speedtouch™

Connecting a SpeedTouch™608/620 to a Cisco IOS Router

Author: Jan Wuyts

Date: January 2006

Version: v1.0

Abstract: This application note describes how a Virtual Private Network can be created with a SpeedTouch™ at one peer as a VPN client and a Cisco IOS router at the other peer, acting as a VPN server.
Two typical application scenarios are presented:
First of all, a typical teleworker scenario is discussed. A single user wants remote access to the network of his company.
Secondly, a branch office scenario is discussed. A small branch office wants access to the corporate network for multiple terminals.
Configuration examples for both the SpeedTouch™ and the Cisco IOS router are provided.
With this application note, you should be able to get started building your own VPN configuration in your network environment.

Applicability: This application note applies to:

- SpeedTouch™608 (Wireless) Business DSL Routers Release R5.3.0 and higher
- SpeedTouch™620 Wireless Business DSL Router Release R5.3.0 and higher.

Note that for the SpeedTouch™620 you must activate the VPN software module in order to get access to the IPSec VPN functions described in this document.

Updates: THOMSON continuously develops new solutions, but is also committed to improve its existing products.

For more information on THOMSON's latest technological innovations, documents and software releases, visit us at:

http://www.speedtouch.com

Contents

1 SCOPE

Application scenarios

This Application Note describes how to connect a SpeedTouch™ to a Cisco Security Gateway (with Cisco IOS) in order to build a secure VPN based on IPSec connections. The SpeedTouch™ acts as the VPN client, while the Cisco Gateway acts as the VPN server. This document shows how to configure the SpeedTouch™ via its Graphical User Interface (GUI), and how the Cisco router should be configured. The basic configurations described in this document allow you to set up a simple, yet realistic VPN network that demonstrates some advanced VPN features of the SpeedTouch™.

Two typical application scenarios are given here:

- ***A basic teleworker scenario.*** A single computer wants to access a corporate network from a remote location via a secure connection over the public Internet. In addition, this user has local access to public Internet sites (split tunneling).
- ***Remote office connection.*** A number of computers in a local network of a branch office share a single secure tunnel over the public Internet to a corporate network. Besides the local traffic of the branch office, and the secure corporate traffic, local access to the public Internet may be allowed, or not. This depends on the corporate's security policy.

These scenarios are explained in more detail in separate chapters.

Prerequisites

It is assumed that the user is familiar with the basic configuration procedures of both the SpeedTouch™ and Cisco IOS.

IP connectivity over the public Internet is established between the peers of the connection. At the client side the connection to the Internet can be based on either one of the access modes of the SpeedTouch™. In this application note, a routed mode is assumed, so the SpeedTouch™ has a public IP address at the WAN side. This address may either be statically configured, or dynamically assigned by the ISP.

If you have a SpeedTouch™620, you need to enable the VPN software module. To activate this VPN module, you have to acquire the optional software activation key. To check whether the software activation key is present, browse to the SpeedTouch™ Web pages and go to **Expert Mode > SpeedTouch > Add-On**. This page shows which keys are enabled. For more information, see the SpeedTouch™ Operator's Guide R5.3.0 and higher.

2 TELEWORKER SCENARIO

Introduction

In this scenario, a residential network is connected to a corporate network via a secure VPN connection. The residential network is connected to the Internet via a SpeedTouch™ Business DSL router. The corporate network uses a Cisco IOS router as a gateway to the Internet.

2.1 Characteristics of the scenario

At the client side

Initially, a small private network is present at the client side. A SpeedTouch™ is used as an ethernet switch and as a gateway router for Internet access. Typically, in this environment various members of a family have access to this private network.

This configuration is enhanced to provide a secure access to a corporate network for teleworking. Typically, a single user is allowed to access this secure connection. Meanwhile, all users are still capable to communicate on the private network, and have local access to the Internet. The SpeedTouch™ needs to be configured as an IPSec VPN client. The SpeedTouch™ is the peer of the IPSec connection at the client side. No IPSec client software is required on the computer of the user.

It is assumed that at any time only a single computer at the teleworker's premises will be granted access to the corporate network. Simultaneous access of multiple computers from a single remote site is not covered by this scenario.

At the corporate side

The corporate network uses a Cisco IOS router as a gateway to the Internet. In order to allow secure connections with teleworkers, this router has to be configured as a VPN server. In IPSec terms, it acts as the Security Gateway at the corporate peer.

Advantages of using the VPN client of the SpeedTouch™

There are several advantages to this network configuration where the VPN client is located in the SpeedTouch™ instead of using VPN client software installed on the computer of the end user.

- The administrator of the corporate network does not have to worry about upgrades of the Operating System on the teleworker's computer (Windows upgrades, new service packs,...). The operation of the VPN client in the SpeedTouch™ is not affected by these upgrades.
- Since the VPN client is fully integrated in the SpeedTouch™, it can not be tampered with, and is probably more secure than software residing on a computer.
- Adverse interactions with computer software, such as firewalls, PPPoE clients, wireless drivers, viruses and worms are avoided. This guarantees a better stability and fewer functionality problems.

2.1.1 Overview of the initial network environment

Illustration

The following figure gives a general overview of the initial network environment. The figure shows an example of two peers, connected to the public Internet via their respective Internet Service Provider.

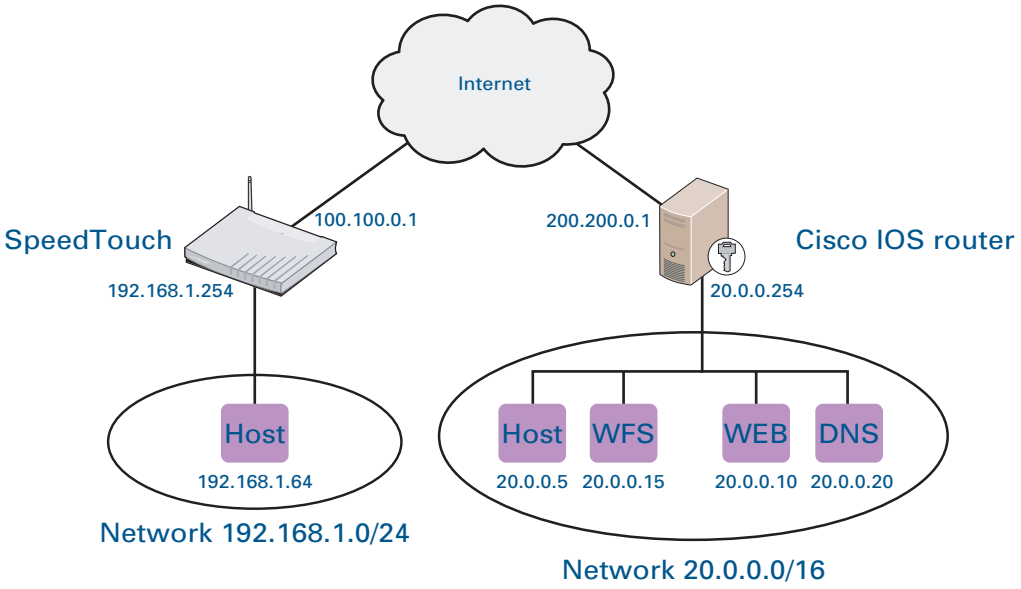


Figure 1: Initial network environment

Public IP addresses

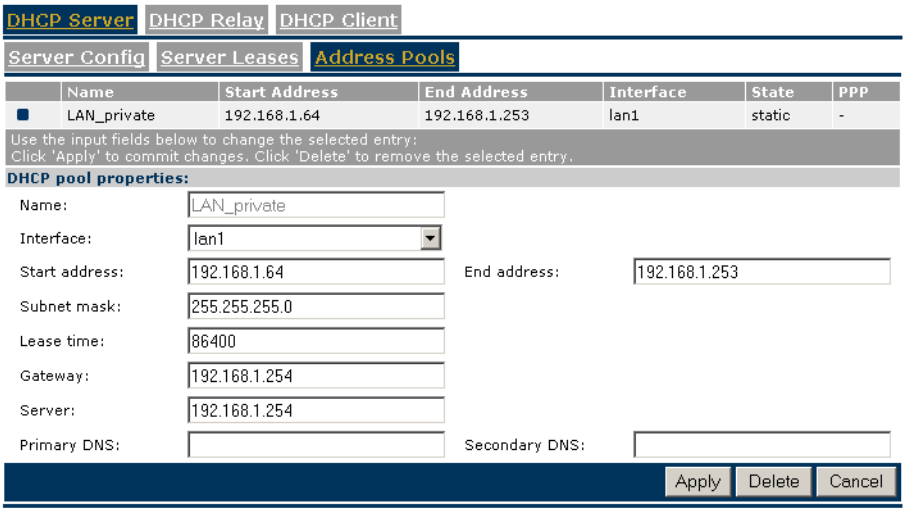
Both peers have a public IP address, assigned by their respective ISP.

At the client side, the public IP address 100.100.0.1 is typically assigned in a dynamic way by the ISP. This means that it has to be considered as a variable: for each session, a different address is attributed to the WAN interface of the SpeedTouch™.

At the corporate office, it is more likely to find a permanently assigned public IP address on the WAN interface. In addition, the corporate router may be known on the Internet by its Fully Qualified Domain Name (something like **vpn.corporate.com**).

Local network environment at the client peer

The teleworker may have a small local network, connected to the Ethernet interfaces of his SpeedTouch™. Typically, he uses dynamic IP addressing on his network, with the SpeedTouch™ acting as a DHCP server. In the example shown in Figure 1, the local network has the address range 192.168.1.0/24, configured as default private address pool in the DHCP pool of the SpeedTouch™.



The LAN interface of the SpeedTouch™ has address 192.168.1.254 and is the default gateway for this network.

Domain name resolving is provided by the SpeedTouch™ DNS server, which consults the DNS server of the Internet Service Provider in case no entry is found for a particular request.

Local network environment at the corporate peer

The corporate local network is typically a large network comprising a number of subnetworks, and providing a variety of services. In this application note only a few relevant aspects of this network are highlighted. Dynamic IP addressing is used on this network, with a local DHCP server attributing IP addresses to the local computers. This service may be provided by the Cisco IOS router. In the example shown in Figure 1, the corporate network has the address range 20.0.0.0/16, The LAN interface of the Cisco router is the gateway for this network and has address 20.0.0.254.

A DNS server is present in the corporate network for resolving domain names. In the example of Figure 1, the DNS server has address 20.0.0.20. Furthermore the figure shows a Web server (for example **intranet.corporate.com**) at address 20.0.0.10, and a computer offering Windows File Sharing service (WFS) at address 20.0.0.15.

2.1.2 The target network

Illustration

The following figure gives a general overview of the target network environment. The figure shows an example of two peers, connected to each other via a secure IPSec tunnel over the public Internet.

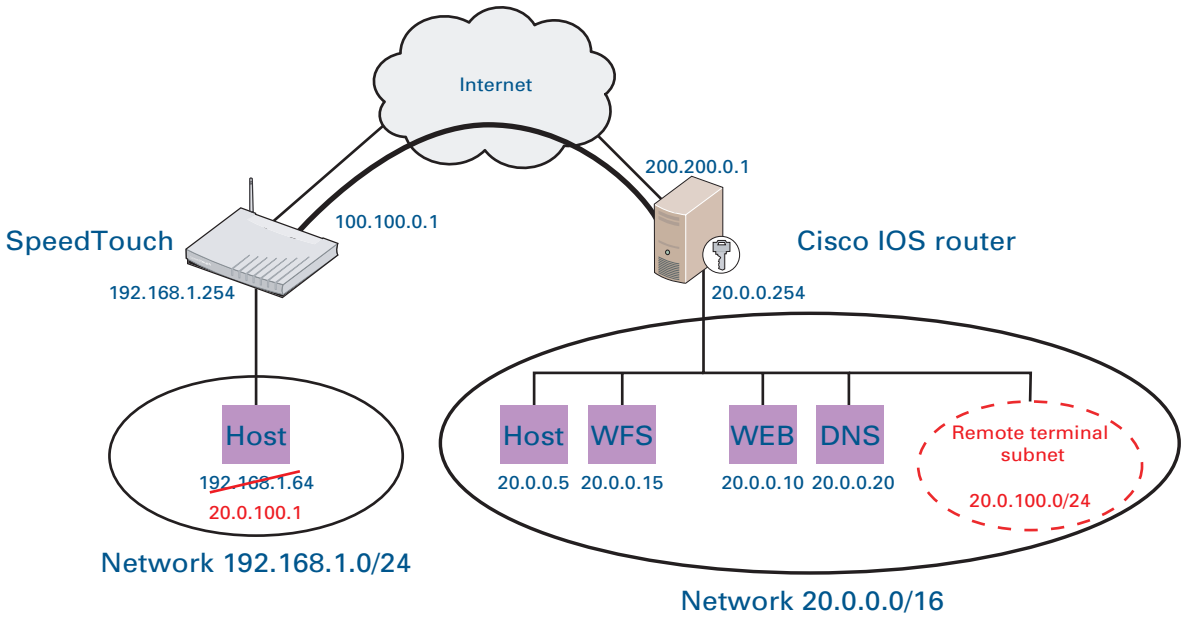


Figure 2: Target network environment

Integrating the teleworkers in the address range of the corporate IP network

The company wants to grant teleworkers a secure access to the corporate network via the Cisco IOS router that will act as a gateway. The teleworkers will be able to access hosts on the corporate network as if they were physically present on the corporate network. The secure connections over the public Internet will make use of IPSec tunnels.

To integrate the teleworkers in the address range of the corporate network, the subnetwork 20.0.100.0/24 is dedicated to these virtual terminals (see Figure 1). In this subnetwork, IP addresses are attributed to the remote terminals in a dynamic way by a DHCP server in the corporate network. We will implement this service by configuring a DHCP server and an address pool for teleworkers on the Cisco IOS router.

This network architecture is called extruded network: an entire subnetwork is located at a remote location. This situation is typical for a large corporate network, where subnets are defined for the various departments.

Providing an IP address to a teleworker

As explained above, the computer of the teleworker is attributed an IP address in the range of the corporate network. In the IPSec protocol framework a protocol, called IKE Mode Config, provides for the transfer of configuration parameters to remote gateways and hosts. In this scenario, IKE Mode Config is used for transferring to the remote SpeedTouch™ an IP address attributed by the Cisco gateway. The SpeedTouch™ can be configured to pass that IP address to the computer of the teleworker. This mode of operation is possible only when the teleworker has access to the corporate network for a single computer at a time.

Teleworker access to the corporate DNS server

Teleworkers should be able to use the corporate DNS server for domain name resolving when they are connected to the corporate network. In the initial network environment, the SpeedTouch™ provides the DNS service to the user, and contacts the DNS server of the ISP for locally unresolvable names.

In the corporate network environment, the computer of the teleworker should use the corporate DNS server. To this end, IKE Mode Config communicates the location of the corporate DNS server to the remote SpeedTouch™, which in its turn transfers it to the host.

IKE Mode Config capabilities of Cisco IOS

The Cisco IOS devices support the following IKE Mode Config functionality:

- Virtual IP address
- Primary DNS
- Primary WINS
- Address Expiry. The IP address lifetime is always equal to the remainder of the lifetime of the Phase 1 Security Association. Therefore, virtual address refreshing only takes place after rekeying of the Phase 1 SA.
- Domain name
- Split-tunneling remote subnets.

2.1.3 Securing the access to the corporate network

Use of secure connections

The IPSec protocol framework is used for the implementation of this secure VPN. A teleworker will dial in to the VPN server in order to set up the secure connections. The security parameters for the IPSec connections, such as encryption and message authentication algorithms, are selected in function of the security policy in the VPN. The security parameters configured at both peers of the connection must match in order to successfully complete the IPSec tunnel negotiations.

Matching networks

In the IPSec negotiations, the description of the local and remote private networks forms part of the security policy. The peers exchange information about which networks are accessible. When peers fail to agree on their common knowledge of the VPN layout, the negotiations are aborted.

Authenticating teleworkers

Two levels of user authentication can be applied in this scenario.

First of all, the establishment of an IPSec connection requires user authentication. Two mechanisms are foreseen in the IPSec framework:

- pre-shared key authentication
- authentication with certificates

In this Application Note pre-shared key authentication is used.

An additional level of user authentication can be established, making use of the Extended Authentication protocol (XAuth). This protocol allows you to define a user group on the VPN server (the Cisco IOS router in this case), where each teleworker authenticates with a user name and password. Each time when the connection is started, the user is prompted to enter his user name and password.

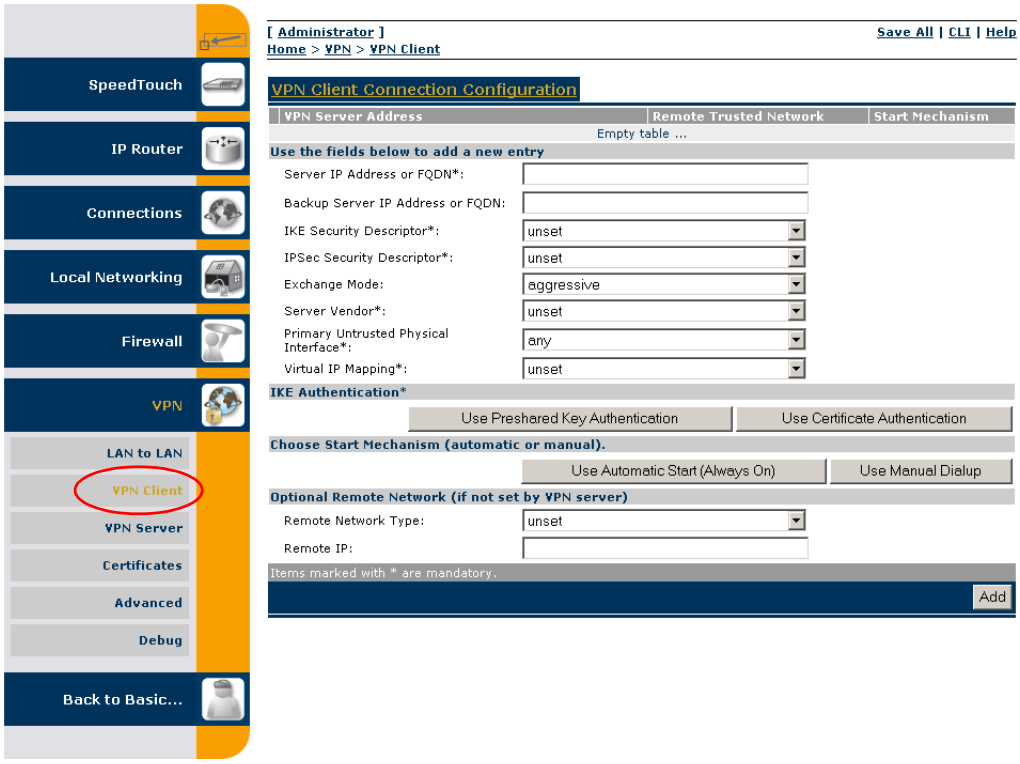
This teleworker scenario describes the use of XAuth.

2.2 Configuring the SpeedTouch™

VPN client configuration procedure outline

Configure the VPN client on the SpeedTouch™ via the internal Web pages.

1. Browse to the SpeedTouch™ Web pages at **http://speedtouch** or at IP address **192.168.1.254**.
2. Go to **Expert mode > VPN > VPN Client**.



3. Fill out the VPN client parameters (see "2.2.1 Fill out the VPN Client parameters" on page 12).
4. Select the IKE Authentication method (see "2.2.2 Select the IKE Authentication method" on page 15).
5. Select the Start Mechanism (see "2.2.3 Select the Start Mechanism" on page 16).

2.2.1 Fill out the VPN Client parameters

Procedure

Proceed as follows:

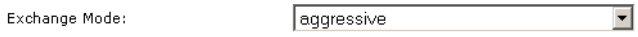
1. Fill out the publicly known network location of the Cisco VPN server. This may be the public IP address, if it is invariable and known to the teleworker. In general, however, it is the publicly known FQDN, such as **vpn.corporate.com**.

2. Leave the **Backup Server IP address or FQDN** field open. This field can be filled out in configurations with a backup server. This is beyond the scope of the present homeworker scenario.

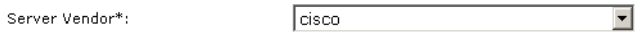
3. Select the **IKE Security Descriptor**. In our example, the pre-configured **DES_MD5** descriptor is selected. For more information, see " IKE Security Descriptor" on page 13.

4. Select the **IPSec Security Descriptor**. In our example, the pre-configured **DES_MD5_TUN** descriptor is selected. For more information, see" IPSec Security Descriptor" on page 14.

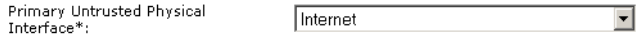
5. Select the **IKE Exchange Mode**: Select **aggressive**. For more information, see " Exchange Mode" on page 14.



6. Select the **Server Vendor**: select **cisco**.



7. Select the **Primary Untrusted Physical Interface**. Select the name of your Internet interface from the list. In our example the Internet connection is called: **Internet**.



8. Select the **Virtual IP Mapping** method: select **dhcp**. For more information, see " Virtual IP mapping" on page 15.

IKE Security Descriptor

The IKE Security Descriptor bundles the security parameters used for the IKE Security Association (Phase1). A number of pre-configured IKE Security Descriptors can be selected from a list. In addition, you can define your own Security Descriptors (this is beyond the scope of this Application Note).

You have to select a Security Descriptor in compliance with the IKE security parameters configured in the Cisco IOS gateway.

In our example the pre-configured **DES_MD5** descriptor is selected. This descriptor contains the following settings:

Parameter	Example: **DES_MD5**
Cryptographic function	DES
Hash function	HMAC-MD5
Diffie-Hellman group	MODP768 (= group 1)
IKE SA lifetime in seconds.	3600 seconds (= 1 hour)

The contents of the IKE Security Descriptors can be verified via **Advanced > Peers > Security Descriptors**.

It is recommended to use **AES** as preferred encryption method. AES is more advanced, compared to DES or 3DES. It is faster for comparable key lengths, and provides better security.

However, AES is not available in all versions of Cisco IOS. Therefore, DES is selected in our example, since it is the default encryption algorithm in Cisco IOS.

IPSec Security Descriptor

The IPSec Security Descriptor bundles the security parameters used for the Phase 2 Security Association. A number of pre-configured IPSec Security Descriptors can be selected from a list. In addition, you can define your own Security Descriptors (this is beyond the scope of this Application Note).

You have to select a Security Descriptor in compliance with the IPSec security parameters configured in your Cisco IOS router.

In our example, the pre-configured **DES_MD5_TUN** descriptor is selected. This descriptor contains the following settings:

Parameter	Example: **DES_MD5_TUN**
Cryptographic function	DES
Hash function	HMAC-MD5
Use of Perfect Forward Secrecy	no
IPSec SA lifetime in seconds.	86400 seconds (= 24 hours)
IPSec SA volume lifetime in kbytes.	no volume limit
The ESP encapsulation mode	tunnel

The contents of the IPSec Security Descriptors can be verified via **Advanced > Connections > Descriptors**.

It is mandatory to select an IPSec Security Descriptor that uses ***tunnel*** mode as **ESP Encapsulation mode.**

It is recommended to use **AES** as preferred encryption method. AES is more advanced, compared to DES or 3DES. It is faster for comparable key lengths, and provides better security.

However, AES is not available in all versions of Cisco IOS. Therefore, DES is selected in our example, since it is the default encryption algorithm in Cisco IOS.

Exchange Mode

IKE specifies two modes of operation for the Phase 1 negotiations: main mode and aggressive mode. Main mode is more secure while aggressive mode is quicker. In main mode, the identity of the communicating parties is not revealed on the public Internet because it is transferred in encrypted form. In order to do so, the encryption and message authentication are negotiated before the identities are exchanged. This results in more messages than the aggressive mode IKE negotiations.

In our teleworker scenario, the use of main mode is excluded due to limitations of the Cisco IOS implementation of the VPN server functionality. In the scenarios presented in this Application Note, the Cisco VPN server attributes a private IP address to the VPN client via IKE Mode Config. In this kind of scenario, Cisco only supports aggressive mode.

Therefore it is mandatory to select **aggressive** mode for the Phase 1 negotiation.

If a SpeedTouch™ would be used at the VPN server side instead of a Cisco IOS device, it would be possible to use main mode.

Virtual IP mapping

The selection of **dhcp** as virtual IP address mapping has the effect that the virtual IP address attributed by the VPN server to the SpeedTouch™ VPN client is effectively assigned to the teleworker's computer. The SpeedTouch™ creates a new IP address pool, called a spoofing address pool. The SpeedTouch™will use this pool to provide a new IP address to the terminal that starts the secure connection. Simultaneous access to the VPN of multiple terminals in the LAN is not possible. The VPN server attributes only a single virtual IP address

The ***spoofing address pool*** inherits the lease time for IP addresses from the ***originally used address pool.*** In order to have a swift renewal of IP addresses, it is advised to set a conveniently low lease time in the original dhcp address pool. A value of 1 minute is recommended.

As an alternative, you can force a renewal of the leased IP address of the computer.

As an alternative, the teleworker scenario could also make use of the **nat Virtual IP Mapping** method. For more information, see the SpeedTouch™ IPSec Quick Start Guide and the SpeedTouch™ IPSec Configuration Guide.

The **dhcp** method has the advantage that it supports all applications, even those applications for which the SpeedTouch™ has no NAPT Application Layer Gateway (ALG) to help the application across Network Address and Port Translation (NAPT), e.g. Unix X-applications.

The **nat** method on the other hand has the advantage that it is not needed to renew the computer's IP address via the DHCP protocol, which poses less problems with IP connectivity. The VPN connection is available immediately when dialling in. In the local LAN, the local addressing remains unchanged.

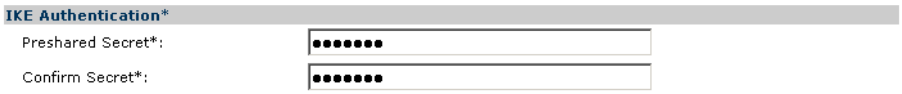
2.2.2 Select the IKE Authentication method

Procedure

Proceed as follows:

1. Select **Use Preshared Key Authentication**.

2. Enter the pre-shared key: a character string to be used as a password for the VPN connection.This secret needs to be identically configured in the VPN client and VPN server.



The pre-shared key value is not shown in clear text on the SpeedTouch™ Web page. In order to protect for typing errors, the key has to be to entered twice, to confirm your entry.

2.2.3 Select the Start Mechanism

Manual start

As a teleworker, you will dial in to the corporate network when needed. Each time you will have to enter your user name and password.

In addition, the selection of the manual start mechanism implies that only the terminal where the dial-in procedure is initiated gets access to the VPN connection. All other terminals can reach the Internet via the SpeedTouch™, but cannot reach the corporate network.

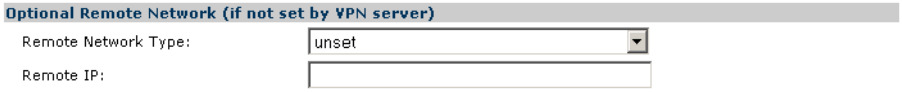
For the teleworker scenario this is the most appropriate option from a security point of view.

Procedure

Proceed as follows:

1. Select **Use Manual Dialup**.

2. Leave the **Optional Remote Network** fields open, as shown below.



These settings allow you to limit the accessible area of the corporate network.

3. Click **Add** at the bottom of the page.
4. Click **Save All** to save the SpeedTouch™ configuration.

All the VPN client configuration parameters have now been entered in the SpeedTouch™.

Section "2.3 Dialling in to the Cisco VPN server" on page 16 describes the manual dial-in procedure.

You can only dial in successfully when the Cisco IOS router is configured properly. For more information, see "2.6 Configuring the Cisco IOS router" on page 26.

2.3 Dialling in to the Cisco VPN server

About DHCP and IP address renewal

During the IKE negotiations, the SpeedTouch™ VPN client receives a new lease for an IP address in the corporate network range. By selecting **dhcp** as **Virtual IP Mapping** in the VPN client, this IP address will effectively be leased to the teleworker's host. The SpeedTouch™ DHCP server will attribute this address to the host at the first address renewal. In the DHCP protocol, the DHCP client initiates the address renewal. In order to get a swift renewal of the IP address, you have to:

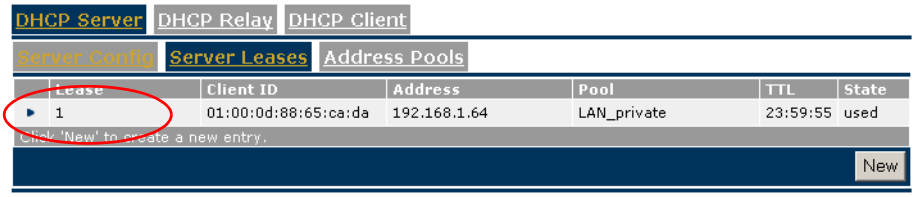
- set a conveniently low lease time in the SpeedTouch™ DHCP server before you dial in to the VPN server
- renew the IP address of your computer after the VPN connection is established ***for the first time***.

For the DHCP lease time, a value of about 60 seconds is recommended. The renewal interval is half of the lease time.

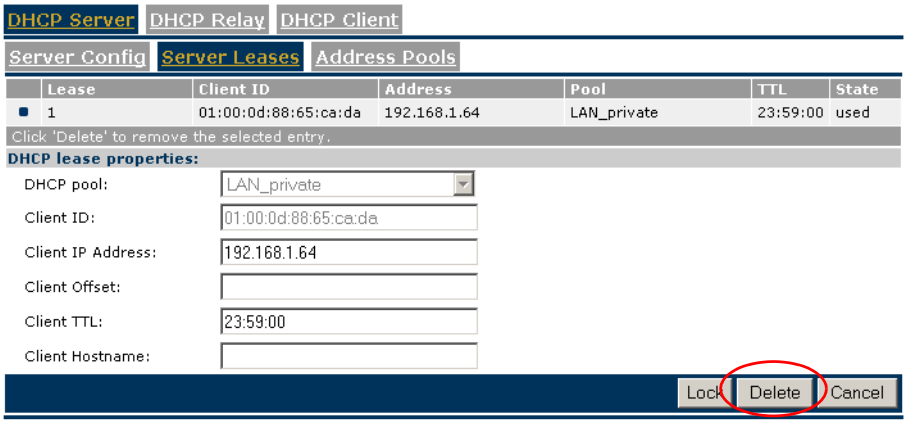
Adjust the DHCP lease time in your SpeedTouch™

Proceed as follows:

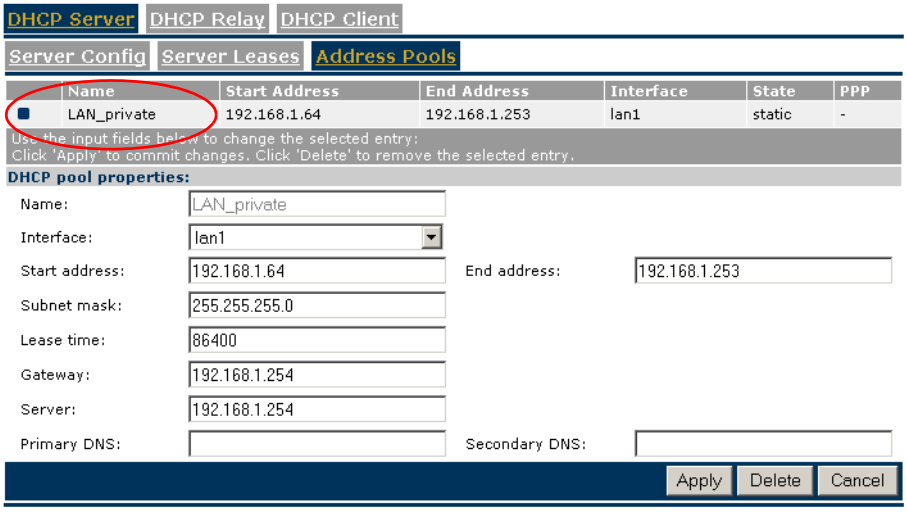
1. Browse to the SpeedTouch™ Web pages.
2. Go to **Expert Mode > Local Networking > DHCP Server > Server leases**.



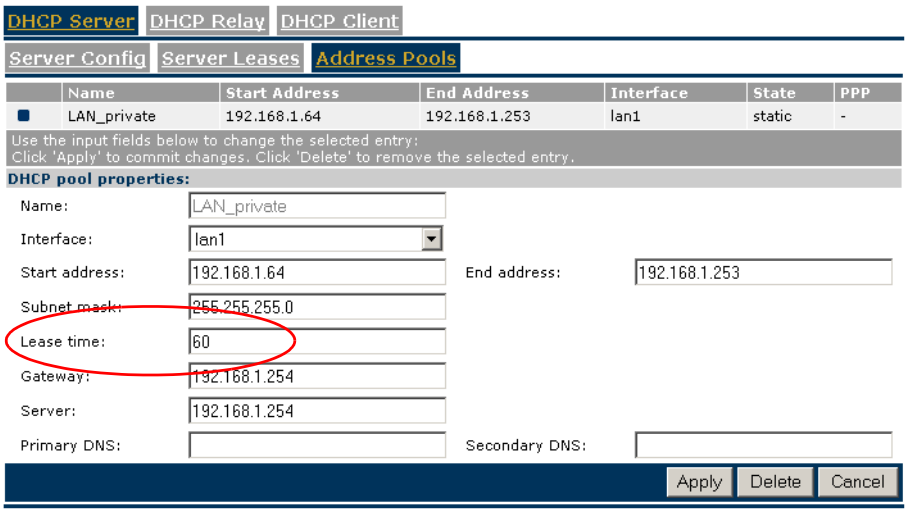
3. If an active lease exists, select the lease attributed to your computer and click **Delete**.



4. Browse to **Address Pools** and select the private LAN address pool.



5 Set the **Lease time** to a conveniently low value, for example 60 seconds.



Setting the lease time to 60 seconds will have the effect that the terminal starts the renewal procedure every 30 seconds. Renewals occur each time when half of the lease time period has passed.

6 Click **Apply** and **Save All** to make your settings permanent.

Now your SpeedTouch™ is ready to dial in to the VPN server.

Dialling in from the SpeedTouch™ home page

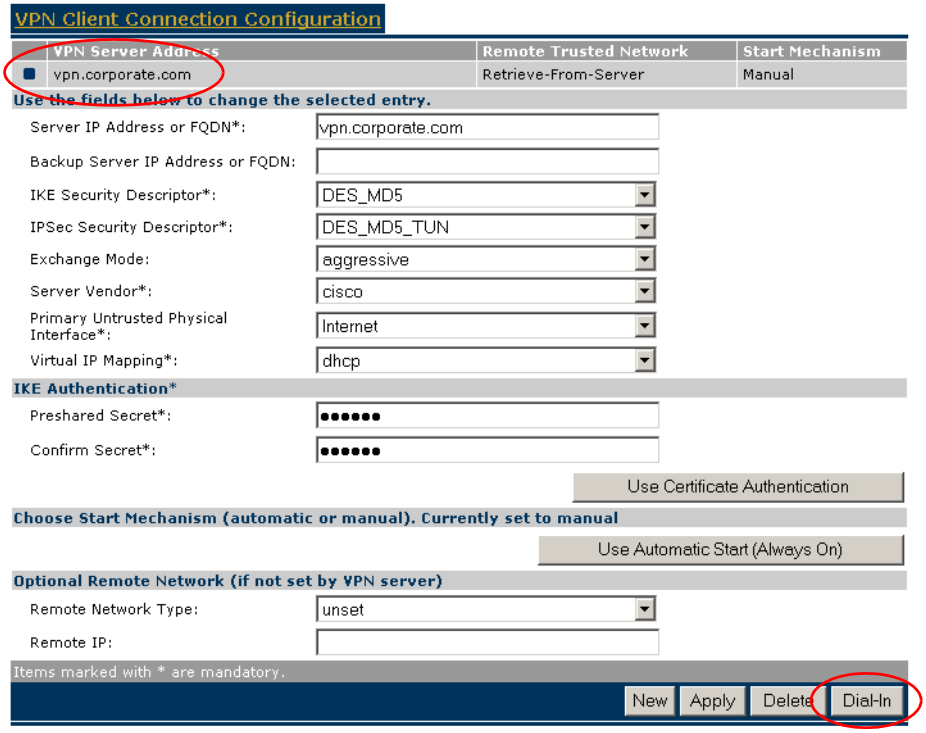
You can dial in to the VPN server using the link on the SpeedTouch™ **home** page. When you define a VPN client, a link is automatically added to the **Broadband Connections** on the **home** page.

In order to dial in successfully, it is required that the Cisco VPN server is properly configured. For more information, see “2.6 Configuring the Cisco IOS router” on page 26.

Dialling in from the VPN Client Connection Configuration page

Proceed as follows:

1 Select the formerly configured VPN client configuration:



2 Click **Dial-in** to start the dial-in procedure.

In order to dial in successfully, it is required that the Cisco VPN server is properly configured. For more information, see "2.6 Configuring the Cisco IOS router" on page 26.

Authenticating yourself with the VPN server

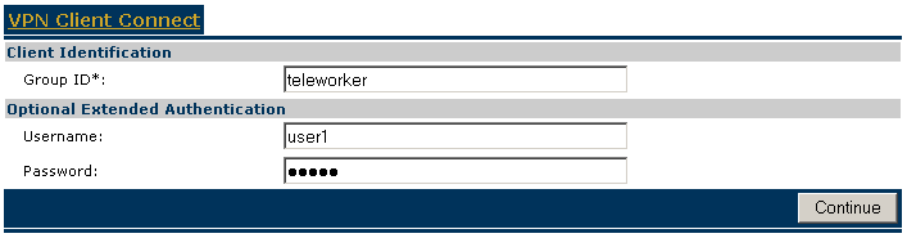
In order to gain access to the corporate network, you need to provide the **client Identification**. In addition, the **Optional Extended Authentication** is used.

Proceed as follows:

1. Fill out the **Group ID** with the group name as configured on the Cisco VPN server for the group of teleworkers.

   In our example this group is called **teleworker**. (See " How to define a client group" on page 29.)

2. Fill out the **Username** and **Password** of a registered user of the Cisco VPN server.



   In our scenario the **Extended Authentication** is used. This allows individual authentication for each individual teleworker. In the Cisco IOS router either a local user list is checked, or a RADIUS server is consulted to control the access to the corporate network.

3. Click **Continue**.

   The dial-in process starts. While the negotiations are ongoing, the following message is displayed.

   Dialup Attempt in Progress -- Please be patient. Page will automatically refresh

   When the connection is established, the following message is displayed.

   Dialup Successful

Now you have to wait until your computer gets a new IP address from the SpeedTouch™ DHCP server.

You can speed up the process by manually requesting a new IP address for your computer. For more information, see" About DHCP and IP address renewal" on page 16.

As soon as your computer has received an IP address in the range of the corporate network, your secure remote connection is operational.

For Microsoft Windows networks: logging on to the WinNT domain of the corporate network requires you to log off and log on again to Windows NT/XP.

First-time connection to the VPN server

When you connect to the VPN server for the first time, it may be required to manually renew the IP address of your computer. In general, your computer received an IP address with a long lease time from the SpeedTouch™ DHCP server ***before*** you adjusted the lease time of the DHCP pool. As a consequence, your computer will most likely not start the renewal procedure in a reasonable time. In this period you are not able to communicate with the corporate network. This situation is inherent to the operation of the DHCP protocol.

The most convenient solution to this problem is to temporarily **disable** your network connection, and subsequently **enable** it again. If you do not know how to do this, simply restart your operating system.

It is important to note that this inconvenient situation occurs only when your computer has an IP address with a long lease time. This is typically the case when you connect to the VPN server for the first time after you lowered the lease time of the DHCP pool.

Access your SpeedTouch™ when you are connected to the corporate network

While your computer is using an IP address in the range of the corporate network, it is still able to access the SpeedTouch™ Web pages, which are in general located in another network. The SpeedTouch™ routing functions still assure that you can access the Web pages at the familiar location (e.g. 192.168.1.254 or http://speedtouch) from the teleworker's computer.

Who has access to the corporate network

It is important to note that only the computer from which the dial-in process is started, will have access to the corporate network.

Moreover, the DHCP Virtual IP Mapping method allows the transfer of a single IP address to a single host only. All other hosts that may be present in the LAN do not comply with the traffic policy, and hence are denied access to the VPN. Of course, these hosts may use the other services offered by the SpeedTouch™, such as Internet access.

Surfing through the VPN tunnel

One of the SpeedTouch™ features for easy Internet access is the so-called Differentiated Services Detection (DSD). This feature monitors your HTTP traffic and alerts you when you want to browse to a location that is not reachable due to the fact that the connection to your Service Provider is not active. A SpeedTouch™ Web page appears that allows you to log on to your Service Provider.

When you configure an IPSec VPN connection, this feature has to be disabled in order to pass HTTP traffic through the VPN tunnel.

To verify that the Differentiated Services Detection is disabled, proceed as follows:

1. Browse to **Basic Mode > Toolbox > Web Site Filtering**.
2. Click **Configure**.
3. Verify that the check box "**Use Address Based Filter**" is not selected.

If Differentiated Services Detection is disabled, Web address based filtering is disabled as well. Keep this in mind if you use the Web based filtering tool for parental control.

Testing the VPN connection and troubleshooting

See "Testing the VPN connection" on page 23.

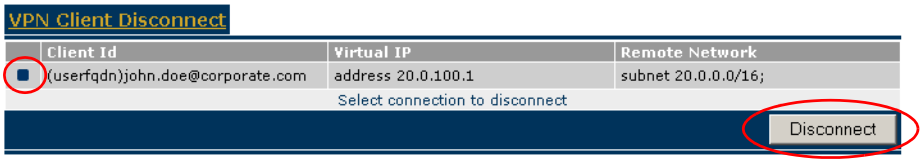
2.4 Closing a VPN connection

Disconnecting

You can disconnect from the VPN server using the link on the SpeedTouch™ **home** page, located under **Broadband Connections**.

As an alternative, you can use the **Disconnect** button on the **VPN Client Connection Configuration** page.

At the bottom of this page, all active VPN connections are shown.



Select the connection you want to terminate and click **Disconnect**.

The secure connection is closed and is removed from the list of active connections

IP address renewal

After you disconnect from the VPN server, the computer still has its IP address in the corporate network range. As a consequence, you temporarily lose connection with the SpeedTouch™. This situation changes only at the first renewal of the computer's IP address. At that moment, the SpeedTouch™ DHCP server leases an IP address in the local LAN environment and IP connectivity is restored.

2.5 Testing the VPN connection

How to verify that the VPN connection is operational

As soon as the VPN connection is active, the teleworker's computer should be able to ping a computer located in the private corporate network. For example, referring to "Figure 2: Target network environment" on page 8, the computer with the new IP address 20.0.100.1 is able to ping the computer with IP address 20.0.0.5.

Use the **debug** pages of the SpeedTouch™ to diagnose any problems.

How to see the status of the VPN connection

Browse to **Expert mode > VPN > Debug > Status**. This page shows the status of the **IKE Security Association (Phase 1)** and the **IPSec Security Association(s) (Phase 2)**. For an operational VPN connection, both an **IKE Security Association** and an **IPSec Security Association** should be active.

Dynamically assigned parameters (such as public IP address) in the debug page examples may differ from the reference networks used throughout this document.

How to monitor the IPSec negotiations

Proceed as follows:

1. Browse to **Expert mode > VPN > Debug > Logging**.
2. Select the desired level of **Trace Detail**. Select **high** to see the most detailed level of logging.
3. Dial-in to the VPN server.
4. Browse again to **Expert mode > VPN > Debug > Logging**.

On the Logging page you can monitor the received and transmitted messages of the IKE and IPSec negotiations. This can help you to diagnose problems during the establishment of VPN connections.

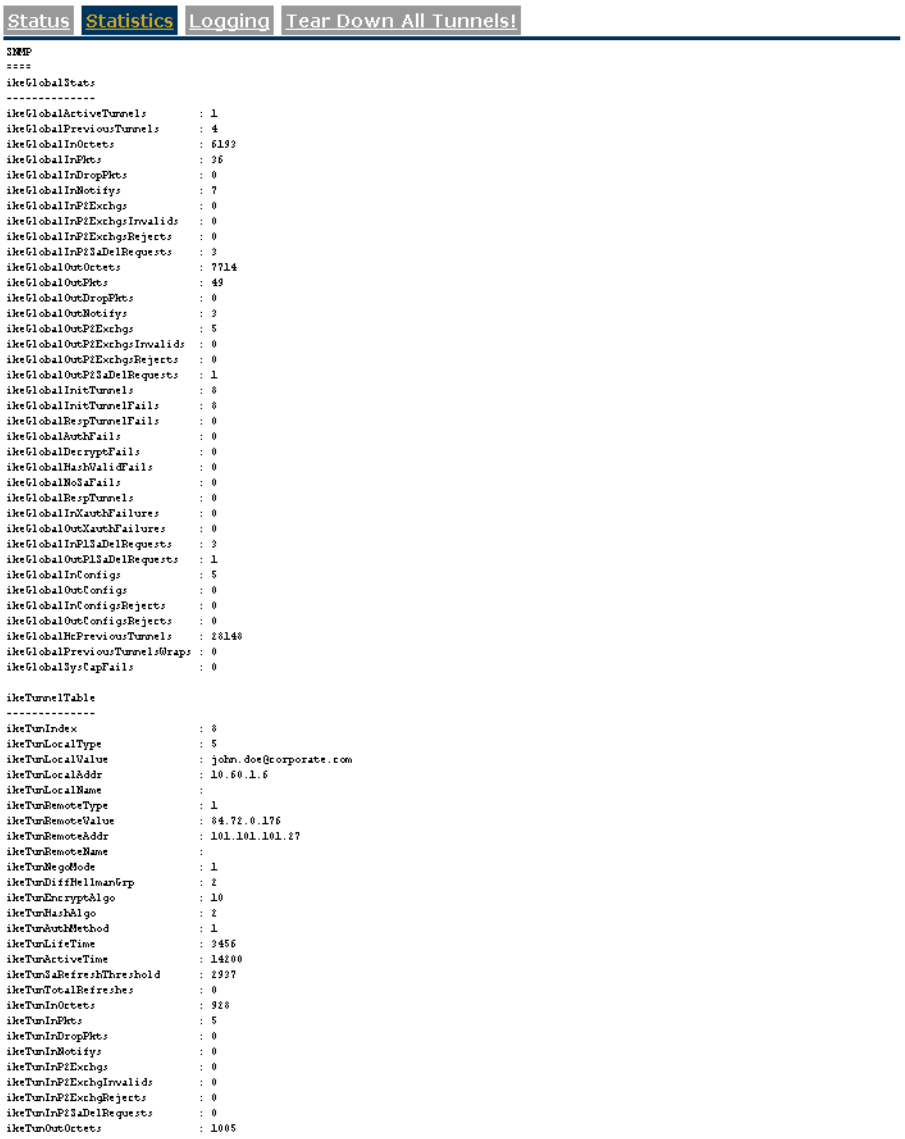
The figure shows the start of the IKE negotiations. You can scroll through the traces to search for the cause of an eventual VPN connection establishment failure.

Click **Clear** to clear the trace.

Click **Refresh** to refresh the page.

How to see the amount of traffic carried by a VPN connection

Browse to **Expert mode > VPN > Debug > Statistics**. This page shows the amount of traffic carried over the **IKE Security Association (Phase 1)** and the **IPSec Security Association(s) (Phase 2)**.



2.6 Configuring the Cisco IOS router

Introduction

It is assumed that you are familiar with the configuration procedures of a Cisco IOS router. In this section, the configuration of a VPN server is explained that complies with the SpeedTouch™ VPN client described in this document. To explain how the Cisco router is configured, the section starts with a printout of a Cisco configuration file. This file has been edited to remove all irrelevant entries. The highlighted commands are discussed briefly in the subsequent sections.

Cisco configuration file

Below, an edited configuration file is shown. It mainly contains the entries that are relevant for the teleworker scenario.

```
Current configuration : 10776 bytes
version 12.3
hostname cisco3660bis
!
username user1 password 0 password1
aaa new-model
!
aaa authentication login xauth_telewrk local
aaa authorization network groupauth_telewrk local
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
!
crypto isakmp client configuration group teleworker
 key secretkey
 dns 20.0.0.20
 pool telewrkpool
 acl 130
!
crypto ipsec transform-set telewrktrset esp-des esp-md5-hmac
!
crypto dynamic-map telewrkdyn 1
 set transform-set telewrktrset
!
crypto map telewrkmap client authentication list xauth_telewrk
crypto map telewrkmap isakmp authorization list groupauth_telewrk
crypto map telewrkmap client configuration address respond
crypto map telewrkmap 1 ipsec-isakmp dynamic telewrkdyn
!
interface ATM3/0.20
 crypto map telewrkmap
!
ip local pool telewrkpool 20.0.100.1 20.0.100.254
ip route 20.0.100.0 255.255.255.0 ATM3/0.20
!
access-list 130 permit ip 20.0.0.0 0.255.255.255 20.0.100.0 0.0.0.255
!
end
```

In the subsequent sections, the blocks in the configuration file are discussed in the order in which they appear in the configuration file.

2.6.1 Setting up the AAA Service

What we want to do

The Extended Authentication of the teleworkers requires the configuration of AAA services on the Cisco IOS router. Only the authentication and authorization services are required. The accounting services are not required.

How to enable the AAA services

Enter the following command:

```
cisco(config)# aaa new-model
```

This command enables the AAA services on the router.

How to define a named method list for authentication

The following command defines a named method list for authentication. This list defines which method(s) will be used to authenticate a user that tries to log on to the network. We define only one method for checking the user identity: a list of users that is locally stored in the router.

```
cisco(config)# aaa authentication login xauth_telewrk local
```

The method list is named: **xauth_telewrk**.
One method is specified in the list: **local**.
This specifies the use of a local user list.

How to define a named method list for authorization

The following command defines a named method list for network authorization. The list defines which method(s) will be used for checking which services are available to a user. We define only one method for checking user service profiles: a list of users that is locally stored in the router.

```
cisco(config)# aaa authorization network groupauth_telewrk local
```

The method list is named: **groupauth_telewrk**.
One method is specified in the list: **local**.
This specifies the use of a local user list.

How to set up a local user list

Enter the following command:

```
cisco(config)# username user1 password 0 password1
cisco(config)#
```

This command creates a single user record with the login name **user1** and the password **password1**.

This is the result in the configuration file

```
username user1 password 0 password1
aaa new-model
!
!
aaa authentication login xauth_telewrk local
aaa authorization network groupauth_telewrk local
```

2.6.2 Defining the security parameters for the IKE SA

What we want to do

This section describes how to define the security parameters for the IKE Security Association. In Cisco terminology, this is called the ***ISAKMP policy***. The security parameters have to be set in compliance with the IKE Security Descriptor selected in the SpeedTouch™ (see " IKE Security Descriptor" on page 13).

How to set the security parameters

Enter the following command:

```
cisco(config)# crypto isakmp policy 10
cisco(config-isakmp)# hash md5
cisco(config-isakmp)# authentication pre-share
cisco(config-isakmp)# exit
cisco(config)#
```

The **crypto isakmp policy** command invokes the ISAKMP policy configuration mode.This is reflected in the appearance of the prompt: **cisco(config-isakmp)#**. In this mode, the following commands are available to set the security parameters in the policy.

Command (in ISAKMP policy config mode)	Default value
encryption	56-bit DES-CBC
hash	SHA-1
authentication	RSA signatures
group	768-bit Diffie-Hellman
lifetime	86400 seconds (= 24 hours)

In our example the **hash** and **authentication** parameters are set to non-default values. The **encryption**, **group** and **lifetime** parameters are not altered in our example. These parameters keep their default value.

This is the result in the configuration file

In the Cisco configuration file, parameters having their default value are not shown in the policy. Because in our example the **encryption**, **group** and **lifetime** parameters have their default value, they are not shown. Only the **hash** and **authentication** parameters are shown.

```
crypto isakmp policy 10
 hash md5
 authentication pre-share
```

2.6.3 Enabling remote configuration of clients (IKE Mode Config)

What we want to do

This section describes how to enable the remote configuration of clients via the IKE Mode Config protocol. The related commands define a user group, and set the relevant parameters applicable to this user group.

These parameters are:

- the pre-shared key
- the location of the DNS server
- the location of the WINS server
- the domain name
- the DHCP address pool to be used
- the access list (i.e. which origin and destination networks are served by the connection).

How to define a client group

Enter the following command:

```
cisco(config)# crypto isakmp client configuration group teleworker
cisco(config-isakmp-group)#
```

This command creates a new group with the name **teleworker**. This name corresponds with the Group ID name to be used in the SpeedTouch™ when dialling in to the Cisco (see " Authenticating yourself with the VPN server" on page 20).

The **crypto isakmp client configuration group** command invokes the ISAKMP group configuration mode. This is reflected in the appearance of the prompt: **cisco(config-isakmp-group)#**. In this mode, we set a number of parameters for the client group.

Set the parameters of the client group

The parameters are set with the commands described in the table below.

Command (in ISAKMP group config mode)	Value	Comment
key	secretkey	The pre-shared key, used by all teleworkers for the Phase 1 negotiation. See SpeedTouch™ setting "2.2.2 Select the IKE Authentication method" on page 15
dns	20.0.0.20	The location of the DNS server in the corporate network.
pool	telewrkpool	Refers to the corporate DHCP address pool to be used for the teleworkers.
acl	130	Refers to the access list number that applies to this connection (see below).

Enter the following commands to set the parameters.

```
cisco(config-isakmp-group)# key secretkey
cisco(config-isakmp-group)# dns 20.0.0.20
cisco(config-isakmp-group)# pool telewrkpool
cisco(config-isakmp-group)# acl 130
cisco(config-isakmp-group)# exit
cisco(config)#
```

In addition to these parameters, also the location of the ***WINS server*** and the ***domain name*** can be remotely configured (with the commands **wins** and **domain**, respectively).

This is the result in the configuration file

```
crypto isakmp client configuration group teleworker
 key secretkey
 dns 20.0.0.20
 pool telewrkpool
 acl 130
```

Defining a domain name

When a domain name is defined, for example corporate.com, this domain name is transferred to the SpeedTouch™ via the IKE Mode Config protocol. The domain name is used to determine the correct server to relay DNS request to, or which domain to add in the Windows DNS lookup search path.

2.6.4 Defining the security parameters for the IPSec SA

What we want to do

This section describes how to define the security parameters for the Phase 2 Security Association (IPSec). In Cisco terminology, this is called an ***ipsec transform-set***. The security parameters have to be set in compliance with the IPSec Security Descriptor selected in the SpeedTouch™ (see " IPSec Security Descriptor" on page 14).

How to set the security parameters

Enter the following command:

```
cisco(config)# crypto ipsec transform-set telewrktrset esp-des esp-md5-hmac
cisco(cfg-crypto-tran)# exit
cisco(config)#
```

The **crypto ipsec transform-set** command invokes the crypto transform configuration mode. This is reflected in the appearance of the prompt: **cisco(cfg-crypto-tran)#**. In this mode, you can adjust the transform set options, such as the encapsulation mode (transport or tunnel). By default, tunnel mode is selected, so in our example we do not have to set any parameter.

This is the result in the configuration file

```
crypto ipsec transform-set telewrktrset esp-des esp-md5-hmac
```

2.6.5 Defining a dynamic crypto map

What we want to do

A dynamic crypto map expresses a dynamic traffic policy. The word dynamic refers to the fact that the remote peer is not known at the moment the router is configured. In the dynamic crypto map we specify the transformation set to be used for the IPSec SA, but no identification or addressing parameters.

How to create a dynamic crypto map

In the following command sequence we create a dynamic crypto map, named **telewrkdyn**. In this dynamic crypto map, we specify to use the transform set, called **telewrktrset**:

```
cisco(config)# crypto dynamic-map telewrkdyn 1
cisco(config-crypto-map)# set transform-set telewrktrset
cisco(config-crypto-map)# exit
cisco(config)#
```

The **crypto dynamic-map** command invokes the crypto map configuration mode. This is reflected in the appearance of the prompt: **cisco(config-crypto-map)#**. In this mode, you can adjust the crypto map parameters, such as the **transform-set** to be used.

This is the result in the configuration file

```
crypto dynamic-map telewrkdyn 1
 set transform-set telewrktrset
```

2.6.6 Defining a crypto map

What we want to do

A crypto map bundles all the parameters describing the access to and the behaviour of the secure connection. It refers to most of the previously defined configuration items, such as the dynamic crypto map and the authentication and authorization methods lists.

How to create a crypto map

In the following command we create a crypto map, named **telewrkmap**:

```
cisco(config)# crypto map telewrkmap 1 ipsec-isakmp dynamic telewrkdyn
cisco(config)#
```

In this definition, we enable the support of dynamic crypto maps by referring to the previously created dynamic crypto map, called **telewrkdyn**

Refer to the authentication method list this crypto map should use

The following command specifies that the crypto map **telewrkmap** should use the previously defined client authentication method list, called **xauth_telewrk**:

```
cisco(config)# crypto map telewrkmap client authentication list xauth_telewrk
cisco(config)#
```

Refer to the authorization method list this crypto map should use

The following command specifies that the crypto map **telewrkmap** should use the previously defined client authorization method list, called **groupauth_telewrk**:

```
cisco(config)# crypto map telewrkmap isakmp authorization list groupauth_telewrk
cisco(config)#
```

Specify the IKE Mode Config operation mode

The Cisco IKE Mode Config implementation can operate either in initiator or responder mode. Responder mode is the preferred mode of operation. In responder mode the SpeedTouch™ requests the required attributes from the Cisco server.

The following command specifies that the crypto map **telewrkmap** should use **responder** mode:

```
cisco(config)# crypto map telewrkmap client configuration address respond
cisco(config)#
```

This is the result in the configuration file

```
crypto map telewrkmap client authentication list xauth_telewrk
crypto map telewrkmap isakmp authorization list groupauth_telewrk
crypto map telewrkmap client configuration address respond
crypto map telewrkmap 1 ipsec-isakmp dynamic telewrkdyn
```

2.6.7 Attach the crypto map to a router interface

What we want to do

In order to activate the previously created crypto map, it must be attached to a router interface.

How to attach a crypto map to an interface

This is done with the following commands:

```
cisco(config)# interface ATM3/0.20
cisco(config-subif)# crypto map telewrkmap
cisco(config-subif)# exit
cisco(config)#
```

The **interface** command invokes the interface configuration mode.

This is the result in the configuration file

```
interface ATM3/0.20
 crypto map telewrkmap
```

2.6.8 Define the corporate DHCP pool for teleworker IP addresses

What we want to do

In this section we define the address range available to distribute IP addresses to remote VPN clients. We define a pool of 254 addresses, ranging from 20.0.100.1 to 20.0.100.254.

How to define an address pool

This is done with the following commands:

```
cisco(config)# ip local pool telewrkpool 20.0.100.1 20.0.100.254
cisco(config)#
```

2.6.9 Add a route to the routing table of the Cisco router

What we want to do

We have to add a route towards the extruded network in the routing table.

How to add a route to the extruded network

This is done with the following commands:

```
cisco(config)# ip route 20.0.100.0 255.255.255.0 ATM3/0.20
cisco(config)#
```

2.6.10 Define an access list

What we want to do

We have to define what the origin and destination networks are for the IPSec connection. This is done via an access list, which is referred to in the crypto map we previously defined (see" Set the parameters of the client group" on page 30).

How to define an access list for the secure connections to the extruded network

This is done with the following commands:

```
cisco(config)# access-list 130 permit ip 20.0.0.0 0.0.255.255 20.0.100.0 0.0.0.255
cisco(config)#
```

The command defines an access list with serial number **130**, which ***permits*** traffic from ***origin*** network **20.0.0.0/16** to ***destination*** network **20.0.100.0/24**.

Cisco uses source and destination wildcards to describe the networks. These wildcards are in fact the logical inversion of subnet masks.

Split tunneling

By defining the access list as described above, only traffic between the network 20.0.100.0/24 and 20.0.0.0/16 is transferred over the secure VPN connection. The teleworker and all other computers in his private LAN have direct access to the Internet via the SpeedTouch™. This mode of operation is called split tunneling. Internet traffic is not transferred via the VPN connection, but the SpeedTouch™ directs it to the local ISP.

As an alternative, we could select to send ***all*** traffic through the secure tunnel. This can be accomplished by specifying the following in the Cisco configuration:

```
cisco(config)# access-list 130 permit ip 0.0.0.0 255.255.255.255 20.0.100.0 0.0.0.255
cisco(config)#
```

By defining the access list in this way, the Cisco will use the VPN connection for all traffic to/from the teleworker in network 20.0.100.0. During the IKE negotiations, the SpeedTouch™ accepts this traffic policy configured in the Cisco IOS router. As a consequence, the SpeedTouch™ uses the VPN connection as its default route. ***All*** traffic will be routed through the VPN connection and no direct access to the Internet is possible. Access to the Internet is to be provided through the corporate network. From the point of view of the corporate network, this is a very secure mode as in this way the company has full control on all traffic to/from the teleworker.

3 REMOTE OFFICE SCENARIO

Introduction

In this scenario, the Virtual Private Network is composed of a number of remote offices connected to a central corporate network in a “hub and spoke” configuration. Each remote office communicates with the corporate network, and no direct connections between the remote offices are established.

3.1 Characteristics of the scenario

At the client side

The remote office networks are composed of a relatively small number of computers. Typically, such a remote office previously had a leased line to securely communicate with the central facilities of the company. A SpeedTouch™ is used as gateway to the Internet. Now, it is the intention to substitute the leased line by building a VPN over the public Internet. The IPSec VPN client capabilities of the SpeedTouch™ allow an easy implementation of this scenario. No IPSec client software is required on the individual computers of the remote office network.

It is assumed that multiple computers can simultaneously access the secure connection. Furthermore, the network should operate unattended. When the SpeedTouch™ starts up, the secure connection is automatically set up, and users do not need to authenticate on an individual basis with the corporate network. They should be able to work on the corporate network as if their office was located in the corporate building.

The main differences with the previously discussed teleworker scenario are:

- the lack of individual user authentication,
- the use of an always-on connection,
- there is no need to change the existing IP addressing scheme of the computers in the remote office, which is an advantage.

At the corporate side

The corporate network uses a Cisco IOS router as a Gateway to the Internet. In order to allow the secure connections with the remote offices, this router has to be configured as a VPN server. In IPSec terms, it acts as the Security Gateway at the corporate peer. For the Cisco configuration, this scenario has no major differences as compared with the teleworker scenario. The only difference is in the fact that the Extended Authentication mechanism is not configured.

3.1.1 Overview of the initial network environment

Illustration

The following figure gives a general overview of the initial network environment. The figure shows an example of two peers, connected to the public Internet via their respective Internet Service Provider.

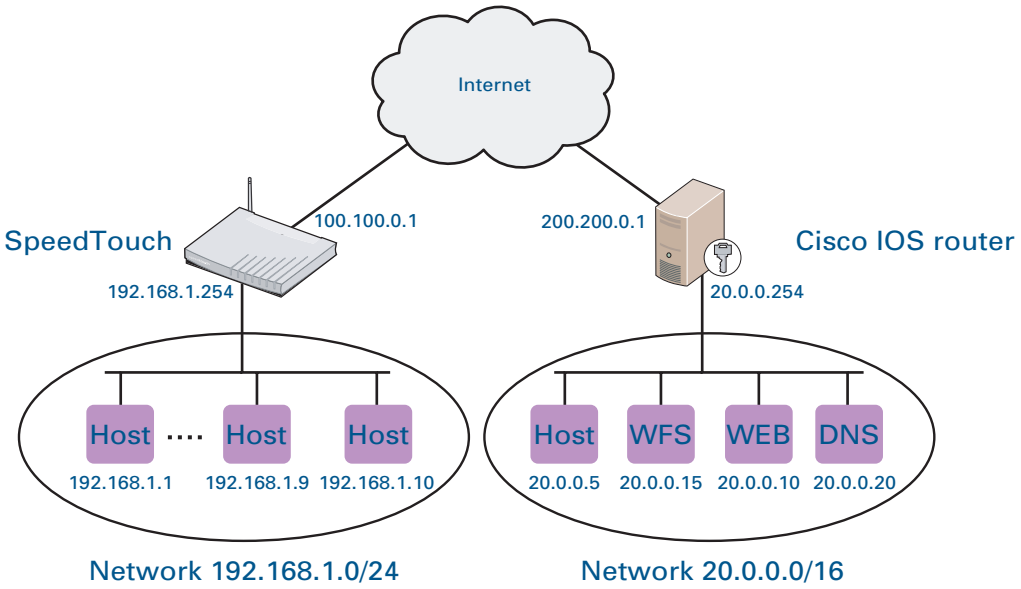


Figure 3: Initial network environment

Public IP addresses

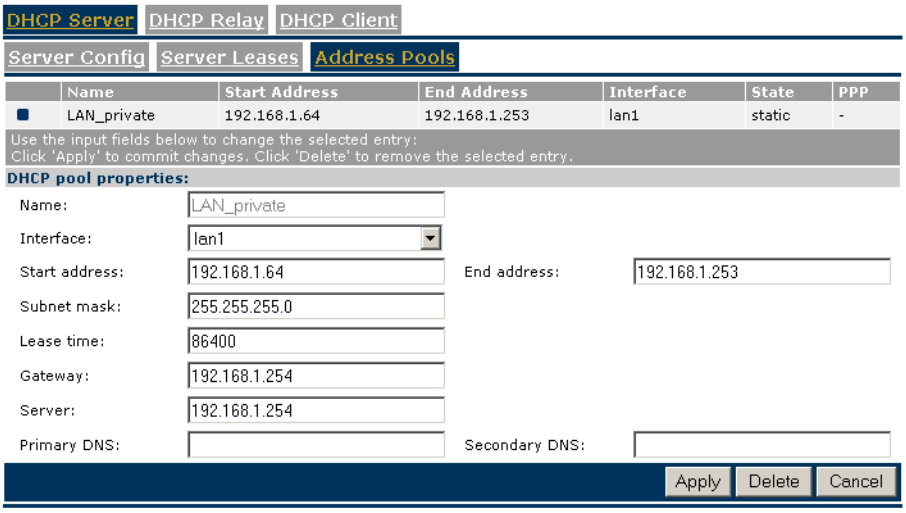
Both peers have a public IP address, assigned by their respective ISP.

At the client side, the public IP address 100.100.0.1 is typically assigned in a dynamic way by the ISP. This means that it has to be considered as a variable: for each session, a different address is attributed to the WAN interface of the SpeedTouch™.

At the corporate office, it is more likely to find a permanently assigned IP address on the WAN interface. In addition, the corporate router may be known on the Internet by its Fully Qualified Domain Name.

Local network environment at the client peer

Compared to the central corporate network, a remote office has a relatively small local network, connected to the Ethernet interfaces of a SpeedTouch™, that acts as a gateway to the Internet. Typically, dynamic IP addressing is used on this network, where the SpeedTouch™ acts as the DHCP server. In the example shown in Figure 3, the local network has the address range 192.168.1.0/24, configured as default local address pool in the DHCP pool of the SpeedTouch™.



The LAN interface of the SpeedTouch™ has address 192.168.1.254 and is the local gateway for this network.

Domain name resolving is provided by the SpeedTouch™ DNS server, which consults the DNS server of the Internet Service Provider in case no entry is found for a particular request.

The remote office may make use of a back-up ISDN connection, in case the DSL connection fails. ISDN back-up scenarios with the SpeedTouch™ are described in a separate application note.

Local network environment at the corporate peer

The corporate local network is typically a large network comprising a number of subnetworks, and providing a variety of services. In this application note only a few relevant aspects of this network are highlighted. Dynamic IP addressing is used on this network, with a local DHCP server attributing IP addresses to the local computers. This service may be provided by the Cisco IOS router. In the example shown in Figure 3, the corporate network has the address range 20.0.0.0/16, The LAN interface of the Cisco router is the gateway for this network and has address 20.0.0.254.

A DNS server is present in the corporate network for resolving domain names. In the example of Figure 3, the DNS server has address 20.0.0.20.

3.1.2 The target network

Illustration

The following figure gives a general overview of the target network environment. The figure shows an example of two peers, connected to each other via a secure IPSec tunnel over the public Internet.

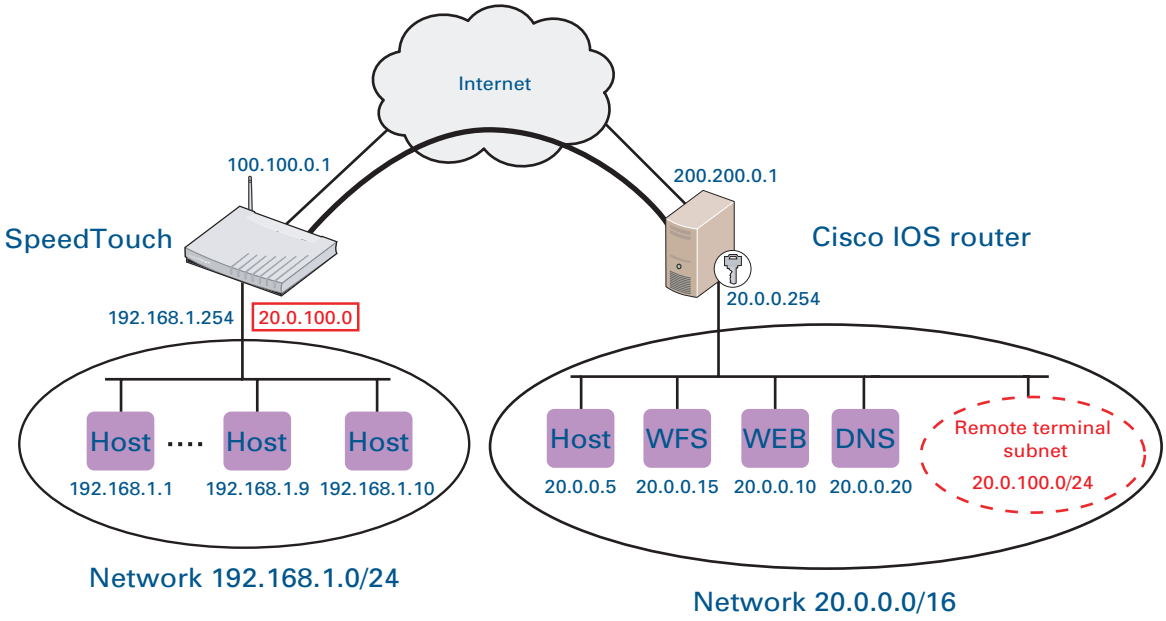


Figure 4: Target network environment

Integrating the remote offices in the address range of the corporate IP network

The company wants to grant remote offices a secure access to the corporate network via the Cisco IOS router that will act as a gateway. All computers of a remote office will be able to access hosts on the corporate network. The secure connections between a remote office and the corporate network over the public Internet will make use of IPSec tunnels.

To integrate the remote offices in the address range of the corporate network, the subnetwork 20.0.100.0/24 is dedicated to these virtual terminals (see Figure 3). From the point of view of the corporate VPN, each remote office represents a single virtual terminal. In the 20.0.100.0/24 subnetwork, a single IP addresses is attributed to each remote office. This is done in a dynamic way by a DHCP server in the corporate network. In our example, this service is implemented by configuring a DHCP server and an address pool for remote offices on the Cisco IOS router.

This network architecture is called an extruded network: an entire subnetwork is located at a remote location. This situation is typical for a large corporate network, where subnets are defined for the various departments.

How IP addresses are handled by the SpeedTouch™ at a remote office

A single IP address is attributed to each remote office. As in each office multiple computers need to access the corporate network, this IP address can not be attributed to one of them via the local DHCP server in the remote office (the approach taken in 2 Teleworker scenario). Another approach is taken, making use of the address translation capabilities of the SpeedTouch™.

In this scenario, IKE Mode Config transfers to the remote SpeedTouch™ an IP address attributed by the Cisco gateway. The SpeedTouch™ will use this IP address for all messages on the IPSec connection to the Cisco IOS router. On the LAN network, all terminals keep on using their original IP address. The SpeedTouch™ manages a NAT translation table to translate IP addresses of the LAN range into the IP address used on the IPSec connection, and vice versa. The SpeedTouch™ keeps track of the message flows to/from the individual terminals on the local network. This mode of operation is referred to as “NAT ahead of the tunnel”.

Accessing the corporate DNS server

The corporate DNS server is used for domain name resolving inside the corporate network. In the initial network environment, the SpeedTouch™ provides the DNS service to the user, and contacts the DNS server of the ISP for locally unresolvable names.

In the corporate network environment, the SpeedTouch™ should relay unresolvable DNS requests to the corporate DNS server. To this end, IKE Mode Config communicates the location of the corporate DNS server to the remote SpeedTouch™.

In the remote offices, local access to the public Internet is still possible when a split-tunneling traffic policy is applied. In this case, for Internet traffic the DNS server of the ISP is still used for domain name resolving.

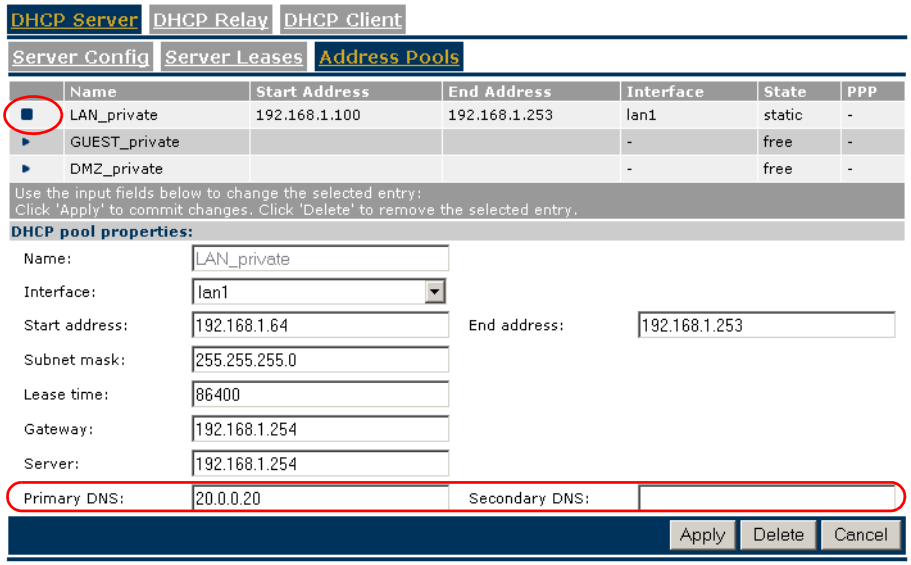
Accessing the corporate DNS server in a Microsoft Windows network

In a Microsoft Windows network environment, it is required to specify the IP address of the corporate network DNS server in the DHCP address pool of the SpeedTouch™ at the remote offices. The DNS relay function of the SpeedTouch™ does not process the SRV and SOA messages used in a Microsoft Windows network. As a result, these messages cannot reach the corporate network DNS server(s). To remedy this situation, simply configure the IP address of the corporate DNS server(s) in the DHCP address pool of the SpeedTouch™.

Configuring the corporate DNS server(s) in the DHCP address pool

Proceed as follows:

1. Browse to **Expert Mode > Local Networking > DHCP Server > Address Pools**.
2. Select the private LAN address pool.
3. Fill out the **Primary DNS**, and optionally the **Secondary DNS** server IP address.



4. Click **Apply**.
5. Click **Save All** to save the SpeedTouch™ configuration.

IKE Mode Config capabilities of Cisco IOS

- Virtual IP address
- Primary DNS
- Primary WINS
- Address Expiry. The IP address lifetime is always equal to the remainder of the lifetime of the Phase 1 Security Association. Therefore, virtual address refreshing only takes place after rekeying of the Phase 1 SA.
- Domain name.
- Split-tunneling remote subnets

3.1.3 Securing the access to the corporate network

Use of secure connections

The IPSec protocol framework is used for the implementation of this secure VPN. The SpeedTouch™ will automatically dial in to the VPN server in order to set up the secure connections. As soon as the secure connection is established, the terminals in the remote office have access to the corporate network, without any individual authentication procedure.

The security parameters for the IPSec connections, such as encryption and message authentication algorithms, are selected in function of the security policy in the VPN. The security parameters configured at both peers of the connection must match in order to successfully complete the IPSec tunnel negotiations.

Matching networks

In the IPSec negotiations, the description of the local and remote private networks forms part of the security policy. The peers exchange information about which networks are accessible. When peers fail to agree on their common knowledge of the VPN layout, the negotiations are aborted.

Authenticating remote offices

In this scenario, a single level of authentication is applied.

The establishment of an IPSec connection requires user authentication. Two mechanisms are foreseen in the IPSec framework:

- pre-shared key authentication
- authentication with certificates

Pre-shared key authentication is used. The pre-shared key acts as a group key for all terminals in a remote office. The key is entered in the SpeedTouch™ by the operator during the configuration procedure. Individual network users have no knowledge of the key.

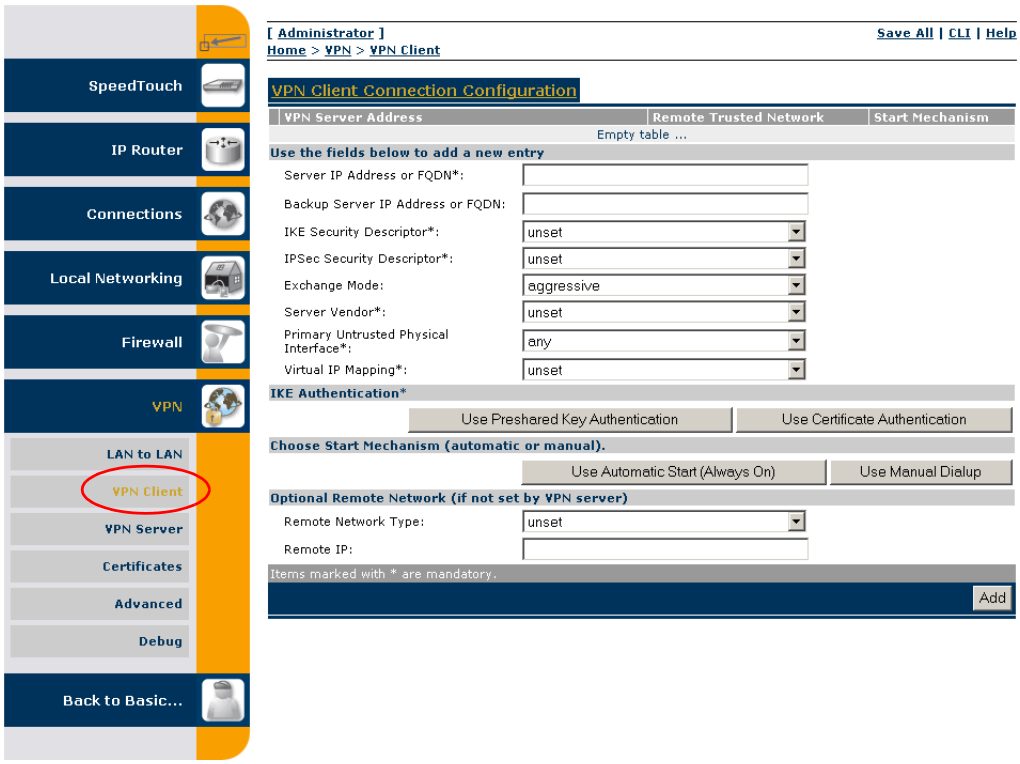
No individual user authentication is required in this scenario.

3.2 Configuring the SpeedTouch™

VPN client configuration procedure outline

Configure the VPN client on the SpeedTouch™ via the internal Web pages.

1. Browse to the SpeedTouch™ Web pages at **http://speedtouch.lan** or at IP address **192.168.1.254**.
2. Open the VPN Client Web page, accessible via **Expert mode > VPN > VPN Client**.



3. Fill out the VPN client parameters (see "3.2.1 Fill out the VPN Client parameters" on page 44).
4. Select the IKE Authentication method (see "3.2.2 Select the IKE Authentication method" on page 45).
5. Select the Start Mechanism (see "3.2.3 Select the Start Mechanism" on page 45).

3.2.1 Fill out the VPN Client parameters

Procedure

Proceed as follows:

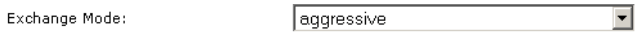
1. Fill out the publicly known network location of the Cisco VPN server. This may be the public IP address, if it is invariable and known. In general however, it is the publicly known FQDN, such as **vpn.corporate.com**.

2. Leave the **Backup Server IP address or FQDN** field open. This field can be filled out in configurations with a backup server. This is beyond the scope of the present scenario.

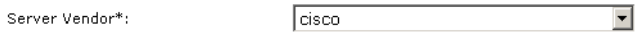
3. Select the **IKE Security Descriptor**. In our example, the pre-configured **DES_MD5** descriptor is selected. For more information, see " IKE Security Descriptor" on page 13.

4. Select the **IPSec Security Descriptor**. In our example, the pre-configured **DES_MD5_TUN** descriptor is selected. For more information, see" IPSec Security Descriptor" on page 14.

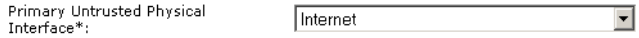
5. Select the **IKE Exchange Mode**: Select **aggressive**. For more information, " Exchange Mode" on page 14.



6. Select the **Server Vendor**: select **cisco**.



7. Select the **Primary Untrusted Physical Interface**. Select the name of your Internet interface from the list. In our example the Internet connection is called: **Internet**.



Select the **Virtual IP Mapping** method: select **nat**. For more information, see " Virtual IP mapping" on page 44

Virtual IP mapping

The selection of **nat** as virtual IP address mapping has the effect that the VPN server attributes a virtual IP address to the SpeedTouch™ VPN client. This virtual IP address is stored in the SpeedTouch™. The SpeedTouch™ will automatically create a new NAPT entry to map the virtual IP address to the IP addresses used on the local network. This is generally referred to as "NAT ahead of the tunnel".

Network Address Translation, as well as Port Number Translation are used. In the SpeedTouch™ documentation this is generally referred to as "N-to-1 NAPT".

For the remote office scenario, the **nat** method is the only viable solution, because multiple terminals need to have access to the VPN connection.

For more information, see "The SpeedTouch™ and Address Translation".

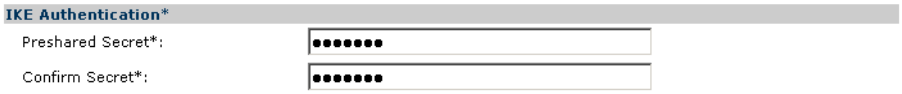
3.2.2 Select the IKE Authentication method

Procedure

Proceed as follows:

1 Select **Use Preshared Key Authentication**.

2 Enter the pre-shared key: a character string to be used as a password for the VPN connection.This secret needs to be identically configured in the VPN client and VPN server.



The pre-shared key value is not shown in clear text on the SpeedTouch™ Web page. In order to protect for typing errors, the key has to be to entered twice, to confirm your entry.

3.2.3 Select the Start Mechanism

Automatic start

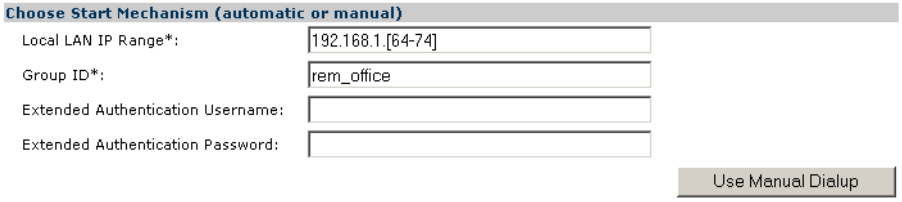
Because multiple computers have access to the secure connection, and individual users do not have to authenticate, the logical choice is to let the SpeedTouch™ automatically dial in. In this way the secure connection is always available to the authorized terminals.

Procedure

Proceed as follows:

1. Select **Use Automatic Start (Always On)**.

2. When selecting the Automatic Start mechanism, it is required to fill out the **Local LAN IP Range** and **Group Identity**.



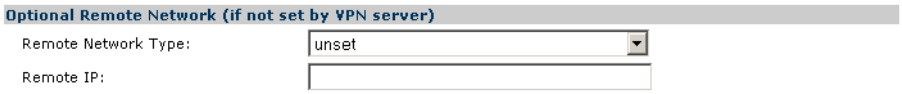
   For the **Local LAN IP Range**, fill out the range of IP addresses that will get access to the secure connection. This can either be the total range of local IP addresses, or a subrange. In the example shown above, a range of 10 terminals in the local LAN can access the corporate network via the secure connection.

   The **Group ID** parameter matches the group name defined in the Cisco IOS router configuration.

3. Leave the **Extended Authentication** fields open.

   Extended Authentication can not be used in the remote office scenario because multiple users (terminals) in the office share a single secure VPN connection. Individual authentication as offered by XAuth is there excluded in this scenario. Note the difference with the teleworker scenario discussed in "2 Teleworker scenario" on page 5.

4. Leave the **Optional Remote Network** fields open, as shown below.



   These settings allow you to limit the accessible area of the corporate network.

5. Click **Add** at the bottom of the page.
6. Click **Save All to s**ave the SpeedTouch™ configuration.

All the VPN client configuration parameters have now been entered in the SpeedTouch™.

3.3 Dialling in to the Cisco VPN server

Automatic dial-in procedure

The dial-in procedure is started automatically by the SpeedTouch™, without any user interaction.

In order to dial in successfully, it is required that the Cisco VPN server is properly configured. For more information, see "3.4 Configuring the Cisco IOS router" on page 48.

Who has access to the corporate network

All computers in the remote office with an IP address complying with the traffic policy have access to the VPN connection.

Surfing through the VPN tunnel

One of the SpeedTouch™ features for easy Internet access is the so-called Differentiated Services Detection (DSD). This feature monitors your HTTP traffic and alerts you when you want to browse to a location that is not reachable due to the fact that the connection to your Service Provider is not active. A SpeedTouch™ Web page appears that allows you to log on to your Service Provider.

When you configure an IPSec VPN connection, this feature has to be disabled in order to pass HTTP traffic through the VPN tunnel.

To verify that the Differentiated Services Detection is disabled, proceed as follows:

1. Browse to **Basic Mode > Toolbox > Web Site Filtering**.
2. Click **Configure**.
3. Verify that the check box "**Use Address Based Filter**" is not selected.

If Differentiated Services Detection is disabled, Web address based filtering is disabled as well. Keep this in mind if you use the Web based filtering tool for parental control.

Testing the VPN connection

From the moment when the VPN connection is active, you should be able to ping a computer located in the private corporate network from a computer in the remote office. For example, referring to "Figure 4: Target network environment" on page 39, the computer with IP address 192.168.1.64 is able to ping the computer with IP address 20.0.0.5.

Use the **debug** pages to diagnose problems. See "Testing the VPN connection" on page 23.

3.4 Configuring the Cisco IOS router

Introduction

An edited configuration file of the Cisco IOS router is found below. This file is valid for the remote office scenario. This file differs from the teleworker scenario in only three lines. More specifically, in the remote office scenario no individual user authentication (XAuth) is used.

Cisco configuration file

Below, a edited configuration file is shown. It mainly contains the entries that are relevant for the remote office scenario.

```
Current configuration : 10776 bytes
version 12.3
hostname cisco3660bis
!
aaa new-model
!
aaa authorization network groupauth_remoffice local
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
!
crypto isakmp client configuration group rem_office
 key secretkey
 dns 20.0.0.20
 pool remofficepool
 acl 130
!
crypto ipsec transform-set remofftrset esp-des esp-md5-hmac
!
crypto dynamic-map remoffdyn 1
 set transform-set remofftrset
!
crypto map remoffmap isakmp authorization list groupauth_remoffice
crypto map remoffmap client configuration address respond
crypto map remoffmap 1 ipsec-isakmp dynamic remoffdyn
!
interface ATM3/0.20
 crypto map remoffmap
!
ip local pool remofficepool 20.0.100.1 20.0.100.254
ip route 20.0.100.0 255.255.255.0 ATM3/0.20
!
access-list 130 permit ip 20.0.0.0 0.255.255.255 20.0.100.0 0.0.0.255
!
end
```

For more information, see “2.6 Configuring the Cisco IOS router” on page 26.

Visit us at:

www.speedtouch.com

Acknowledgements

All Colleagues for sharing their knowledge.

Coordinates

THOMSON Telecom Belgium

Prins Boudewijnlaan 47
B-2650 Edegem
Belgium

E-mail: documentation.speedtouch@thomson.net

speedtouch™

Copyright

A THOMSON BRAND