    Ethernet0/0
10.10.10.147/32     DIRECT   0    0           127.0.0.1       InLoopBack0
100.100.100.0/24    DIRECT   0    0           100.100.100.2   Tunnel0
100.100.100.2/32    DIRECT   0    0           127.0.0.1       InLoopBack0
127.0.0.0/8         DIRECT   0    0           127.0.0.1       InLoopBack0
127.0.0.1/32        DIRECT   0    0           127.0.0.1       InLoopBack0
192.168.1.0/24      RIP      100  1           100.100.100.1   Tunnel0
192.168.22.0/24     DIRECT   0    0           192.168.22.254  Ethernet0/1
192.168.22.254/32   DIRECT   0    0           127.0.0.1       InLoopBack0
[OTHER]
```

Note the RIP entry.

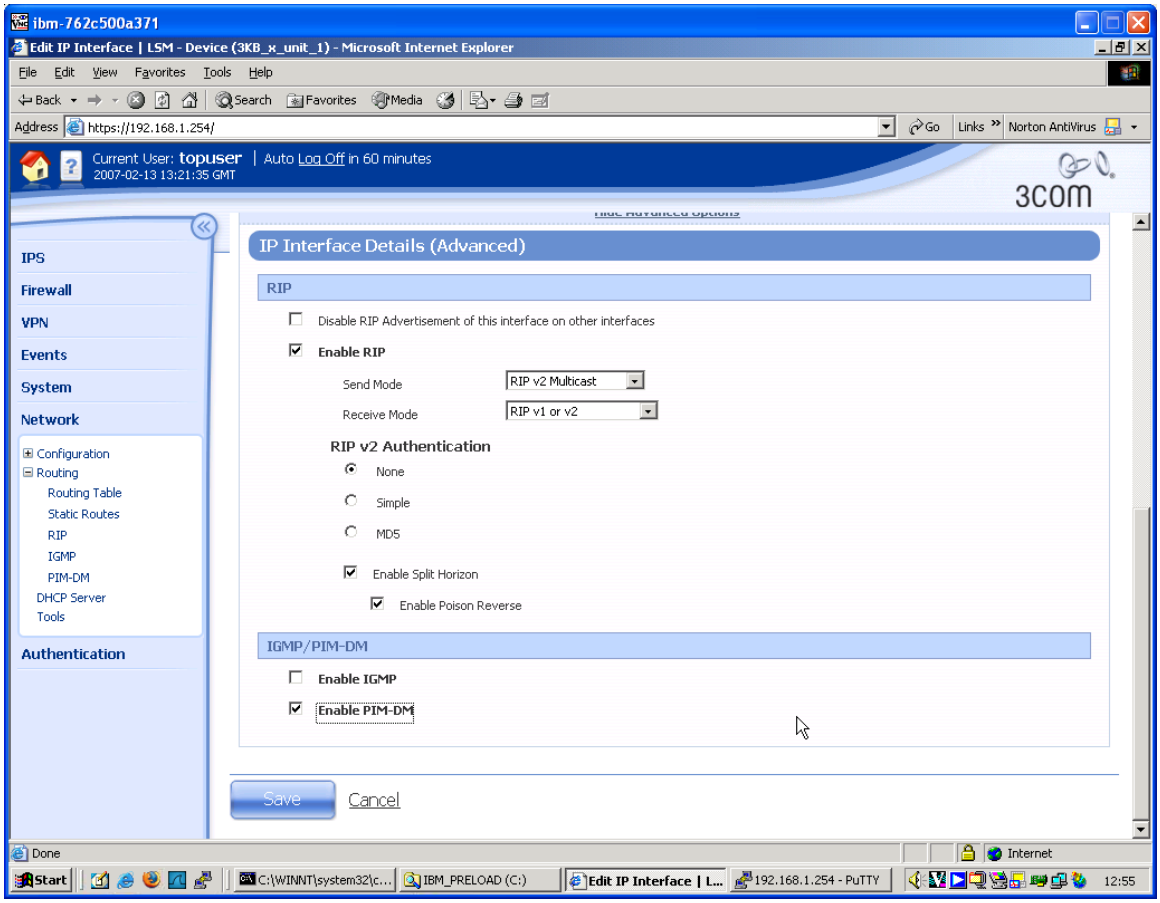
7.2 Adding Multicast Dynamic Routing Using PIM-DM

7.2.1 Configuring X-FAMILY Device

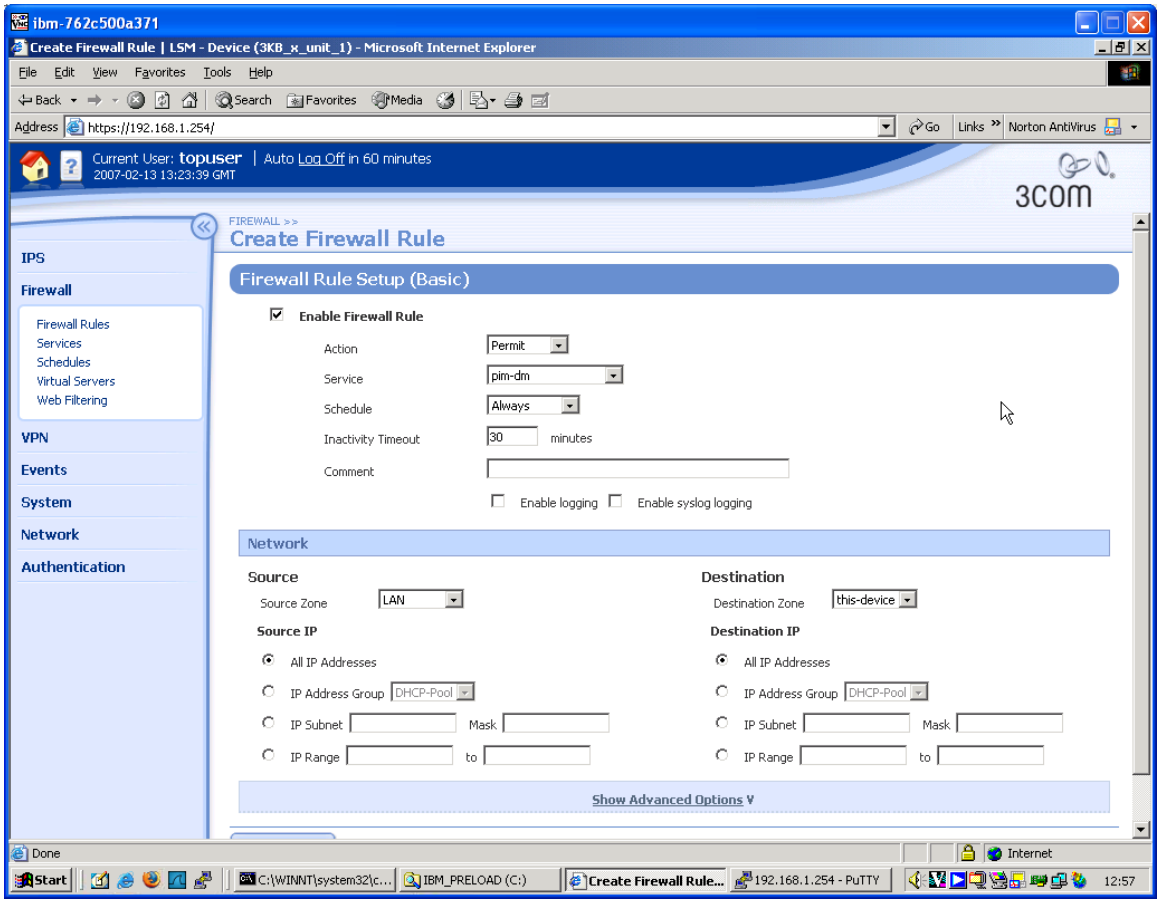
1. Firstly globally enable PIM-DM on the Network->Routing->PIM-DM page by checking the “Enable PIM-DM” checkbox and clicking “Apply”.



2. Then, on the same page, click on the GRE interface and complete the form as shown below. You will need to click the "Show Advanced Options" hyperlink to access the "Enable PIM-DM" checkbox.



3. Click the "Save" button to save the change.
4. Finally create a firewall rule to permit the PIM-DM updates into the X-FAMILY device from the GRE tunnel (which, remember, terminates on the LAN zone). Navigate to Firewall->Firewall Rules, click on "Create Firewall Rule" and complete the form as follows.



5. Click the "Create" button to create the rule.

7.2.2 Configuring the 3Com 5642 Router

1. Using direct console port connection, telnet or SSH, login to the 5642 Command Line Interface and perform the sequence of commands shown below to enable multicast routing and to enable PIM-DM globally and on the GRE Tunnel interface:

```
<OTHER>system-view
System View: return to User View with Ctrl+Z.
[OTHER]multicast routing-enable
[OTHER]pim
[OTHER-pim]quit
[OTHER]interface Tunnel0
[OTHER-Tunnel0]pim dm
[OTHER-Tunnel0]quit
[OTHER]
```

7.2.3 Testing

Adding PIM-DM does not actually add any multicast connectivity- we need IGMP for that. However, we can test that both the X-FAMILY device and the 5642 "see" the other device as a "PIM Neighbor".

1. On the 5642, perform the following commands.

```
<OTHER>display pim interface
PIM information of interface Tunnel0:
  IP address of the interface is 100.100.100.2
  PIM is enabled
  PIM version is 2
  PIM mode is Dense
  PIM query interval is 30 seconds
  PIM neighbor limit is 128
  PIM neighbor policy is none
  Total 1 PIM neighbor on interface
  PIM DR(designated router) is 100.100.100.2
```

i.e. The 5642 is seeing a PIM neighbour…

```
<OTHER>display pim neighbor
Neighbor's Address  Interface Name                Uptime    Expires
100.100.100.1       Tunnel0                      00:04:40  00:01:37
<OTHER>
```

…and it is at the other end of the GRE tunnel.

2. Unfortunately the X-FAMILY GUI doesn't have a page to display multicast information, but there is information available on the CLI. Login to the X-FAMILY CLI (direct console connection or SSH) and type the following:

```
3KB_x_unit_1# show routing multi

IGMP Querier Status

Interface  IP Address       Querier          Groups
---------- ---------------- ---------------- ----------------
1          192.168.1.254
2          10.10.20.147
3          100.100.100.1

PIM-DM Neighbor Table

Neighbor         Interface  Uptime     Expires    Version
---------------- ---------- ---------- ---------- ----------
100.100.100.2    3          73         79         2


Multicast Routing Table

Source IP        Group IP         Next Hop IP      Age
---------------- ---------------- ---------------- ----------

3KB_x_unit_1#
```

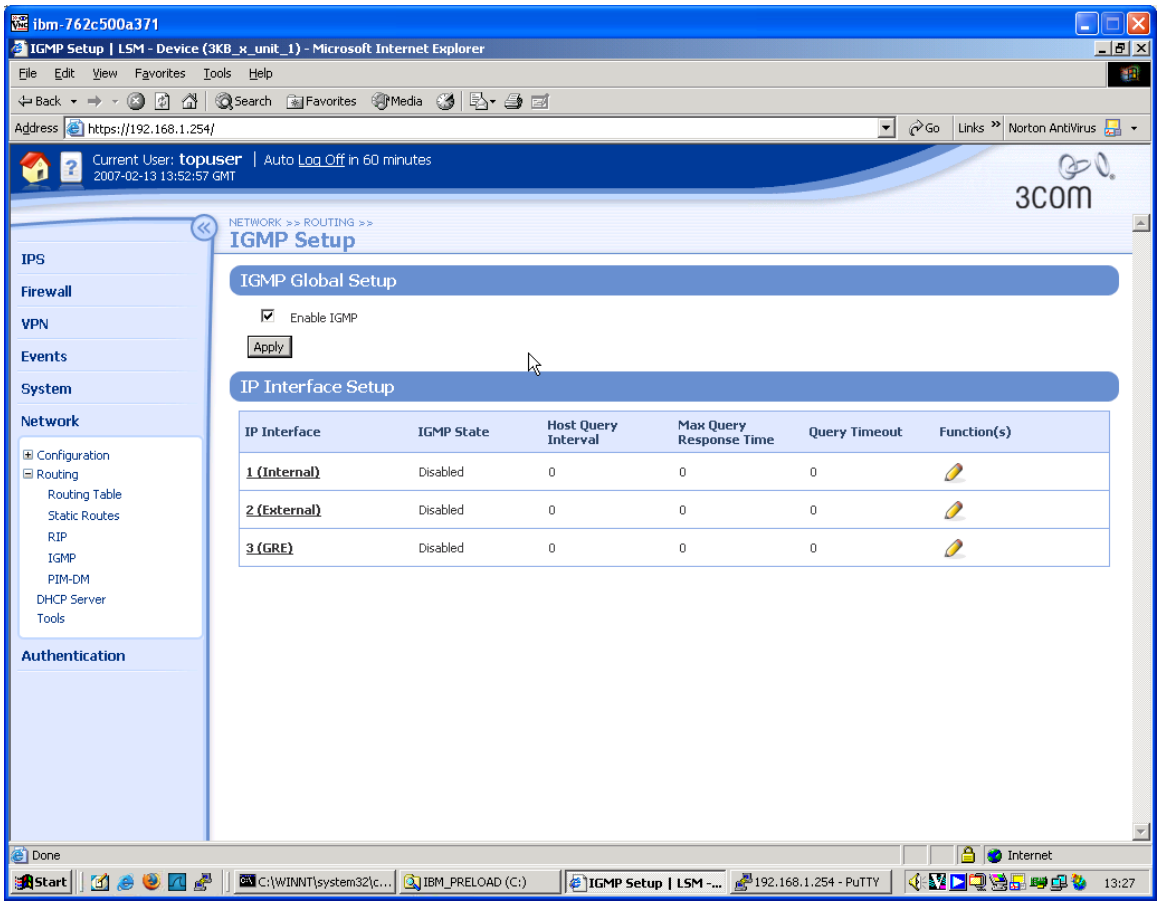
The PIM-DM Neighbor is clearly present.

7.3 Adding Multicast Group Support Using IGMP

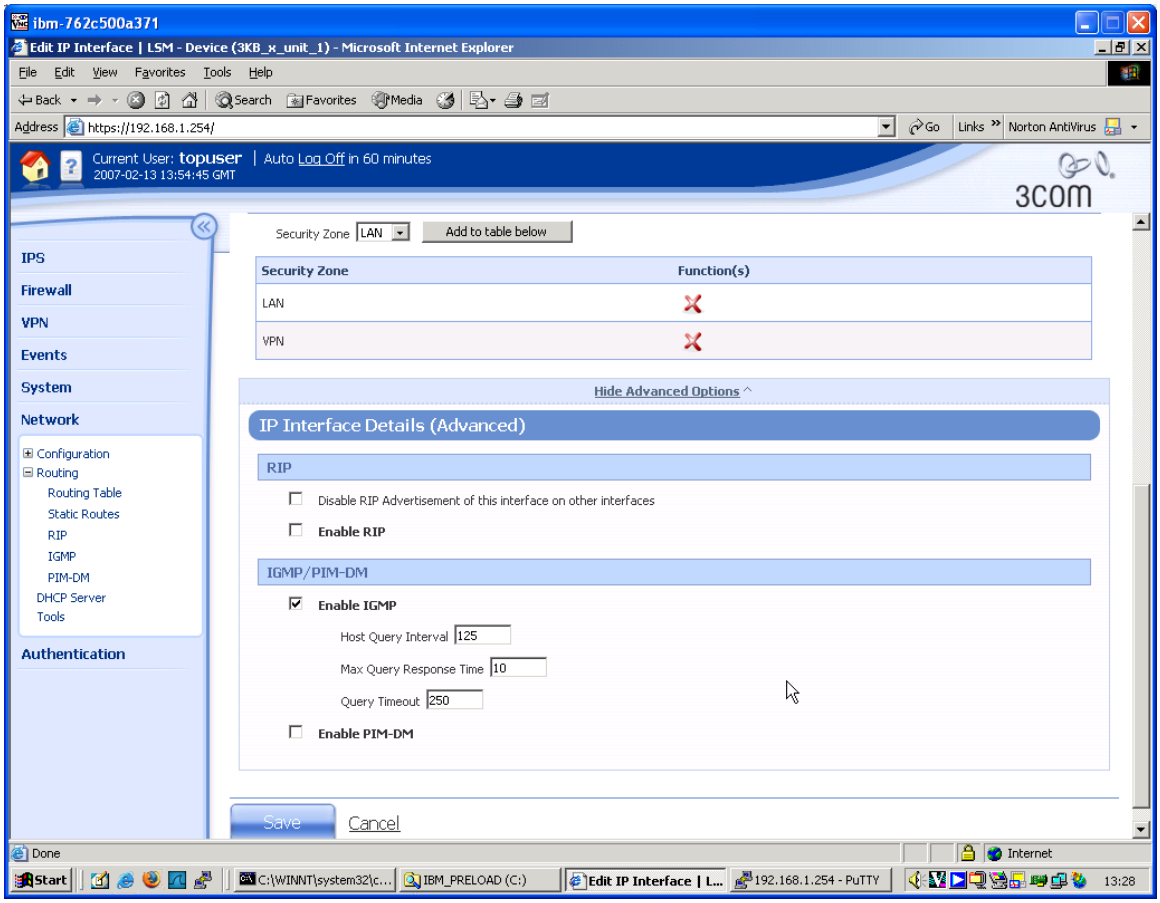
7.3.1 Configuring X-FAMILY Device

IGMP must be enabled globally and on all interfaces that will use it.

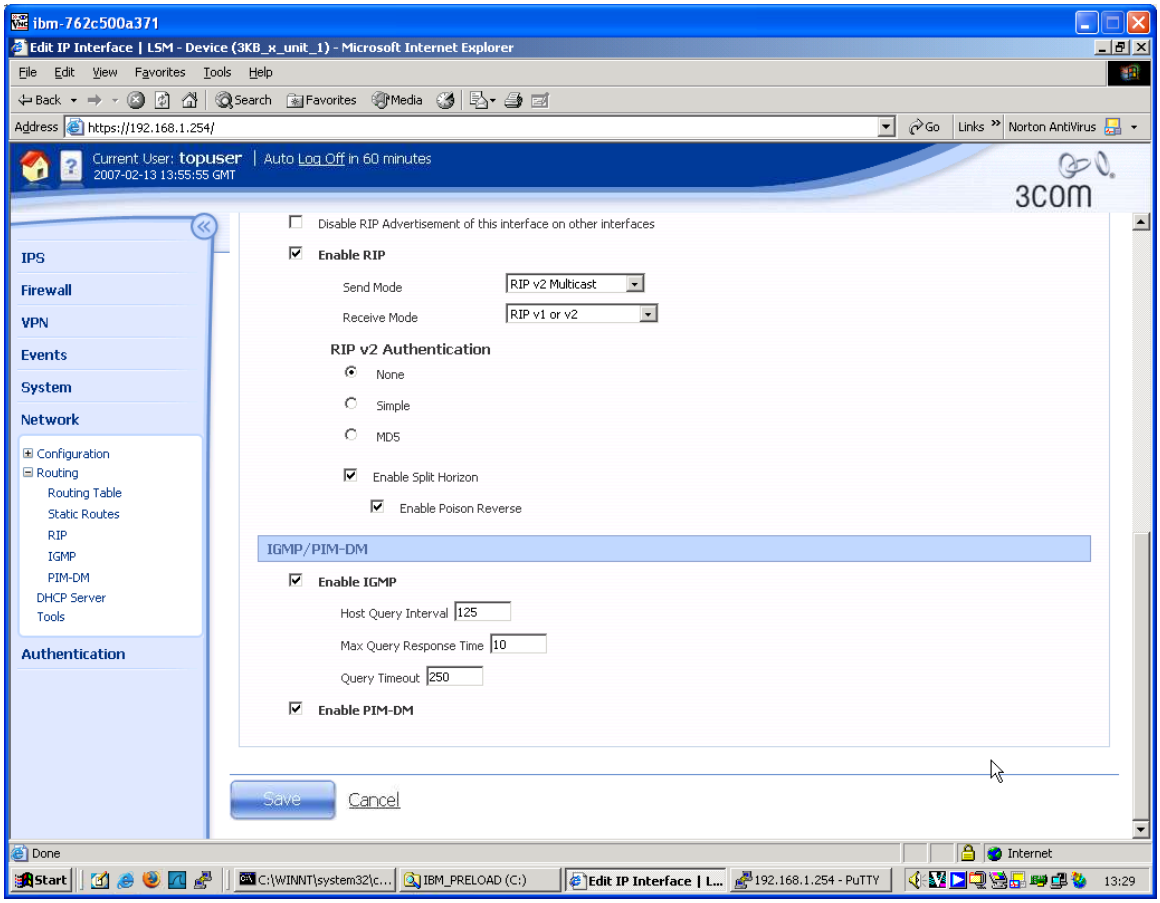
1. Firstly globally enable IGMP on the Network->Routing->IGMP page by checking the "Enable IGMP" checkbox and clicking "Apply".



2. Then, on the same page, click on the internal interface and complete the form as shown below. You will need to click the "Show Advanced Options" hyperlink to access the "Enable IGMP" checkbox.



3. Click on “Save” to save the change.
4. Then do the same for the GRE interface.



5. Click on "Save" to save the change.
6. Check the changes worked via the CLI:

```
3KB_x_unit_1# show routing multi

IGMP Querier Status

Interface  IP Address       Querier          Groups
---------- ---------------- ---------------- ----------------
1          192.168.1.254    192.168.1.254
2          10.10.20.147
3          100.100.100.1    100.100.100.1

PIM-DM Neighbor Table

Neighbor         Interface  Uptime     Expires    Version
---------------- ---------- ---------- ---------- ----------
100.100.100.2    3          113        83         2


Multicast Routing Table

Source IP        Group IP         Next Hop IP      Age
---------------- ---------------- ---------------- ----------
```

```
3KB_x_unit_1#
```

Note the Querier addresses.

7.3.2 Configuring the 3Com 5642 Router

1. Using direct console port connection, telnet or SSH, login to the 5642 Command Line Interface and perform the sequence of commands shown below to enable multicast routing and to enable IGMP globally and on the GRE Tunnel and internal Ethernet interfaces:

```
<OTHER>system-view
System View: return to User View with Ctrl+Z.
[OTHER]interface Tunnel 0
[OTHER-Tunnel0]igmp enable
[OTHER-Tunnel0]interface Ethernet0/1
[OTHER-Ethernet0/1]igmp enable
[OTHER-Ethernet0/1]quit
[OTHER]
```

2. Now check that this worked:

```
[OTHER]display igmp interface
Ethernet0/1 (192.168.22.254):
  IGMP is enabled
  Current IGMP version is 2
  Value of query interval for IGMP(in seconds): 60
  Value of other querier time out for IGMP(in seconds): 120
  Value of maximum query response time for IGMP(in seconds): 10
  Value of robust count for IGMP: 2
  Value of startup query interval for IGMP(in seconds): 15
  Value of last member query interval for IGMP(in seconds): 1
  Value of query timeout for IGMP version 1(in seconds): 400
  Policy to accept IGMP reports: none
  Querier for IGMP: 192.168.22.254 (this router)
  IGMP group limit is 1024
  Total 1 IGMP group reported

Tunnel0 (100.100.100.2):
  IGMP is enabled
  Current IGMP version is 2
  Value of query interval for IGMP(in seconds): 60
  Value of other querier time out for IGMP(in seconds): 120
  Value of maximum query response time for IGMP(in seconds): 10
  Value of robust count for IGMP: 2
  Value of startup query interval for IGMP(in seconds): 15
  Value of last member query interval for IGMP(in seconds): 1
  Value of query timeout for IGMP version 1(in seconds): 400
  Policy to accept IGMP reports: none
  Querier for IGMP: 100.100.100.2 (this router)
  IGMP group limit is 1024
  No IGMP group reported

[OTHER]
```

Note two interfaces have IGMP enabled and the internal interface is seeing a multicast group.

7.3.3 Testing

Each configuration step in this Appendix has been tested as far as possible, but we now need real multicast traffic to test that all this works together.

VideoLAN's VLC is available free here:

http://www.videolan.org/vlc/

It can be used as both a streaming multicast server and as a client. Both can run on the same PC concurrently.

1. Install VLC on both PC1 and PC2.
2. Start the server running on PC1 and streaming out a multicast stream (on address 239.250.1.1) by the following command in a command window:

   ```
   vlc  -vvv Dolphins_720.wmv --sout udp:@239.255.1.1  --ttl 5
   --loop
   ```

   Where `Dolphins_720.wmv` should be replaced with the filename of a suitable video file.

3. Then start a VLC client running on the same machine as a simple check that the server is running.

   ```
   vlc -vvv udp:@239.255.1.1
   ```

4. The client on PC1 should open up and display the video – looped indefinitely.
5. Now start a VLC client running on PC2.

   ```
   vlc -vvv udp:@239.255.1.1
   ```

6. The client on PC2 should open up and display the video – looped indefinitely.

Note: The above commands work on older versions of VLC. Newer versions of VLC may be set up more easily using the GUI than the command line.

7.4 Use with NBX.

There is no special setup required on the NBX NCP. The NCP default multicast addresses will be used for the multicast groups (e.g. for Conference Calls, Paging, etc.). In order to take part in calls with Layer 3 phones, Layer 2 phones will require an IP address to be allocated (e.g. by using a IP-on-the-Fly address pool). Layer 3 phones can either use static IP addresses or pick up addresses from the X-family device using DHCP.