IP Office

Virtual Private Networking

Issue 3b (22nd June 2005)

Contents

Contents (Cont.)

Figures

Introduction

Virtual Private Networks (VPNs) have evolved from the growing needs of businesses for more wide area network connectivity. This need has been driven by a combination of technological progress and changing trends in work habits and work environments.

The new VPN capability in Avaya's IP Office gives small and medium sized businesses a cost effective alternative to private leased line or Frame Relay (FR) services for interconnecting sites. It also allows Small Medium Businesses (SMBs) to avoid the high costs associated with teleworkers and the mobile workforce using Remote Access Servers (RAS). Instead they can leverage the ubiquity and low cost of the public Internet.

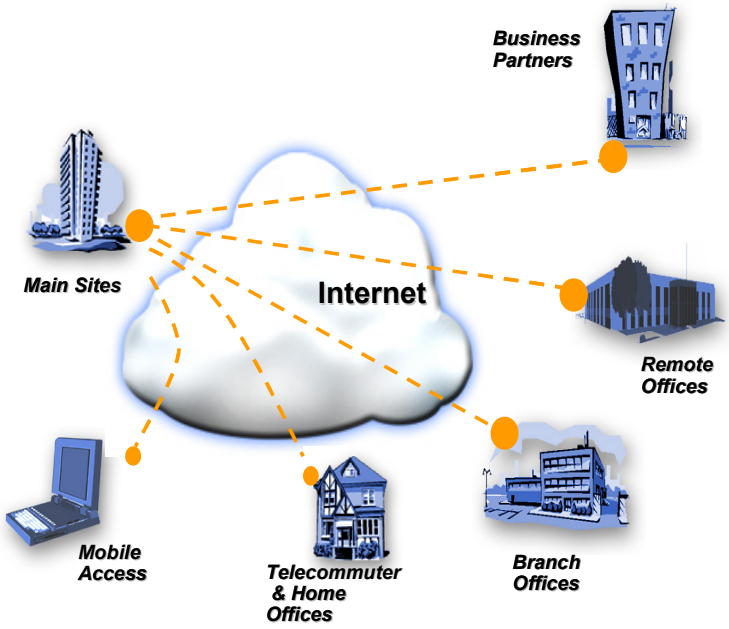

Figure 1. A Virtual Private Network

IP Office VPN is implemented as a customer premises based VPN, by far the most common method adopted amongst SMBs. VPN capability is integrated into the IP Office server delivering a single box solution, with the ease of common management, and lower total cost of ownership than a multi box solution.

General

This manual provides scenarios and worked examples for VPN implementation on an IP Office running software level 3.0+. Throughout this manual is assumed that the reader has networking knowledge but not necessarily any detailed understanding of security protocols and encryption.

Further Reading

The IPSec and L2TP specifications are widely discussed in open forums. The reader is encouraged to seek a fuller explanation than is provided within this manual. Refer to the Virtual Private Network Consortium http://www.vpnc.org/terms.html for further information.

Overview of IPSec and L2TP Technologies

This section presents a brief overview and describes key terms and references specific to tunneling protocols that comprise the new IP Office 3.0+ features of secure VPN networking using Internet Security (IPSec) and L2TP. The information and discussion in this document is specific to the following software revisions:

Equipment	Software Version
IP Office (all platforms)	3.0+
SysMonitor	3.0+
Manager	3.0+
Cisco IOS® using pre-shred mode only	12.2+
NetScreen Remote VPN Client	10.0

General

For **secure VPNs**, the technologies that IP Office supports are:

- IPSec
- L2TP Compulsory/Voluntary (optional pre-shared secret Authentication)

IPSec is the primary VPN security protocol and is a licensable IP Office feature.

CAUTION: Throughout this document, examples are given for various VPN scenarios. The IP addresses used must be considered as **EXAMPLES ONLY**. For definitive IP addresses, always consult your Network Administrator.

IPSec

IP packets have no inherent security. Hence, where security is required, then IPSec is used. IPSec is a method of protecting IP datagrams and provides:

1. Data origin authentication
2. Data integrity authentication.
3. Data content confidentiality.

IPSec protects IP packets by specifying the traffic to protect, how that traffic is to be protected and to whom the traffic is sent. The method of protecting IP packets is by using one of the IPSec protocols, the Encapsulating Security Payload (ESP) or the Authentication Header (AH).

IPSec is a suite of protocols developed and maintained by the Internet Engineering Task Force (IETF). The framework for IPSec is modular and component oriented. The diagram below illustrates the interrelationship between all of the IPSec components that maintain this modular approach. It is important to understand that each of these groups serve a specific purpose and work together to provide a modular solution to Internet security problems. By breaking IPSec into these seven different areas it become easier to understand the objective of each group of components.

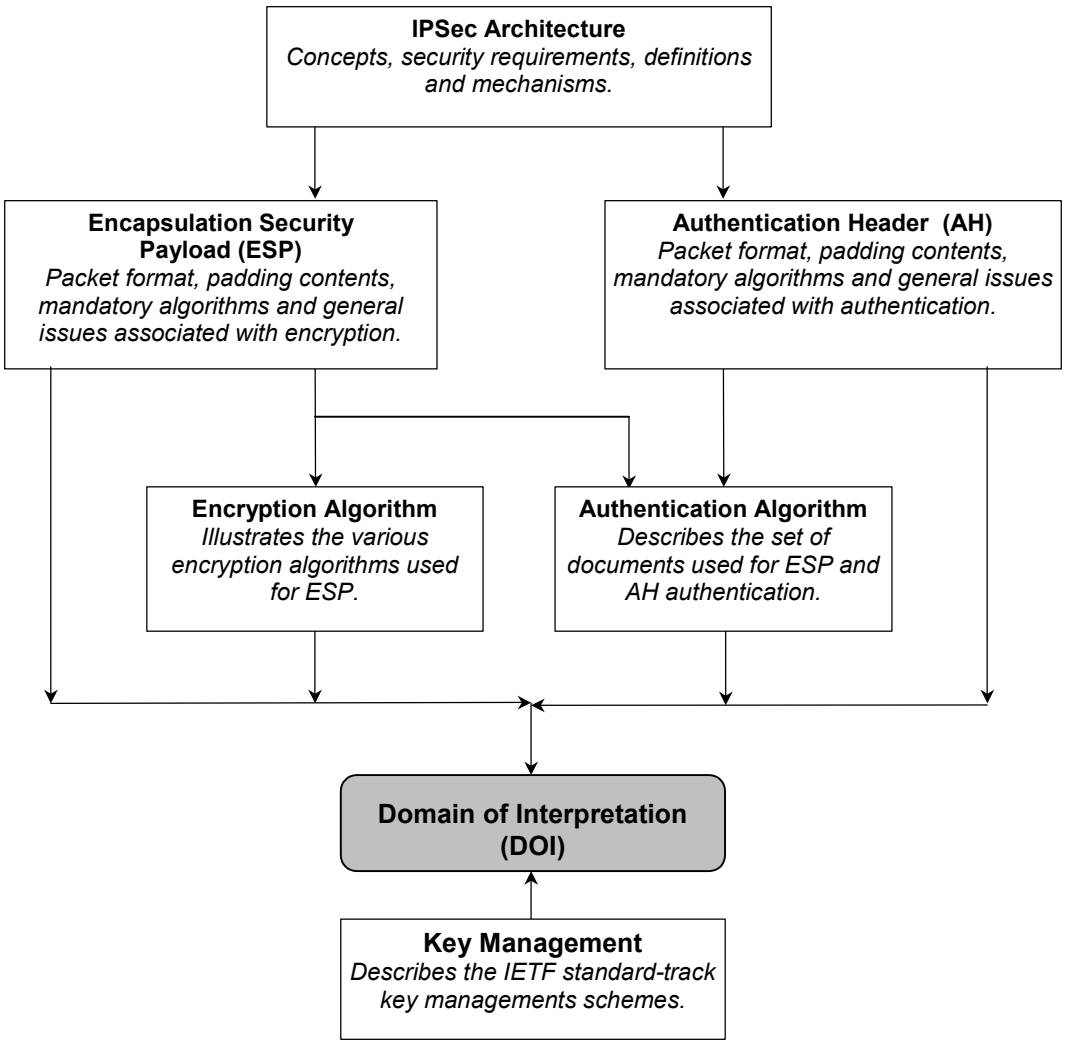

Figure 2. An IPSec Framework

L2TP

Layer 2 Tunneling Protocol (L2TP) provides a means for tunneling IP traffic at layer 2 and is derived from two other tunneling protocols (PPTP and L2F). L2TP is built upon the well-established Internet communications protocol Point-to-Point Protocol (PPP), and Transmission Control Protocol/Internet Protocol (TCP/IP).

L2TP tunneling encapsulates IP data packets in PPP, for transmission through an IP network. Upon receipt, the IP and PPP headers are stripped away, exposing the original IP data packet. In this way encapsulation allows the transportation of IP packets over a PPP authenticated connection.

The diagram below demonstrates the two modes of tunneling that an L2TP tunnel may operate.

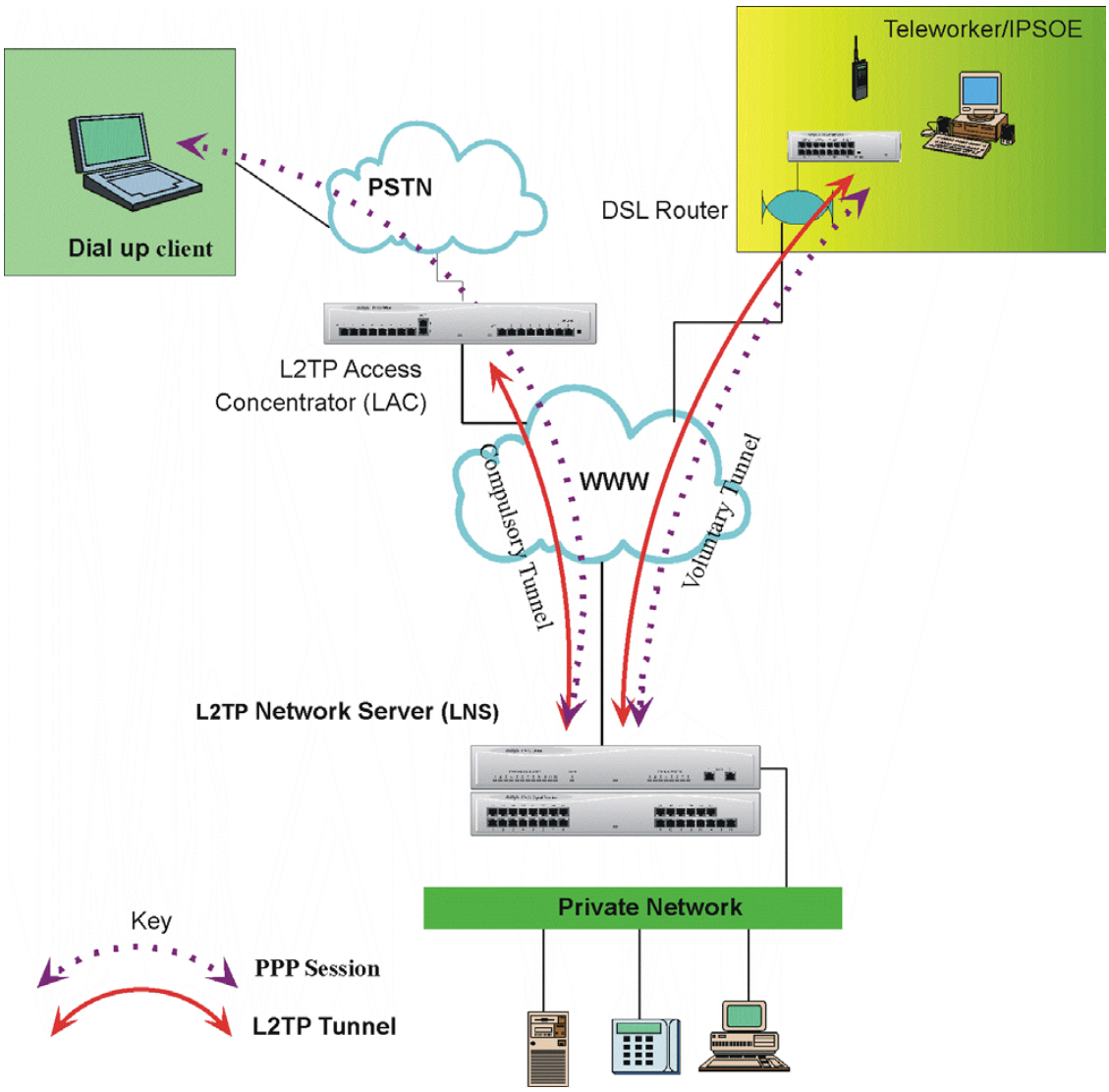

Figure 3. LT2P Tunneling Modes

Compulsory Tunneling

A compulsory tunnel is an L2TP tunnel which is not controlled by the user. In compulsory tunneling the dial-up client PC accesses the Private Network by first dialing to an L2TP Access Concentrator (LAC), which terminates the Public Switched Telephone Network (PSTN) connection and then establishes an L2TP tunnel to the L2TP network Server (LNS). In this mode the PPP session is established between the dial-up client PC and the LNS and L2TP is established between the LAC and the Network Access Server (NAS).

IP Office can be used to provide LAC operation but does not provide PPP transportation. Under the IP Office 3.0+ implementation the incoming PPP session is terminated locally and the L2TP tunnel is then established to the LNS. The contents of the incoming PPP session are extracted and routed through the established tunnel in the normal way.

Voluntary Tunneling

Voluntary tunneling mode operation describes an L2TP tunnel, which is established directly between the user and the LNS. Once L2TP is established the PPP protocol then runs over the session. Running voluntary tunneling is the primary operating mode for the IP Office L2TP implementation.

The table below provides a summary of the L2TP packet exchanges that are used in the establishment and control of an L2TP tunnel.

Message Type	Description
Start-Control-Connection-Request (SCCRQ)	Sent by the L2TP client to establish the control connection. Each L2TP tunnel requires a control connection to be established before any other L2TP messages can be issued. It includes an Assigned Tunnel-ID that is used to identify the tunnel.
Start-Control-Connection-Reply (SCCRP)	Sent by the L2TP server to reply to the Start-Control-Connection-Request message.
Start-Control-Connection-Connected (SCCRN)	Sent in reply to a Start-Control-Connection-Reply message to indicate that the tunnel establishment was successful.
Outgoing-Call-Request	Sent by the L2TP client to create an L2TP tunnel. Included in the Outgoing-Call-Request message is an Assigned Call ID that is used to identify a call within a specific tunnel.
Outgoing-Call-Reply	Sent by the L2TP server in response to the Outgoing-Call-Request message.
Start-Control-Connection-Connected	Sent in reply to a received Outgoing-Call-Reply message to indicate that the call was successful.
Hello	Sent by either the L2TP client or L2TP server as a keep-alive mechanism. If the Hello is not acknowledged, the L2TP tunnel is eventually terminated.
WAN-Error-Notify	Sent by the L2TP server to all VPN clients to indicate error conditions on the PPP interface of the L2TP server.
Set-Link-Info	Sent by the L2TP client or L2TP server to set PPP-negotiated options.
Call-Disconnect-Notify	Sent by either the L2TP server or L2TP client to indicate that a call within a tunnel is to be terminated.
Stop-Control-Connection-Notification	Sent by either the L2TP server or L2TP client to indicate that a tunnel is to be terminated.

Overview of Secure VPN Implementation

IP Office's secure VPN solutions comprise both IPSec and L2TP tunneling protocols. Both of these protocols may be used independently or collectively to provide the required secure VPN. In order to explain the IP Office secure VPN solution this section describes each protocol implementation in turn and, for IPSec, how IP Office handles an unprotected packet arriving at an interface.

IPSec Implementation

An inbound unprotected packet is one that is **not protected** by IPSec and is therefore received on an interface outside an established IPSec tunnel. In the context of IPSec it is an unsecured packet. If the inbound unprotected packet matches the condition on any configured IPSec form then a Security Association (SA) is formed with the specified Secure Gateway. Once the SA is established the inbound packet is secured and forwarded to the Secure Gateway as an ESP packet.

Note: IPSec implementation on IP Office requires a valid licence.

If the packet does not match any condition set on an IPSec configuration then it is simply forwarded unencrypted to the appropriate destination interface. The diagram below details the case for an inbound unprotected packet.

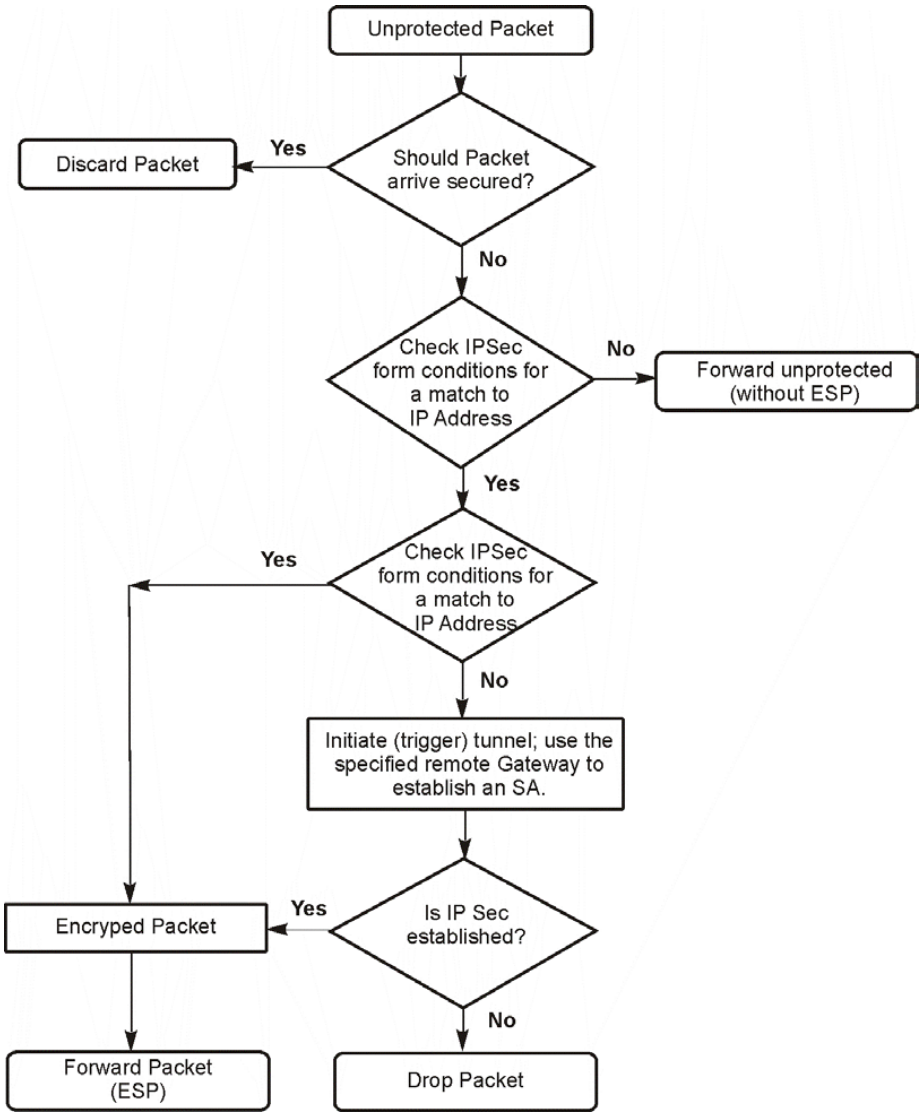

Figure 4. Inbound Unprotected Packet

If the unprotected packet matches the configured IP address condition for an established SA it is forwarded to the destinations using the SA.

If the unprotected packet matches a condition for which there is not an established SA then IP Office will initiate IPSec tunnel establishment (ISAKMP) to the specified remote gateway. Once the tunnel is established the packet is encrypted and forwarded to the appropriate interface. In this way, an inbound unprotected packet serves as the trigger mechanism for IPSec tunnel establishment.

The other case for a packet arriving on an interface is where the packet is an IPSec packet type. There are two types:

1. ISAKMP - used to establish the tunnel and thereby form the SA.
2. ESP - used to carry the encrypted data.

If the received IPSec packet is an ESP addressed to the IP Office, then IP Office will check for a valid SA. If a valid SA is found then the packet is decrypted and forwarded. If not, the ESP packet is discarded.

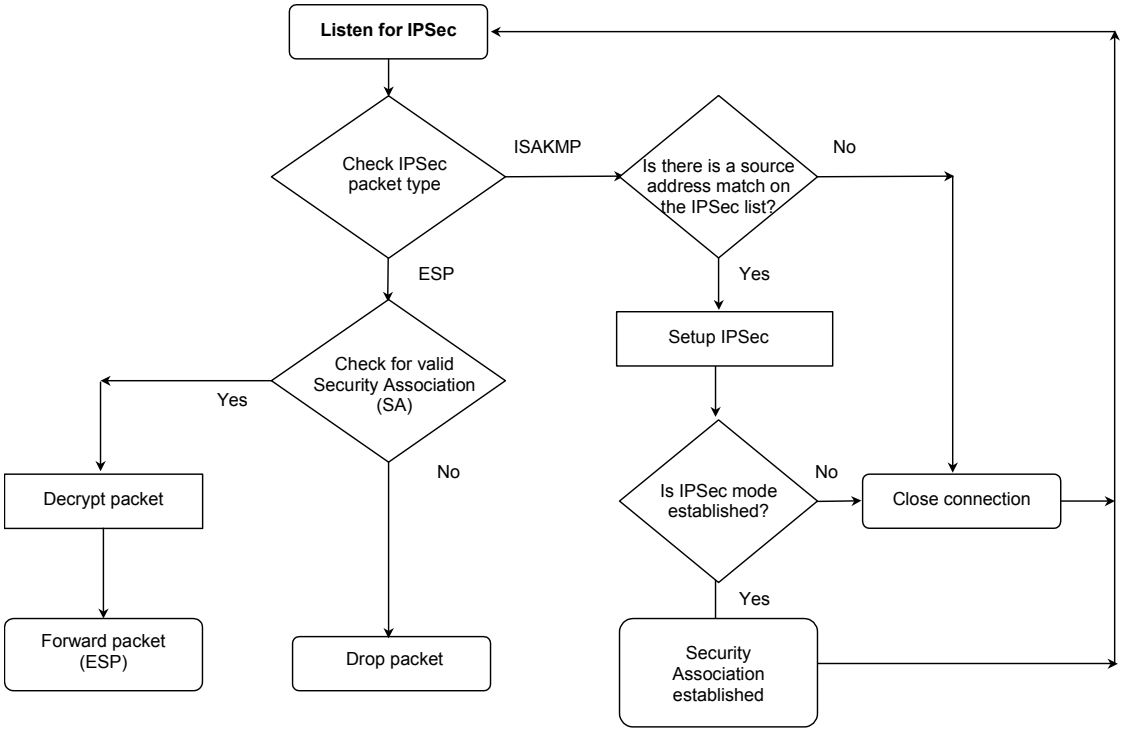

Figure 5. Inbound Unprotected Packet Type Detection

L2TP Implementation

With IP Office version 3.0+, VPN implementation of an L2TP tunnel presents a routable destination. The configured L2TP tunnel is available in the routing table as an IP destination interface. IPSec is different in this respect in that it applies a treatment or protection to specified IP addresses. Protected packets are encrypted packets (called ESPs) that are routed to the appropriate destination using the routing table in the normal way. IP Office secure VPN solutions comprise both IPSec and L2TP. The relationship between IPSec and L2TP is therefore symmetrical and provides for the following:

- IPSec inside L2TP: IPSec protected packets (ESP) routed to an LT2P destination
- L2TP inside IPSec: LT2P packets to be protected by IPSec

The table below details the advantages/ disadvantages of IPSec, L2TP and the symmetrical relationship between the two:

IPSec	**L2TP**	**IPSec in L2TP**	**L2TP Inside IPSec**
Advantages • Encrypts data Disadvantages • Packets **must not** be excessively re-ordered in the same tunnel	Advantages • Can be used for Inter-tunneling • PPP IP Header compression support Disadvantages • No Data Encryption • Packets **must not** be excessively re-ordered in the same tunnel	Advantages • Can be used to with existing LT2P systems Disadvantages • L2TP negotiation can be observed on the Public Network • Packet size	Advantages • Can be used for inter-tunneling • L2TP negotiation cannot be observed on the Public Network • Commonly used by Microsoft Disadvantages • Packet size

Guidelines

1. IP Office is able to allow IPSec packets to pass through a NAT enable interface. However this facility is only available when the IPSec tunnel is either originated or terminated on a local interface.

For any routable packet the routing table is referenced to determine the appropriate destination. If the packet is for an L2TP destination then IP Office checks the status of the tunnel. If established the packet is forwarded. If the packet is addressed to an L2TP destination and the tunnel is not active, then IP Office uses the remote gateway entry on the L2TP form and initiates the tunnel setup. The routable packet is queued until the tunnel is established. When the tunnel is established the routable packet is forwarded inside the tunnel.

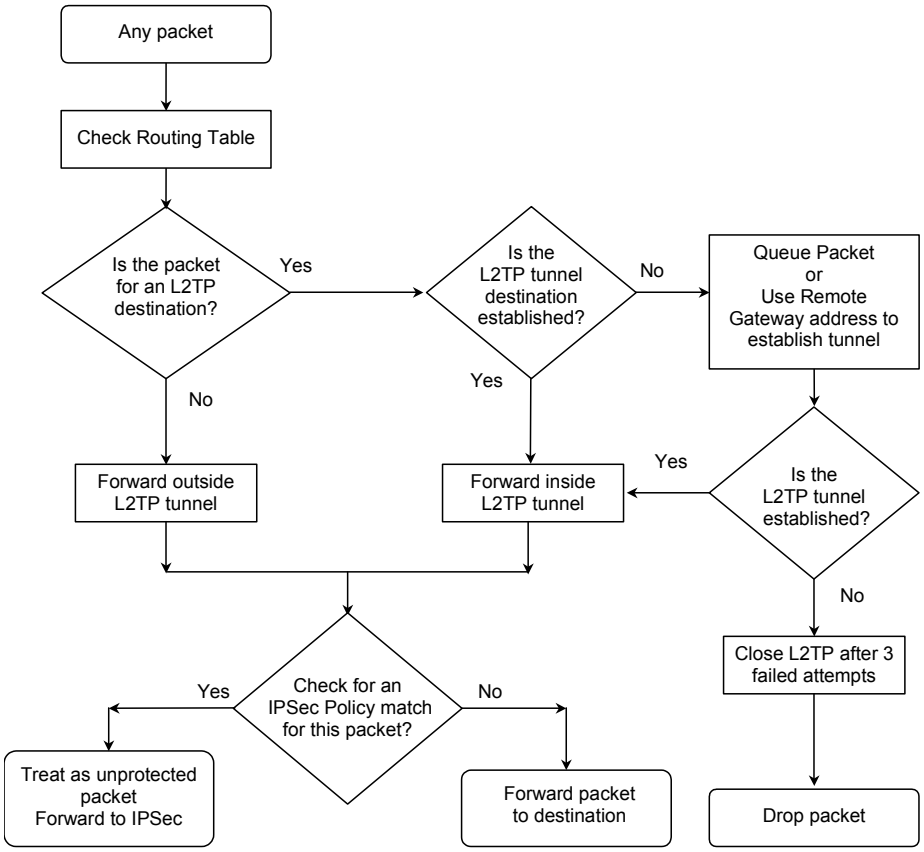

Figure 6. L2TP Implementation

When the L2TP packet is to be forwarded it may be the case that the IPSec tunnel peer or endpoint address require IPSec protection. If so, the outgoing L2TP packet is encrypted inside IPSec, as in the case for an unprotected packet (see previous paragraphs). In this way L2TP can be tunneled inside IPSec. If the L2TP tunnel peer address does not require protection then an L2TP packet is sent directly without IPSec protection.

With IP Office version 3.0+ implementation it is also permissible for an ESP packet to be routed to an L2TP destination (i.e. using the routing table) and in this way IPSec to tunnel inside L2TP.

Logical LAN Implementation

The Logical LAN feature is new to IP Office (2.0+ software). Logical LAN feature allows a second LAN interface to operate together with the primary System LAN interface (LAN 1). The Logical LAN feature allows a second LAN interface to operate together with the primary System LAN interface (LAN1). Once a Logical LAN interface is created and configured it is then available as an IP route destination. The table below summaries the terms used to describe the Logical LAN feature.

Term	Description
Physical LAN	For a single LAN system (IP403 and IP406) this is the actual Ethernet interface and consists of both the Logical LAN (see below) and the System LAN (see below).
Logical LAN	The Logical LAN has the same collision domain as the System LAN but uses a different MAC address and operates on a different subnet. The Logical interface can be regarded as a secondary or a sub-interface to the primary System LAN (LAN1) interface – see below. The Logical LAN provide the function of the Public or External Interface (see page 17).
System LAN	The System LAN has the same collision domain as the Logical but uses a different MAC address and operates on a different subnet. When a Logical LAN is created (see above) the System LAN becomes active and is referred to as LAN1.The System LAN performs the function of an internal LAN.
Single LAN systems	IP Office systems that have a single LAN interface (IP403 and IP406).
Dual LAN systems	IP Office systems that have dual Ethernet interfaces (Small Office Edition and IP412)

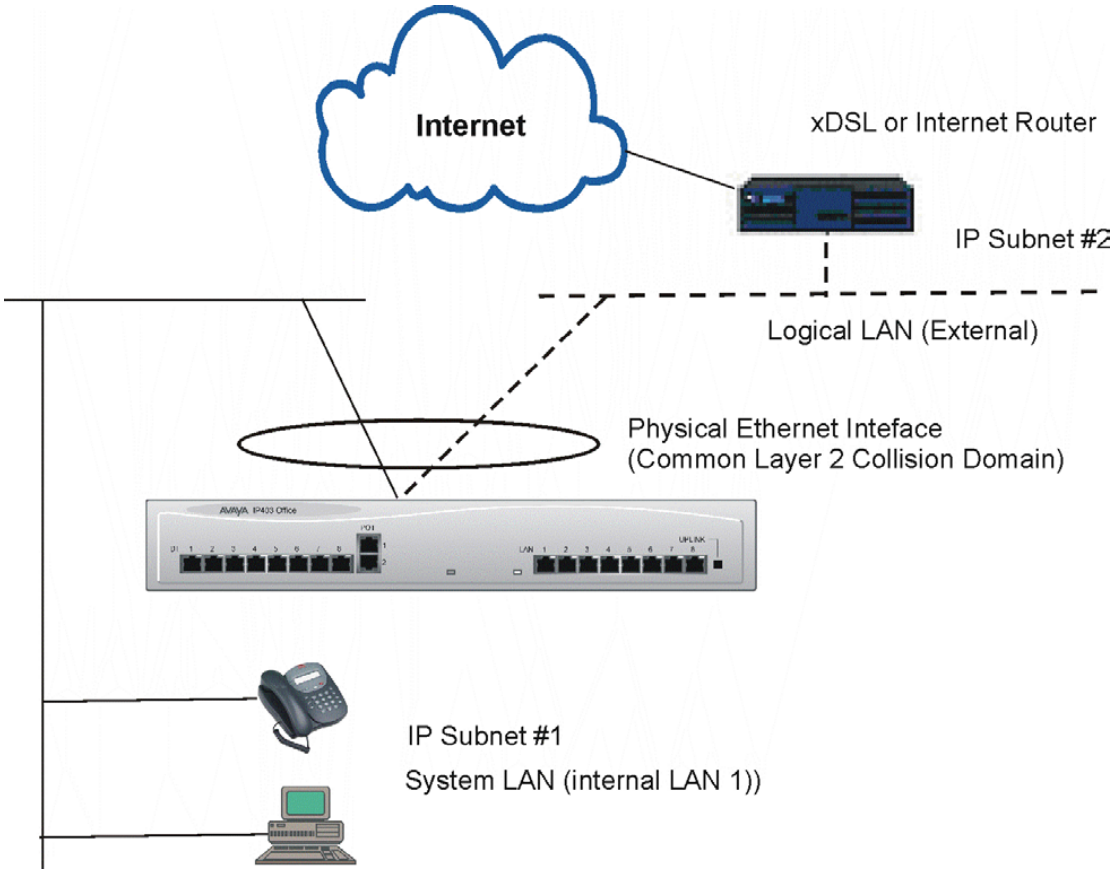

Figure 7. Logical LAN Implementation

The Logical and System LAN interfaces use different MAC addresses, function on a common Layer 2 collision domain but operate on separate Layer 3 subnets. Both the Logical and System LANs are tied to a same Physical LAN

The Logical LAN feature allows single LAN systems such as the IP403 and IP406 to be used in conjunction with an external Internet router or xDSL device. The feature allows single LAN systems to operate external and internal IP subnets in support of VPN networking

NAT functionality is applied to traffic from LAN1 using the IP address assigned to the Logical LAN. This and other Logical LAN facilities are detailed in the Public Interface section (see page 17). In addition, an example of the use of a Logical LAN can be seen on page 34.

For dual LAN systems the second Physical LAN interface (LAN2) should be used as the Public (External) LAN interface.

Typical VPN Deployment

The diagram below shows a typical IP Office VPN networking deployment using the Internet and other public access network. Within this section the elements that are detailed in the diagram will be discussed with respect to the IP Office 3.0+ VPN implementation. The following elements will be discussed:

- Public Access
- Public Interface
- IP Office VPN solutions
- Internal LAN
- VPN Client
- VPN and VoIP
- Maximum Load

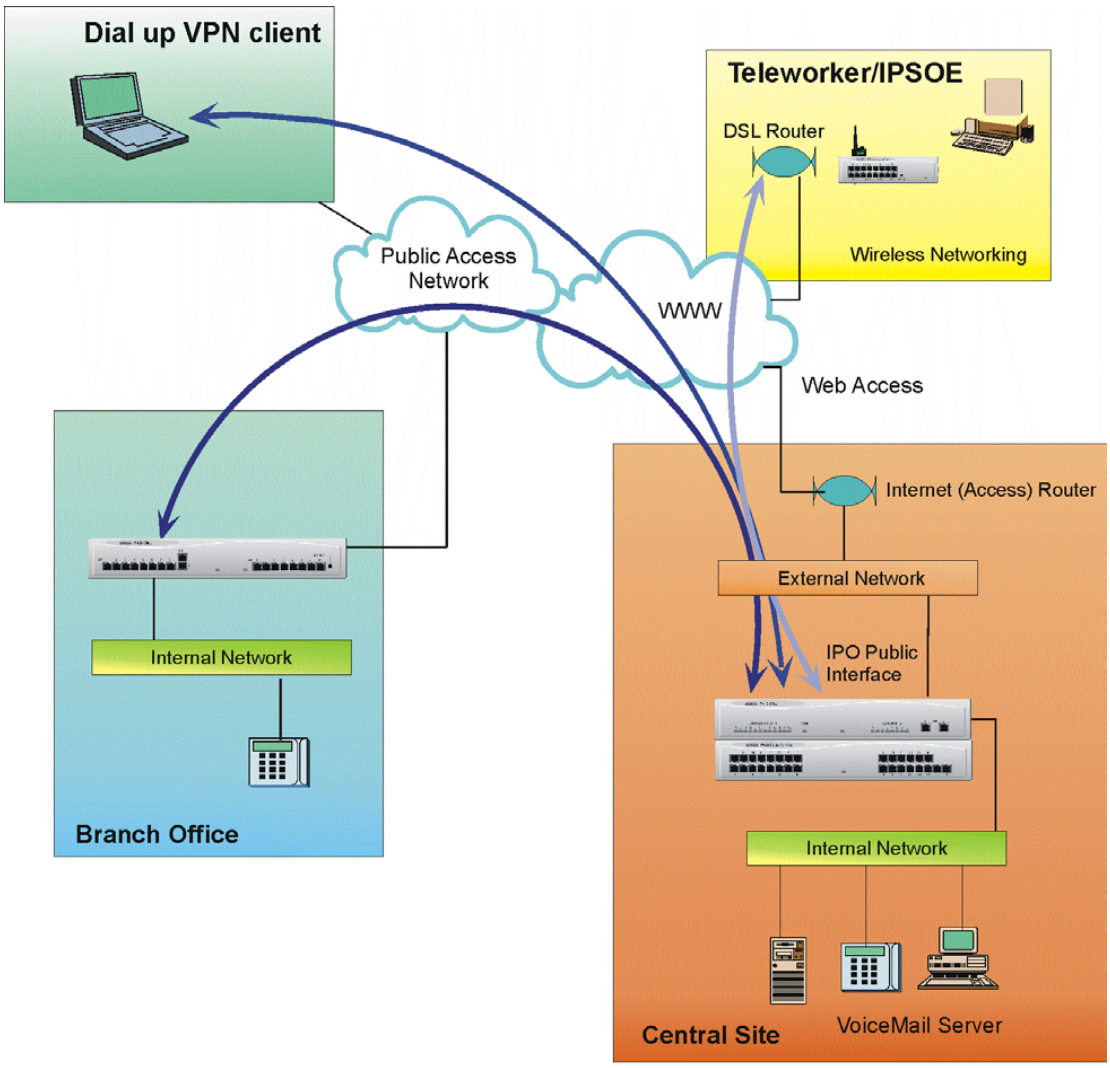

Figure 8. IP Office VPN Networking

Public Access Networks

IP Office can be connected to the Internet or other public networks in a number of ways. This section details the supported technologies and media types for connection to public networks.

Media	Description
Frame Relay	IP Office supports Frame Relay using PPP or FRF12 fragmentation for interoperability. IP Office supports common electrical interfaces such as X21, V24 and V35 for Frame Relay connection.
PPP	IP Office support PPP over a dedicated WAN link using X21, V24 and V35 electrical interfaces.
PSTN	The PSTN network can be used to access the Internet via an ISP. IP Office supports both digital and Analogue PSTN services.
xDSL /Internet Router	xDSL and Internet routers provide shared Internet access for the business or home user. The xDSL and Internet Router is a managed connection to the ISP network (CO) that is terminated on an Ethernet interface on the customers premises (CPE) IP Office may be used in conjunction an xDSL or Internet Router. Both the Logical or the Physical LAN2 interface (dual LAN systems) can be used to provide Public Interface functionality as described in the following sections.

Guidelines

1. Generally, for site-to-site VPN using xDSL, it is recommended that the two end points are sourced from the same service provider.
2. The IP Office VPN secure implementation is such that IP Office concurrently performs the functions of a NAT enabled gateway as well as terminating and originating VPN tunnels. This allows IP Office to be used for both Secure VPN networking between branch offices as well as for NAT access to Internet services.
3. IPSec connections that are not originated or terminated by IP Office cannot be facilitated through a NAT enabled interface.

Further Reading

The IPsec and L2TP specifications are widely discussed in open forums. The reader is encouraged to seek a fuller explanation than is provided here. Refer to the Virtual Private Network Consortium http://www.vpnc.org/terms.html for further information.

Public Interface

A public interface is one that is used to connect IP Office directly to an xDSL or Internet router and thereby provide Internet access. (A public LAN is sometimes referred to as a demilitarized zone.) It is the function of the public interface to secure the Internal LAN from the Internet. IP Office uses a firewall and NAT functionality to afford the necessary protection on a public interface. A public interface connection is facilitated by the following IP Office interface types:

- LAN2
- Logical LAN
- WAN (PPP numbered)

The IP Office product family includes both single and dual interface systems as follows:

Single interface - IP403 and IP406: For single LAN systems a Logical LAN must be used for the configuration of the public interface.

Dual interface - IP 412 and IP Office Small Office Edition (IPSOE): For dual LAN systems the physical LAN2 interface is available and should be used as the public (external) LAN interface.

The following table summarizes the feature support for these public interface types:

Feature	IP412	IP406	IP403	IPSOE	Description
Firewall	√	√	√	√	IP Office Integral Firewall
Logical LAN	X	√	√	X	For single LAN systems a Logical LAN is a secondary interface which is created on the physical LAN1 interface.
LAN2	√	X	X	√	The LAN2 is a second physical Ethernet interface.
NAT	√	√	√	√	NAT allows multiple devices to communicate using a single IP address.
NAT Reverse Translation	√	x	x	√	The function that allows an unknown incoming IP session to be mapped to a local internal LAN IP address.
DHCP Client Mode	√	x	x	√	IP Office can automatically obtain an IP address from a DHCP server and add the IP address to the interface. This function is not supported on a Logical LAN interface.
H323	√	√	√	√	Originate or terminate H323.
IPSec	√	√	√	√	Originate or terminate IPSec.
L2TP	√	√	√	√	Originate or terminate L2TP.

Guidelines

1. DHCP client mode is not supported on the Logical LAN interface
2. DHCP client mode automatically adds a default route for Internet operation
3. RIP is not supported for IP Office secure VPN networking
4. For a PPP numbered WAN link:
   a. QOS is applied to VOIP traffic destined for VPN tunnel traffic before the encryption stage.
   b. A minimum bandwidth of between 1-2 Mbps is required for the link between the two systems is recommended.
   c. Do not run Multilink / QOS or IPHC on a WAN link that is passing VPN traffic.
   d. The QoS characteristics of IPO VoIP implementation is shown below:

Description	Value
Voice UDP port numbers range	OxC000 to 0xCFFF
Signalling TCP port number	1720
DSCP (TOS/Diffserv) value	OXB8

Internal LAN

An Internal LAN or private Internet is a secure networking area that has Internet access but is protected from the Internet by an external or “demilitarized zone”. Typically an internal LAN will use a private IP addressing scheme. The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private internets:

```
10.0.0.0      -   10.255.255.255   (10/8 prefix)
172.16.0.0    -   172.31.255.255   (172.16/12 prefix)
192.168.0.0   -   192.168.255.255  (192.168/16 prefix)
```

The pertinent IP Office features and function for VPN networking that relate to the Internal LAN are summarized in this section.

Feature	Description
DHCP Server	IP Office can perform the functions of a DHCP server for the Local LAN attached devices.
Wireless Networking	IP Office Small Office Edition supports 802.11b for wireless networking.
Telephony	Extensive and proven telephony features including Small Community Networking allow VPN wide virtual PABX .

Client VPN

A VPN client application is used to initiate secure VPN tunnels from a personal computer (PC) or notebook to a secure gateway. A VPN client application can be used, for example, to secure remote dial up connection over the Internet to the corporate office. Once the VPN client connection is established the PC and user application can be used transparently. Using MS-Windows, once the IPSec connection has been established an L2TP connection can then be established over the IPSec VPN. The IP Office Phone Manger Pro application can be used in conjunction with the supported VPN clients for secure VoIP transmission over the Internet.

IP Office running 3.0 software supports dynamic VPN endpoints. The dynamic VPN Tunnel support allows a VPN connection to be established in the instance where the VPN client IP address is unknown. This is the case for example when the Client VPN is initiated from a PC on a dialup ISP connection. Typically, in a dialup ISP connection, IP addresses are allocated only for the duration of the connection.

When configuring a dynamic tunnel endpoint on IP Office the same IPsec configuration form and hence the same password is used to facilitate all such remote users

Guidelines

1. Certificate Authority (CA) authentication is not supported for IPSec.
2. When using the generic Windows environment for IPSec, client operation uses the Microsoft Management Console (MMC) to add the IP Security Policy management snap-in. A windows register key change is required in order to support IPSec in pre-shared mode. To avoid this requirement, Avaya recommends the use of the NetScreen VPN client.
3. When configuring multiple Dynamic tunnels all such tunnels are supported by a single IPSec configuration instance (all remote users share the same pre-shared secret).

VPN and VoIP

Telephony

IP Office incorporates many advance telephony features which can be used in conjunction with VPN networking to provide secure speech over the Internet. Using such features as Small Community Networking, it is possible to create a virtual PABX that is transparent to the physical location.

VoIP

IP Office marks VPN packets with the DSCP value of the encapsulated VoIP packet. Under normal condition this allows IPSec or L2TP encapsulated packets to be distinguished and prioritized over non-voice traffic. Necessarily on slow speed links, packets may be re-ordered or dropped in support of voice quality when running QoS mechanisms. However, IPSec and LT2P packets cannot be excessively re-ordered which is an issue when mixing IPSec with VoIP and non-VoIP traffic over a heavily congested link.

IPSec is the primary VPN security protocol and is a licensable IP Office feature. To support IPSec with VoIP and non-VoIP traffic IP Office running version 3.0+ software employs a pre-emptive IPSec QoS mechanism that ensures that QoS is applied to packets before the IPSec process. This way, IPSec packet loss and packet re-ordering is significantly reduced.

The IPSec QoS feature is only available to IPSec. If it is a requirement to run L2TP with a mix VoIP and non-VoIP traffic then L2TP must be encapsulated in IPSec.

Under link congestion the IPSec QoS works on a pre-emptive basis by controlling the amount of packets that are sent to the IPSec engine and prioritizes VoIP traffic over non-VoIP traffic. In this way packet discard, when it occurs, will be on the inbound router interface. The provisions of the IPSec QoS mechanism allow for QoS support on slow speed xDSL links for example.

For voice traffic, IP Office performs concurrent call load restrictions on a per call basis and does not assume the bandwidth requirement. The IP line is used to configure concurrent call restrictions and works on the basis of an “allowed number of calls” irrespective of bandwidth. Hence, whilst IP Office is configured in terms of “an allowed number of calls” and not bandwidth requirements, it is important to understand the bandwidth requirement and calculations for any VoIP link. The bandwidth used by a given compression type for a single VoIP stream over a given VPN technology can be calculated using the formula shown below.

RTP Bandwidth:

(L2_ header + Tunneling _header + VoIP_header + Payload) X Payload_per_sec X Bit__conversion

For Fax traffic, the bandwidth used can be calculated using the formula shown below.

(L2_ header + Fax_header + Payload) X Payload_per_sec

Notes:

1. These calculations are strictly to estimate the "media" transport portion of the bandwidth. Even for the Media transport, an implementation dependent additional factor (e.g., 10%) should be considered to cover RTCP traffic, transitory effects, etc. For example, even when header compression is used, it it not effective on 100% of the packets.
2. Separate bandwidth must be allocated for signaling, including call setup and small community network signaling between systems. This traffic should be given a separate "assured forwarding" queue treatment, rather than the expedited forwarding required for RTP, but still must be given bandwidth needed.

An example of the Bandwidth Requirement Calculation is shown on page 21 and a table of the Bandwidth Calculation Variables used in the formula is shown on page 20.

Bandwidth Calculation Variables

Variable	Description	Option	Values
L2_ header			
Frame Relay RFC1490 + FR12	Assuming 2 bytes Frame Relay header.		5
Frame Relay Multilink PPP	Assuming 2 bytes Frame Relay header		6
Ethernet	The Ethernet header without the CRC	+ 4 bytes CRC	14
PPP (WAN)			2
Tunneling _header			
L2TP	The L2TP header comprising: IP = 20, UDP = 8 and L2TP header =11		39
IPSec	The IPSec header comprising the IP and ESP header (Tunnel Mode). The values specified here also include the ESP padding value. Use the appropriate IPSec header value to match the codec.	G723	52
		G729	52
		Net 8K	52
		G711	56
VoIP header			
VoIP_header	The VoIP header comprising the IP, UDP and RTP headers and is dependant on whether link is running IPHC.	With IPHC	4
Fax header			
Fax_header See note below:	The Fax header comprising: IP = 20, UDP = 8, RTP = 12 and Avaya info = 6	Without IPHC	46
Payload			
Payload	The number of bytes per sample	Type	Value
	VOIP	G711 G723 G729 Net 8K	160 24 20 20
	Fax	14400 12000 9600 7200	72 60 48 36
Sample Rate			
Payload_per_sec	The number of samples per second	Type	Value
	VOIP	G711 G723 G729 Net 8K	50 33.3 50 50
	Fax ((bytes to bits conversion is implicit))	14400 12000 9600 7200	200 200 200 200
Bytes to Bits per second			
Bit__conversion	Transmission speeds are always specified in Bits Per Second (BPS). The multiplication factor of 8 (i.e. X 8) is used to convert the calculation to bytes per second		8

Note: Fax bandwidth varies throughout the call, and is quite asymmetrical. It first starts out as RTP, then there is a period of relatively little bandwidth as the systems handshake, then there is asymmetrical bandwidth as the fax is transferred and the acknowledgements come back. E.g. there will be transitory periods during a "fax" call, where it will want the bandwidth of a voice call with the configured characteristics.

Bandwidth Requirement Calculation

Example 1

The following example uses the formula below to determine the total bandwidth required for a G729 call using IPSec encryption (3DES) over Ethernet. See page 20 for details of the variables.

(L2_ header + Tunneling _header + VoIP_header + Payload) X Payload_per_sec X Bit__conversion

Use the calculation above to determine total bandwidth requirement then set the appropriate values (in terms of the allowed number of calls) by using IP Line parameters.

Task	Description
Step 1 Chose the layer 2 media type: 14	For Ethernet the “L2_ header” value is 14 bytes.
Step 2 Choose the tunnel type: 52	For IPSec this value must be chosen with respect to the VoIP compression type that is to be used, for G729 this value is = 52. For L2TP the value is fixed for all compression types. For the case where IPSec and L2TP are used in conjunction e.g. L2TP protected IPSec both tunneling headers must be added.
Step 3 Choose the VoIP_header header type: **40**	Without IPHC the VoIP header is = 40.
Step 4 Choose the PAYLOAD type: **20**	This choice must be consistent with tunnel type (see step 2 above). For G729 this value is 20.
Step 5 Choose the sample rate: **50**	This choice must be consistent with tunnel type (see step 2 above). For G729 this value is 50.

For example, total bandwidth for a G729 call using IPSec over Ethernet is:

50400 = (14 + 52 + 40 + 20) * 50* 8 = 50.4Kbps (in each direction)

Note: The Ethernet header is generally stripped by the DSL.

Example 2

The following example uses the formula below to determine the total bandwidth required for a 14400 baud fax call using PPP encapsulated in Frame Relay. See page 21 for details of the variables.

(L2_ header + Fax_header + Payload) X Payload_per_sec

Use the calculation above to determine total bandwidth requirement then set the appropriate values (in terms of the allowed number of calls) by using IP Line parameters.

Task	Description
Step 1 Chose the layer 2 media type: **8**	For PPP encapsulated in Frame Relay the "L2_ header" value is 2 + 6 = 8 bytes.
Step 2 Choose the Fax_header type: **46**	
Step 3 Choose the PAYLOAD type: **72**	For 14400 Fax this value is 72.
Step 4 Choose the sample rate: **200**	For 14400 Fax this value is 200.

For example, total bandwidth for a 14400 fax call using PPP over Frame Relay is:

25200 = (8 + 46 + 72) * 200 = 25.2Kbps (in the direction of the fax traffic)

Guidelines

1. IP Office running 3.0+ has been limited to 1Mbps of throughput for all traffic types.
2. IP Office running 3.0+ does not support IPHC for VPN networking.
3. IPSec performs IP fragmentation in order to avoid illegal VPN frame sizes. IP Office does not perform IP fragmentation in support of QoS.
4. Although IP Office is able to perform fragmentation, IP Office will not respond to fragmented ICMP ping requests directed to its system interface address
5. The IPSec QoS feature is only available to IPSec. If it is a requirement to run L2TP with a mix of VoIP and non-VoIP traffic, then L2TP traffic must be encapsulated in IPSec.
6. When running IPSec over a WAN link and using PPP, the normal QoS mechanism (multilink and IPHC) should not be used. Under IP Office 3.0+ implementation IPSec uses a separate QoS mechanism which is not configurable. The DSCP values that are specified on the Manager application System/Gatekeeper form are however used in the normal way to distinguish VoIP traffic types.

Maximum Load

The table below shows the maximum load figures for VPN and VoIP calls for all IP Office platforms running 3.0+ software. The bandwidth figures quoted below are for both directions.

Description	IP406 V2		IP412		IP403/IP406		SOE	
	Calls	Bandwidth	Calls	Bandwidth	Calls	Bandwidth	Calls	Bandwidth
G711	16	3.8Mbs	6	1.4Mbs	2	0.47Mbs	2	0.47Mbs
G729	22	2.4Mbs	13	1.4Mbs	5	0.55Mbs	4	0.44Mbs
G723	30	2Mbs	19	1.4mbs	7	0.53Mbs	6	0.49Mbs
Recommended max. number of Tunnels	10		10		4		4	

Notes:

1. The higher speed and bandwidth of the IP406 V2 platform (running 2.1+ software) is because the IPsec encryption and decryption processing is now performed in hardware. The encryption and decryption hardware for IPSec removes this processing overhead from the CPU. In this way the throughput performance for IPSec is significantly increased. The IP Small Office, IP403 and IP412 platforms IPSec encryption and decryption processing within software.
2. The bandwidth figures quoted above are for VoIP calls **without** data. Therefore, as VoIP calls take precedence in transmission, consideration should be made to reduce the number of VoIP calls where data is to be transmitted. E.g. an 80/20% ratio between VoIP and Data is recommended.

Configuration

IPSec Configuration

The IP Security form is used to configure an IPSec security policy between two IPSec peers. Three tabs are available on the IPSec form (Main, IKE and IPSec). The Main tab is used to set the IP addressing conditions and Local/Remote gateway IP addresses while the IKE and IPSec Policies tabs are used to configure specific IPSec parameters.

The general method of IPSec configuration is shown below:

1. Configure and test IP connectivity between the two peers.
2. Configure an IPSec form and set the IP addressing conditions to trigger a Security Association (SA).

The IP Security Menu

Access to this menu is:

1. With the Manager application open, click on **Tunnel**.
2. Click the **IPSec** radio button and then click **OK**.
3. The following menu is displayed:

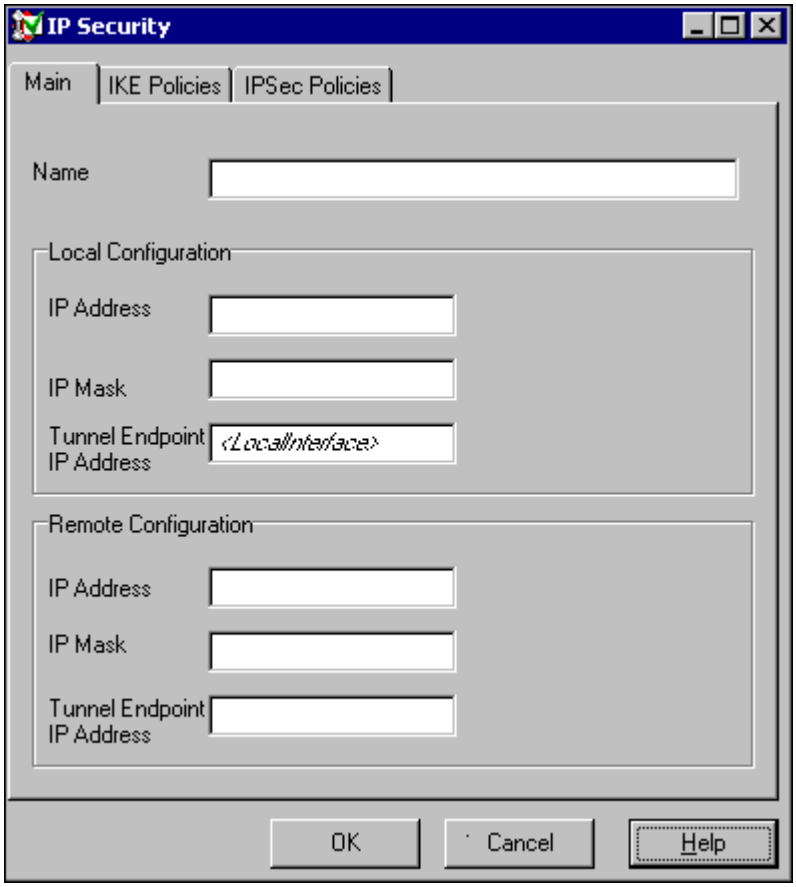

Figure 9. The IP Security Menu

Caution: Although the IPSec Menu is displayed and can be completed, a valid IPSec Tunneling licence is required for the feature to be activated. Indication of the absence of a License is given in the SysMonitor application when an attempt is made to activate the configuration; an example of this message is shown below.

```
29967mS IPSecEvent: IPSec Not Licensed - VPN security is not
available

32005mS PPP LCP Rx: v=wan_link
```

The table below details the parameters that are included on the Main tab of the IPSec Security menu.

<table>
<tr><th>Main tab</th><th colspan="2">Description</th></tr>
<tr><td>Name</td><td colspan="2">A unique name for the tunnel.</td></tr>
<tr><td rowspan="3">Local Configuration:
• IP Address
• IP Mask

Remote Configuration
• IP Address
• IP Mask</td><td colspan="2">The IP Address and IP Mask are used in conjunction with each other to configure and set the conditions for this Security Association (SA) with regard to inbound and outbound IP packets.
In order to understand the relationship between the Local and Remote configuration when setting the conditions of the policy, the direction of the packet must be considered.
With respect to the local system an IP packet is inbound or outbound to the IPSec tunnel. The table below details the relationship between the Local and Remote configuration in these two cases.</td></tr>
<tr><td>Inbound (from tunnel)</td><td>Outbound (into tunnel)</td></tr>
<tr><td>Local IP Address/Mask defines the destination IP address.
Remote IP Address/Mask defines the source IP address.
For any received IPSec encapsulated packet there must be a match on the SA for the destination and source IP addresses else the packet is discarded.</td><td>Local IP Address/Mask defines the source IP address.

Remote IP/Address defines destination IP address.

For any IP packet that is to be forwarded, IP Office determines a match to a SA on the basis of source and destination IP addresses.
When an IP packet is matched in this way it is forwarded with IPSec encapsulation (ESP).
When an IP packet is not matched in this way it is forwarded without IPSec encapsulation.</td></tr>
<tr><td>Local Configuration
• Tunnel Endpoint IP Address</td><td colspan="2">The local source IP address that is to be used to establish the SA to the remote peer. If left un-configured, IP Office will use the IP address of the local interface on which the tunnel is to be originated, except in the case of numbered PPP link. In this case, the IP Address that is assigned to the PPP service must be used. See IPSec over the WAN on page 49.</td></tr>
<tr><td>Remote Configuration
• Tunnel Endpoint IP Address</td><td colspan="2">The IP address of the peer to which a SA must be established before the specified local and remote addresses can be forwarded.</td></tr>
</table>

Note: The term Main tab does not relate to the IPSec Main mode (IPSec Main mode is the function of the IKE tab, see page 28).

Guidelines - Local and Remote IP Address/Mask configuration

1. When both IP Address and IP Mask fields are left un-configured this means “match all”. Typically this case is used to match Internet traffic.
2. Unless an explicit policy exists for the local subnet it will not be matched. This means an un-configured entry as detailed above will **not** match any locally attached subnets (i.e. LAN interfaces).
3. IP Office does not AND the IP Address with the Mask Fields but ensures that the network address and Mask are compatible when configuring. For example, an IP address of 192.168.42.1 with a mask 255.255.255.0 is an invalid combination. Two valid combinations are shown below:
   a. IP Address 192.168.42.1 Mask 255.255.255.255
   b. IP Address 192.168.42.0 Mask 255.255.255.0
4. A single "condition" in terms of addressing can be specified for a given SA. The SA condition can be applied between two hosts or between two subnets or a combination of these, i.e. host to subnet. Multiple conditions for an SA are not supported in the IP Office VPN implementation.

Guidelines - Local and Remote Gateway

1. The Local Gateway field is used to specify a source IP address to be used when originating a tunnel. Left un-configured (default), IP Office uses the IP address of the outgoing interface at which the tunnel is to be established.
2. Similarly, for Client initiated tunnels, where the IP Address (dynamically allocated by the ISP) of the remote peer is unknown, the Remote Gateway field should be left un-configured.

IKE and IPSec Policies Tabs

Previously, the way in which the Main tab is used to set the conditions that "trigger" the SA was described (see page 24). The IKE and IPSec Policies tabs are used to configure and complete the rest of the policy for the SA. Each SA requires a unique IPSec form in respect of each peer which can be either a Client or another IPSec Gateway.

Note: Client applications and other third Party IPSec implementations may refer to Phase 1 and Phase 2 negotiations as Proposal 1 and Proposal 2. The IKE and IPSec Policies tabs equate to Phase 1 and Phase 2 negotiations respectively.

Generally, it is not important to understand the requirements in the detail of these tabs but it is however important that they are matched between two IPSec peers seeking to establish an SA.

During Phase 1 of negotiations, IKE is used to establish a secure channel for performing further IKE negotiations. In Phase 2, IKE is used to negotiate the SA (Authentication Header or Encapsulation Security Payload). This method prevents a third party from knowing the type of encryption that is to be used. The diagram shows the elements and functions of these tabs and shows the first stage of the negotiations.

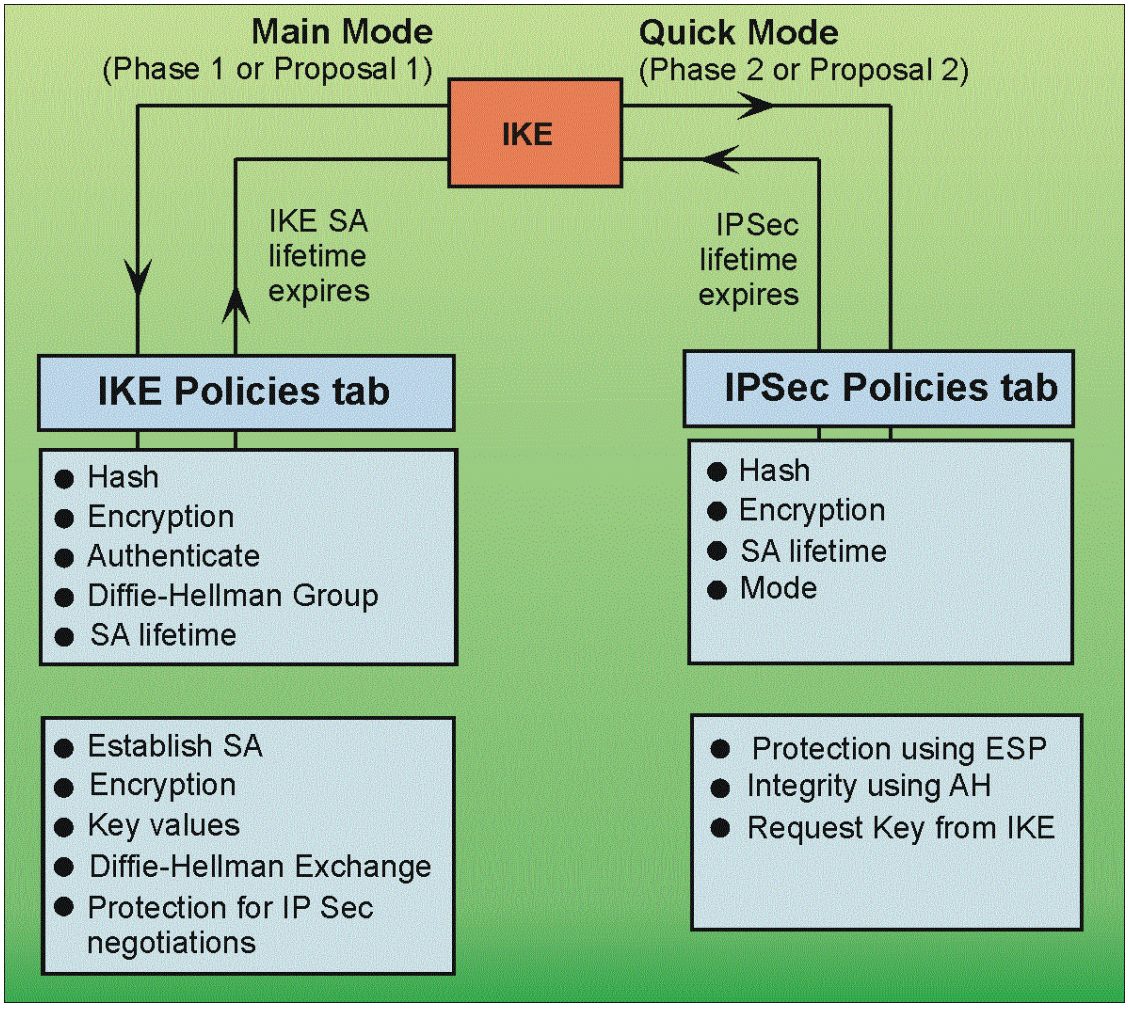

Figure 10. IP Phase 1 and Phase 2 negotiations

The following sections detail the configurable options for both the IKE and IPSec Policies tabs.

IKE Policies tab

During Phase 1 negotiations, Internet Key Exchange (IKE) is used to establish a secure channel for performing further IKE negotiations (see page 27). In Phase 2, IKE is used to negotiate the SA (using either the Authentication Header or Encapsulation Security Payload).

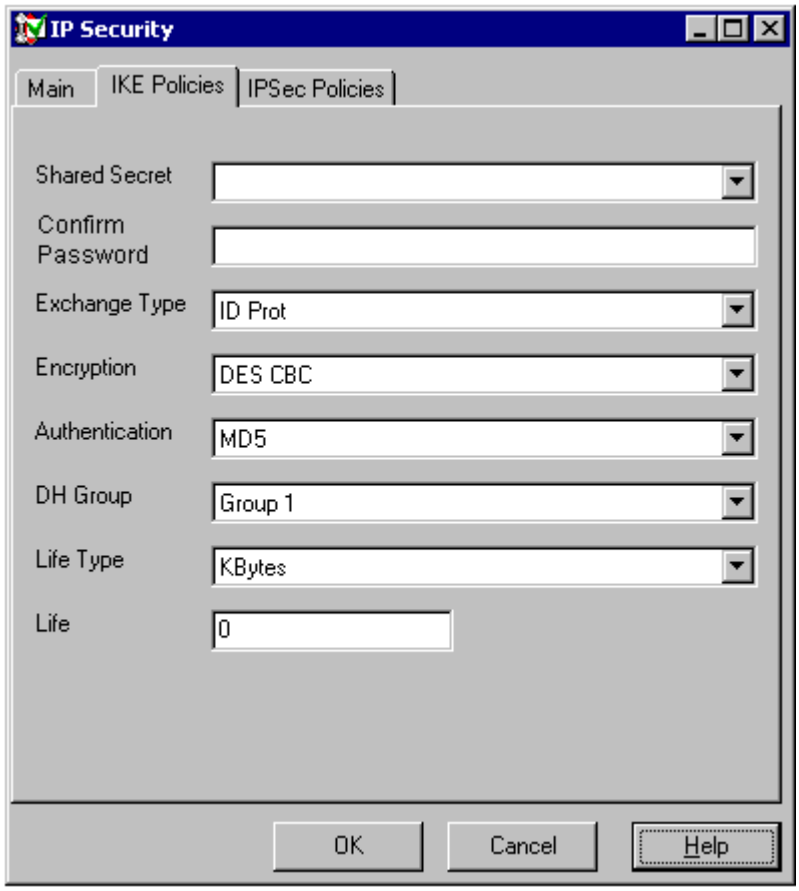

Figure 11. The IKE Policies tab

Parameter	Options	Description
Shared Secret		**Must be** the same on both ends.
Exchange type	Default = ID Prot/Aggressive	Aggressive provides faster security but does not hide the IDs of the communicating device. ID is slower but does hide the IDs of the communicating device.
Encryption	DES or 3DES	Set the encryption method.
Authentication	MD5 – 128 bit (default) SHA – 160 bit. Any	The method of password authentication.
DH Group	Group 1 = 768 bits (default) Group 2 = 1024	Diffie-Hellman Key Exchange.
Life Time	<Seconds or Kilobytes >	Set whether **Life** below is measured in seconds or Kilobytes.
Life	Blank at default – set in either seconds or Kilobytes as defined in **Life Time** above	Determines the period of time or the number bytes after which the SA key is refreshed or re-calculated.

IPSec Policies tab

The IPSec Policies tab is used to configure and complete the SA policy. Each SA requires a unique IPSec form for each peer, which can be either a client or another IPSec Gateway (see page 27).

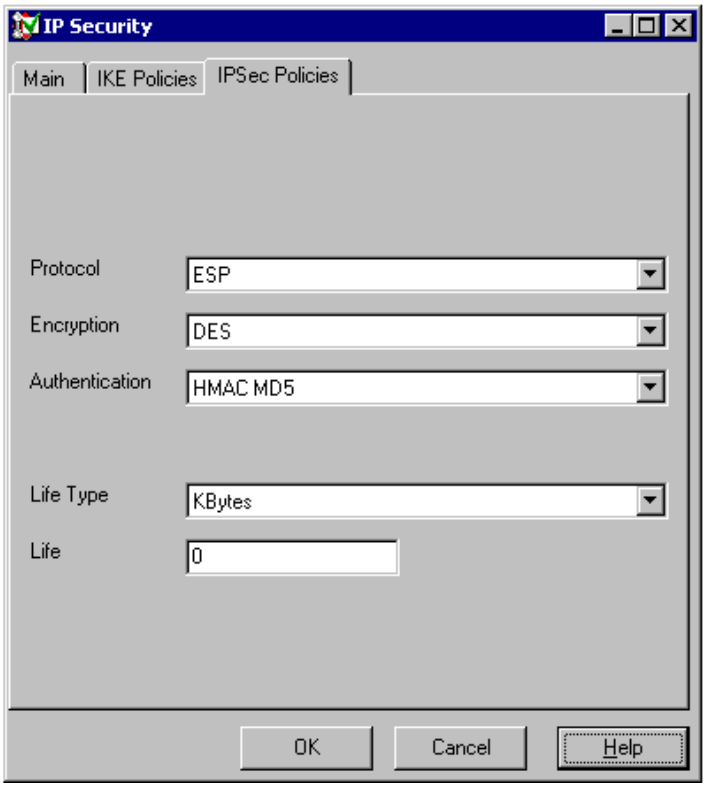

Figure 12. The IPSec Policies tab

Caution: Although the IPSec Menu is displayed and can be completed, a valid IPSec Tunneling licence is required for the feature to be activated (see The IP Security Menu on page 24).

Parameter	Options	Description
Protocol	ESP (Encapsulation Security Payload) AH (Authentication Header)	**ESP** Provides authentication, integrity and confidentiality. Secures everything in the packet that follows the header. Also authenticates the packet payload on a packet-by-packet basis. **AH.** No encryption, encapsulation or confidentiality. Only authentication and integrity. Also authenticates portions of the IP header of the packet (source /destination).
Encryption	DES - 56 Bit 3DES - 168 Bit AES – 128, 192, 256	The encryption method to be used.
Authentication	HMAC MD5 – 128 bit. HMAC SHA – 160 bit.	The method of password authentication.
Life Time	<Seconds or Kilobytes >	Set whether **Life** below is measured in seconds or Kilobytes.
Life	Blank at default – set in either seconds or Kilobytes as defined in **Life Time** above	Determines the period of time or the number bytes after which the SA key is refreshed or re-calculated.

L2TP Configuration

The L2TP form consists of three tabs (Tunnel, L2TP and PPP).

Access to these tabs is:

1. With the Manager application open, click on **Tunnel** and then right click in the display panel.
2. Select **New** and the **Tunnel Selection** menu is displayed.
3. Click the **L2TP** radio button and then click **OK**.

The L2TP/Tunnel menu is displayed.

The general method of L2TP configuration is:

1. Configure and test IP connectivity between the two peers.
2. Configure the LTP2 Tunnel parameters
3. Configure an IP route entry.

L2TP/Tunnel tab

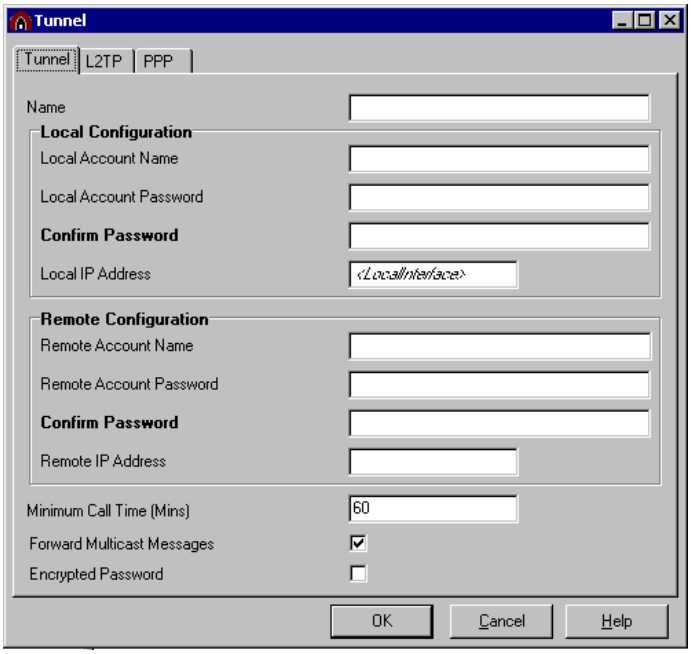

Figure 13. The L2TP/Tunnel Menu

Parameter	Options	Description
Name	A unique name for the tunnel. Once the tunnel is created, the name can be selected as a destination in the IP Route table.	
Local /Remote Configuration	Account Name and Password	Used to set the PPP authentication parameters The Local name is the username that is used in outgoing authentication. The Remote name is the username that is expected for the authentication of the peer.
Local IP Address	<IP address>	The source IP address to use when originating an L2TP tunnel. By default <un-configured> IP Office uses the IP address of the interface on which the tunnel is to be established as the source address of tunnel.
Remote IP Address	<IP address>	The IP address of the remote L2TP peer.
Minimum Call Time (mins)	Default = 60 mins	The minimum time that the tunnel will remain active.
Forward Multicast Messages	Default = On	Permits the tunnel to carry multicast messages when on.
Encrypted Password	Default = off	When selected, the CHAP protocol is used to authenticate the incoming peer.

L2TP/L2TP tab

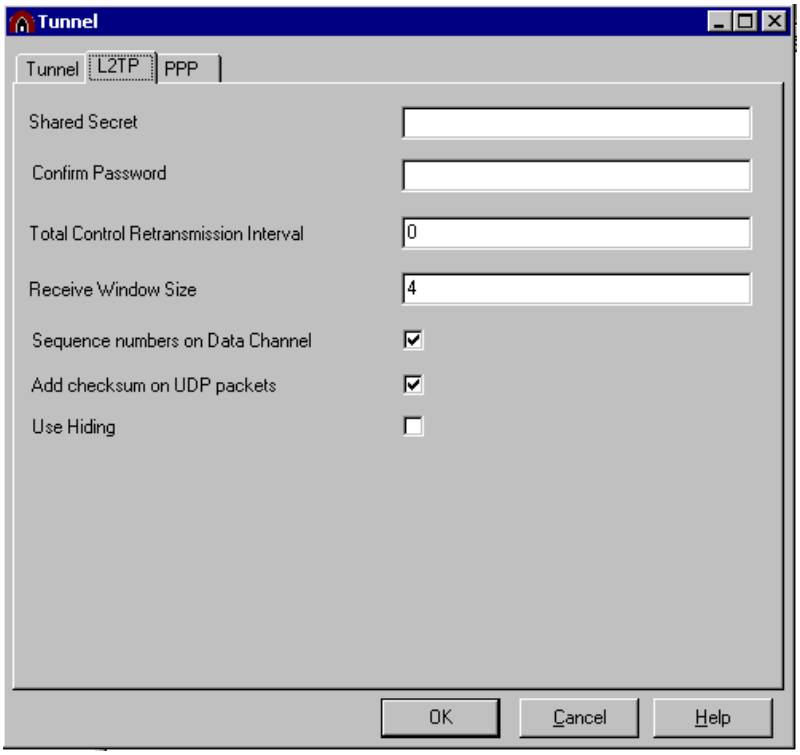

Figure 14. The L2TP/L2TP tab

Parameter	Options	Description
Shared Secret/Confirm Password		User setting used for authentication. **Must be** matched by both peers. This password is separate to the PPP authentication parameters defined on the L2TP/Tunnel tab (see page 30).
Total Control Retransmission Interval	Default = 0	The time delay before retransmission.
Receive Window Size	Default = 4	The number of unacknowledged packest allowed.
Sequence numbers on Data Channel	Default = On	When on, add sequence numbers to L2TP packets.
Add checksum on UDP packets	Default = On	When on, uses a checksum to verify L2TP packets.
Use Hiding	Default = Off	When on, encrypts the tunnel's control channel.

L2TP/PPP tab

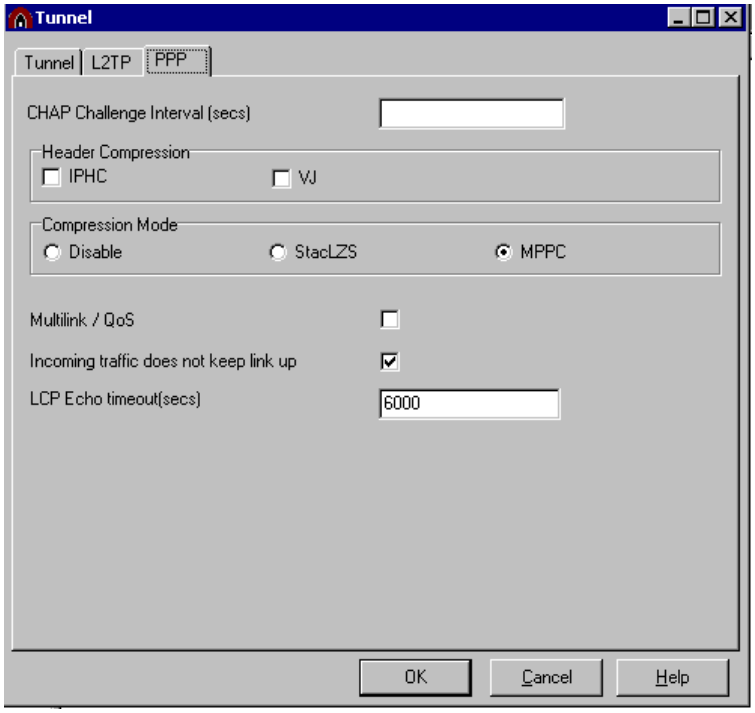

Figure 15. The L2TP/PPP tab

Parameter	Options	Description
CHAP Challenge Interval		A time interval between the successive CHAP challenges on an active link.
Header Compression IPHC VJ	Default = Off	IP header Compression.
Compression Mode Disable StackLZS MPPC	Default = all Off	Data compression of PPP packets.
Multlink /QoS	Default = Off	Enables the Multlink PPP protocol in support of QoS.
Incoming traffic does not keep link up	Default = On	Prevents the link remaining connected unnecessarily.
LCP Echo	Default = 6000 sec	The time period to wait for response to a PPP keep-alive message. The connection is terminated if the peer fails to respond to 3 LCP Echo Requests. Increasing this value will increases the time IP Office takes to determine if a L2TP peer is not responding.

Guidelines

1. Unless there is a specific requirement, it is recommended that the default parameter value is used.
2. It is recommended that Encrypted Password option is used. When selected, the CHAP protocol hashes the password during authentication exchanges and is used to authenticate the incoming L2TP peer. PAP authentication, which employs clear text password exchanges, is used when the Encrypted Password option is not selected.

Logical LAN Menu

The Logical LAN feature allows a secondary LAN or logical Ethernet interface to be created. Hence, single LAN systems, such as the IP403 or IP406, can be used as dual LAN systems. Using this arrangement the Logical LAN provides the public interface and the physical LAN1 provides the internal LAN functions.

Because a logical LAN interface is NAT enabled, any number of PCs on the system LAN interface (LAN1) can access the Internet. The Logical LAN interface may be used with any xDSL or a third party Internet LAN attached router. The MAC address of the next hop router must be known to complete the configuration of the Logical LAN interface.

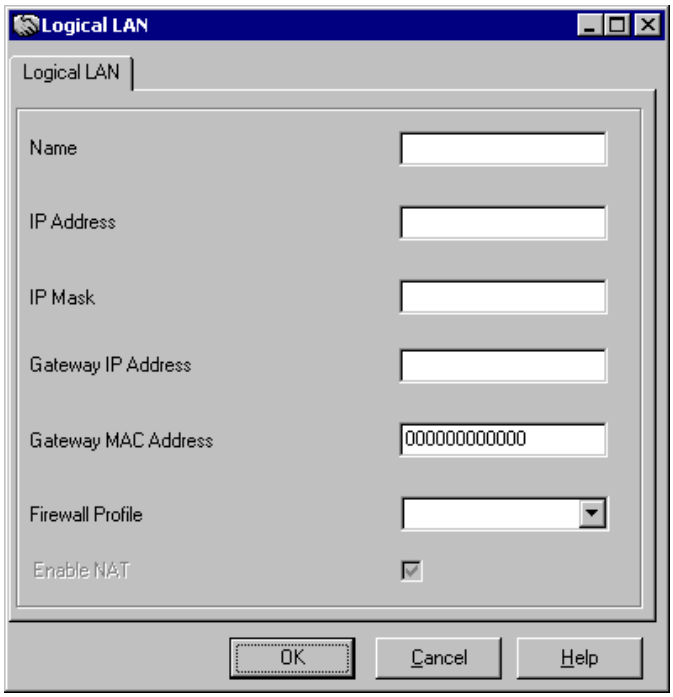

Figure 16. The Logical LAN Menu

Parameter	Options	Description
Name		A unique name for the logical interface. Once the logical interface is created, the name can be selected as a destination in the IP Route table.
IP Address/IP Mask		IP address/IP Mask of the logical interface.
Gateway IP Address		The IP Address of the next hop router (see Guidelines below).
Gateway MAC Address		The Ethernet MAC address of the next hop router (see Guidelines below).
Firewall		A Firewall Profile that is associated to this interface.
Enable NAT	Default = On	NAT functionality allows any number of PC on LAN1 (the Internal LAN1) to access the Internet via the Logical LAN. NAT is enabled by default and cannot be disabled for this interface type.

Guidelines

1. With the IP Office VPN implementation, the Logical LAN parameter Gateway MAC Address must be used to specify and configure the router that is the next hop. The Gateway IP Address field can be used for information purposes or can be left un-configured. It is not used to resolve the next hop router MAC address.
2. When adding an IP route entry, which uses a Logical LAN interface destination, the Gateway field should be left un-configured. It must not be set to the next hop router address. This is because the next hop router MAC address must be specified on the Logical LAN Gateway MAC address parameter (see previous Guideline).

Configuration Examples

This section details example configuration and guidelines for IP Office VPN scenarios. To aid clarity, the configuration procedure for VPN has been separated from general IP connectivity and therefore this section is divided into three parts:

Part 1 Basic Internet Access: Highlights a number of ways to connect IP Office to the Internet (see page 34).

Part 2 VPN configuration: Details of VPN configuration examples (see page 37).

Part 3 VoIP configuration: Details of a VoIP configuration example (see page 53).

This three-part approach allows the configuration to be verified at each stage.

The organization of this section is such that the advanced IP Office administrator may choose to go directly to the to the relevant section.

To assist with debugging it is recommended that the Ethereal application is used. Ethereal is a free network protocol analyzer for Windows and Unix systems. Ethereal provides real-time analysis of network traffic and capture to disk. The application is available for download at http://www.ethereal.com/. Some of the examples include packet exchanges captured using this application, an example of which is shown below.

```
L2TP    Control Message - SCCRQ
L2TP    Control Message - SCCRP
L2TP    Control Message - SCCRN
```

Part 1: Basic Internet Access

Internet Access using a Logical Interface

The Logical LAN allows a secondary interface to be created on the LAN1 interface and hence IP Office to be used as a LAN to LAN router (IP403 or IP406). Because a logical LAN interface is NAT enabled any number of PC on the system LAN interface (LAN1) can access the Internet. The Logical LAN interface may be used with any xDSL or a third party Internet router.

VPN connections are typically between two systems. This configuration forms the basis of the configuration examples detailed in Parts 1 and 2 (see pages 34 and 37).

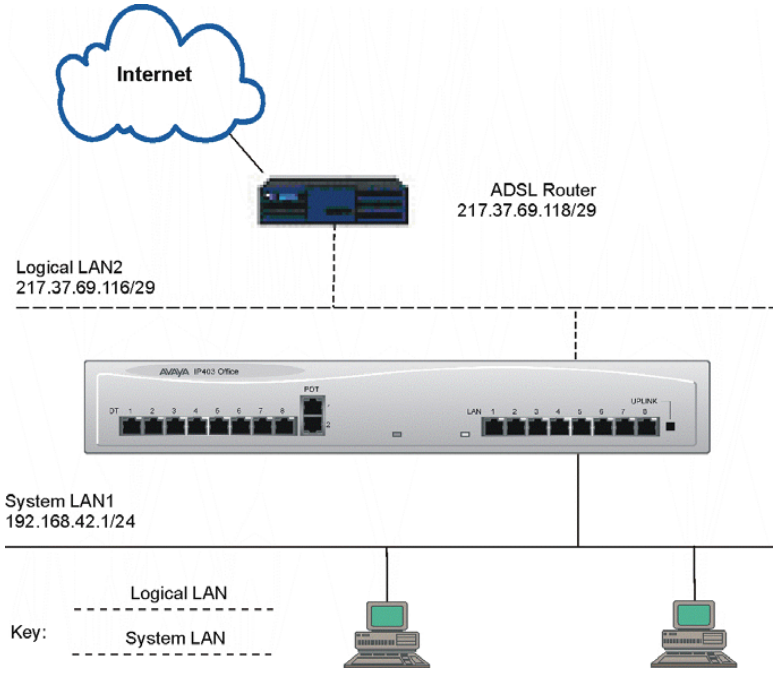

Figure 17. Internet Access Via the Logical LAN

Task	Description
Step 1 Within Manager, right click the Logical LAN entity and create a new Logical LAN.	See page 33.
Step2 Logical LAN values • Name = LLAN • IP Address = 217.37.69.116 • IP Mask = 255.255.255.248 • Gateway IP Address = <217.37.69.118> • Gateway MAC Address = <MAC address of the ADSL router> * See Note below* • Firewall Profile = <un-configured>	The logical interface is in effect a secondary LAN and is normally used on single LAN IP Office system, to connect to ADSL routers for example. Name – A name for the Logical LAN The Gateway IP Address and Gateway MAC Address will be that of the ADSL. * See Note below: NAT is enabled by default on the logical interface and cannot be disabled. IP Office facilitates the locally originated system to tunneling traffic through an attached NAT enabled interface. NAT is applied to traffic that is **not** tunneled using the Logical LAN interface address.
Step 3 Within Manager, right click the IP Route entity and create a new IP Route. Add a default route for Internet access pointing to the Logical LAN interface. • IP Address = <un-configured> • IP Mask = <un-configured> • Gateway = <un-configured> • Destination = LLAN	See page 33. The Logical LAN interface is a special case and does not require the use of the Gateway parameter for the IP route configuration.
Step 4 Check the configuration. It should be possible to perform the following. • PING the ADSL router • Browse the Internet	It will **not** be possible to PING the Internal LAN from the Internet. Do not proceed until all tests are successful.

*** Note:** One method of obtaining the MAC address of the default gateway is to plug your PC directly into the DSL Router, use *ipconfig /renew* to obtain the Default Gateway IP Adress. Ping this address and then obtain the MAC address of the ADSL router by checking your PC's arp cache with the *arp -a* command.

Basic Internet Access using LAN2

This configuration example provides similar functionally as the previous example (see page 34) but is different in that a physical interface is used to provide Internet access.

VPN connections are typically between two systems. This configuration forms the basis of the configuration examples detailed in Parts 1 and 2 (see pages 34 and 37).

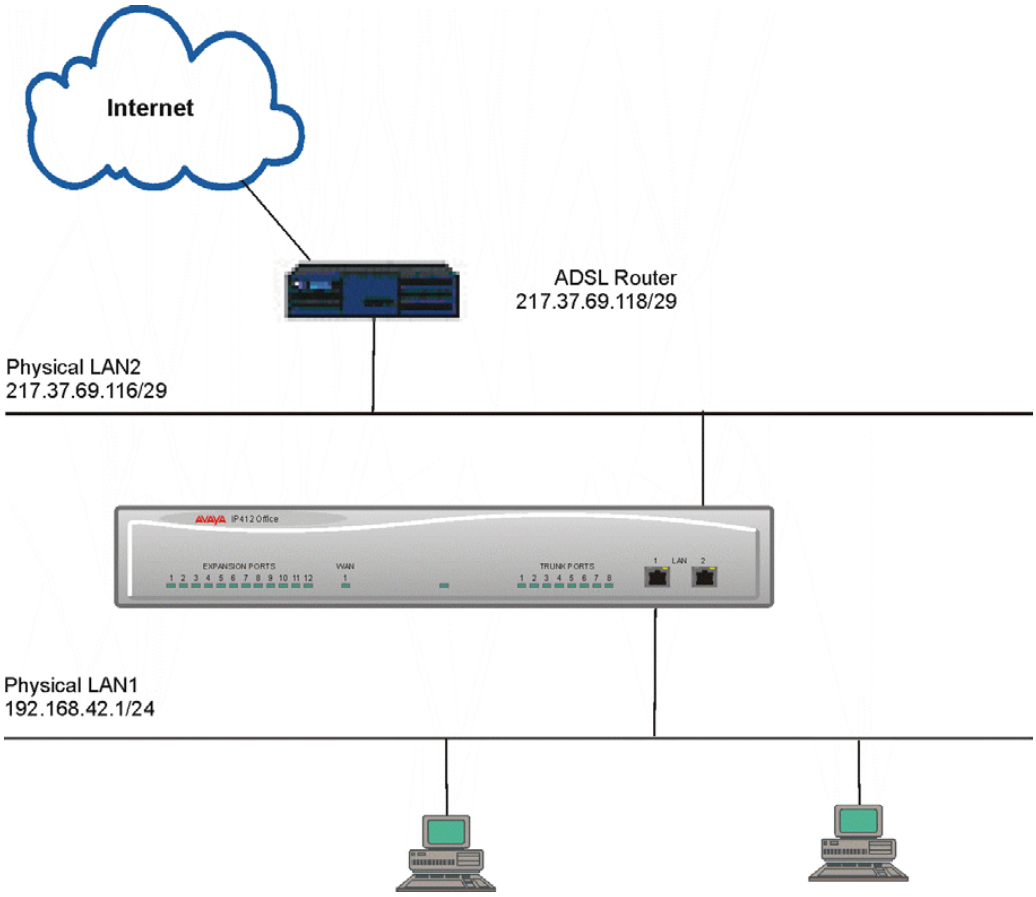

Figure 18. Internet Access Via LAN2

Task	Description
Step 1 Within Manager, configure the LAN2 tab on the System form with the values shown below. • IP Address = 217.37.69.116 • IP Mask = 255.255.255.248 • DHCP = <Disabled> • Enable NAT = <selected> • Firewall Profile = <un-configured>	Firewall is optional in this configuration. This configuration uses the NAT functionality on LAN2. Without this NAT the private IP addressing scheme of LAN1 would not be able to access the Internet.
Step 2 Add the Default IP Route for the LAN2. • IP Address = <un-configured> • IP Mask = <un-configured> • Gateway = 217.37.69.118 • Destination = LAN2	Default route for Internet access.
Step 3 On completion of the above steps, test the configuration. It should be possible to perform the following • PING the ADSL router • Browse the Internet	Do not proceed until all tests are successful.

Part 2: VPN configuration

IPSec - Between Two IP Office systems over ADSL using the Logical LAN

The network consists of two IP403 systems that are linked to the Internet using ADSL modems. The configuration utilizes NAT functionality to access the Internet and IPSec to establish a secure VPN between the two sites. The network provides the following benefits:

- Secure VPN data networking for shared resources
- Internet access for corporate users
- Secure IP telephony between corporate sites.

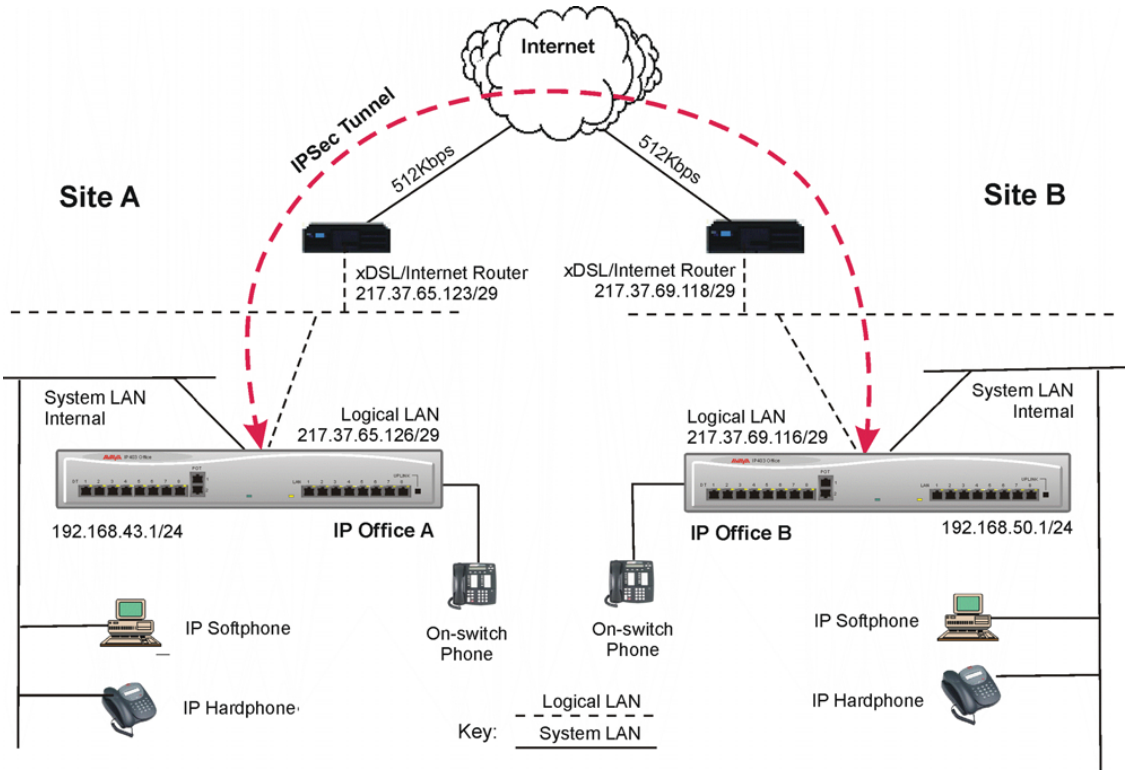

Figure 19. IP Office to IP Office via Logical LAN

The following step-by-step instructions describe how to configure the network shown above. Refer to page 53 for details on configuration of the VoIP element of this network. This configuration utilizes a Logical LAN Interface, the configuration of which is detailed in Internet Access using a Logical Interface on page 34.

Task	Description
Step 1 In order to establish IP connectivity, configure the two systems using the IP addressing details above.	See the Basic Internet access section - Internet Access using a Logical Interface on page 34.
Step 2 Check for IP Connectivity	Before beginning the configuration of the IPSec element of this example it must be possible to perform the following tasks. • IP Office A: Ping the local ADSL router • IP Office A: Ping the remote ADSL router • IP Office A: Ping the remote IP Office B [1] • IP Office A: Browse the Internet • IP Office B: Browse the Internet • IP Office B: Ping the local ADSL router • IP Office B: Ping the remote ADSL router • IP Office B: Ping the remote IP Office A [1] [1] Assumes that the Firewall Profile is not active on the receiving interface. Do not proceed until all of these tests are successful. It should **not** be possible to ping between the Internal LANs at this stage.
Step 3 Install the IPSec licence.	An IPSec licence is required for each IP Office system in an SA. Make sure the IPSec licences are valid on both systems. Licence name – IPSec Tunneling.
Step 4 For IP Office A create an IPSec tunnel. Main tab • Name = IPSec_Tunnel • Local IP Address = 192.168.43.0 • Local IP Mask = 255.255.255.0 • Gateway - <LocalInterface> • Remote IP Address = 192.168.50.0 • Remote IP Mask = 255.255.255.0 • Gateway = 217.37.69.116	A unique name for the IPSec tunnel is required. The Local IP Address/Mask is the range of IP addresses you want to secure through the tunnel. The Remote IP Address is the remote networks IP address range to be secured through the tunnel. The Gateway is the IPSec tunnel endpoint address.
Step 5 For IP Office A perform the following. IKE Polices tab • Shared Secret = password • Exchange Type = ID port • Encryption = DES • Authentication = MD5 • DH Group = Group 2 • Life Type = Seconds • Life = 86400	Both tunnel endpoints must have the same-shared secret. Encryption set to DES. Authentication set to MD5 Diffie-Hellman Group = Group 2 This is the time period before a new key is generated (86400 represents one day in seconds).

Task	Description
Step 6 For IP Office A perform the following. IPSec Policies tab • Protocol = ESP • Encryption = DES • Authentication = MD5 • Life Type = Seconds • Life = 86400	Protocol set to Encapsulating Security Payload. Encryption set to DES Authentication set to MD5 This is the time period before a new key is generated (86400 represents one day in seconds).
Step 7 For IP Office B create an IPSec tunnel. Main tab • Name = IPSec_Tunnel • Local IP Address = 192.168.50.0 • Local IP Mask = 255.255.255.0 • Gateway - <LocalInterface> • Remote IP Address = 192.168.43.0 • Remote IP Mask = 255.255.255.0 • Gateway = 217.37.65.126	A unique name for the IPSec tunnel is required. The Local IP Address/Mask is the range of IP addresses you want to secure through the tunnel. The Remote IP Address is the remote networks IP address range to be secured through the tunnel. The Gateway is the IPSec tunnel endpoint address.
Step 8 For IP Office B use the parameters shown in Steps 5 and 6 to complete the IKE and IPSec form configurations.	In order for an IPSec SA to be established between two systems the IKE and IPSec Policies form must be identical for each peer.

Step 9
Check to see if the tunnel is up.
	Using a protocol analyzer, check to see that the six ISAKMP Main Mode messages appear.
	Check to see that four Quick Mode messages appear.
	This Signifies that the IPSec Tunnel is up.
	
	`ISAKMP Identity Protection (Main Mode)`
	`ISAKMP Identity Protection (Main Mode)`
	`ISAKMP Identity Protection (Main Mode)`
	`ISAKMP Identity Protection (Main Mode)`
	`ISAKMP Identity Protection (Main Mode)`
	`ISAKMP Identity Protection (Main Mode)`
	`ISAKMP Quick Mode`
	`ISAKMP Quick Mode`
	`ISAKMP Quick Mode`
	`ISAKMP Quick Mode`
	
	When passing data through the tunnel you should see ESP packets on the protocol analyzer.
	
	The tunnel will be activated when routable traffic is presented.

Step 10 For VoIP configuration refer to Part 3 VoIP Configuration on page 53	Before beginning the VoIP configurations for this example it **must be** possible to ping between the Internal LANs Do not proceed until all tests are successful.

L2TP/IPSec between two IP Office's

The network consists of an IP412 at the corporate office and a number of IP Office - Small Office Editions at the branch offices. These are linked to the Internet using xDSL/Internet routers. The configuration utilizes NAT functionality to access the Internet and IPSec to establish a secure VPN between the two sites. The network provides the following benefits:

- Secure VPN data networking for shared resources
- Internet access for corporate users
- Secure IP telephony between corporate sites

The following example can be used to form the basis of a star networking VPN topology where the corporate office IP412 (IPO_CO) is the central VPN terminator and the PABX/data router for several remote branch offices equipped with IP Office - Small Office Editions.

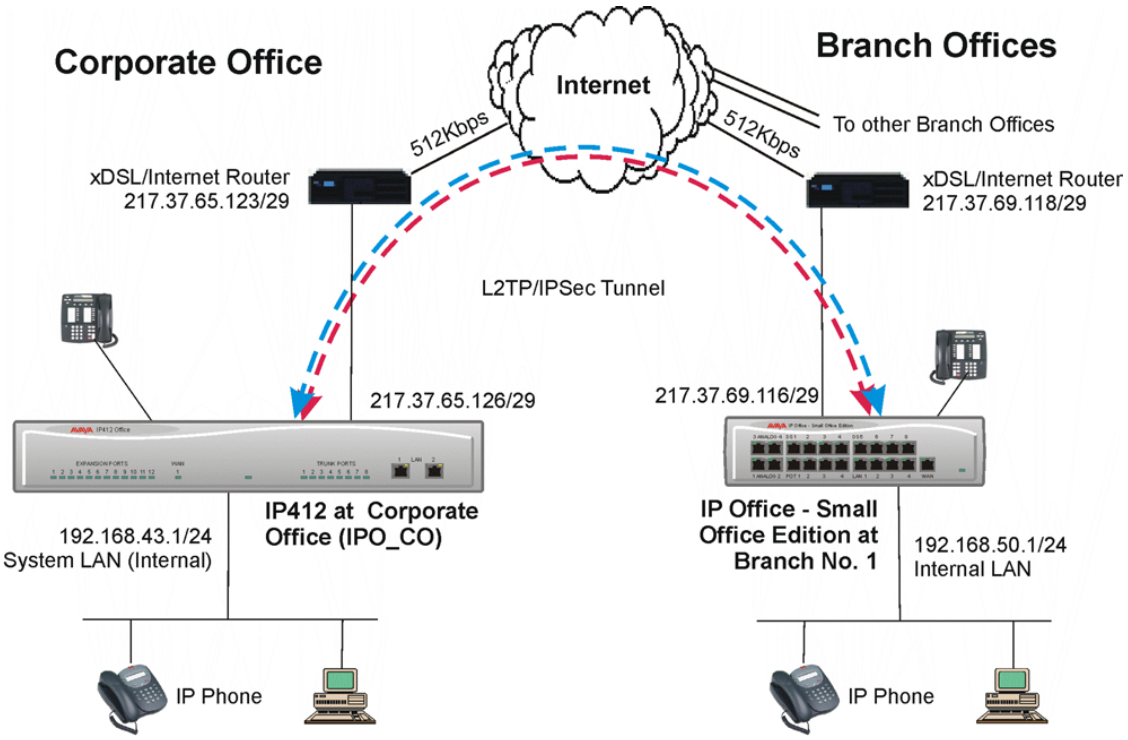

Figure 20. L2TP/IPSec - IP Office to IP Office

The general method of configuration used in this example is:

1. Configure and test IP connectivity between the two peers.
2. Configure the LTP2 tunnel parameters and test.
3. Configure the IPSec tunnel parameters and test.

This procedure is divided into two parts

- Part 1 = L2TP configuration (see page 41).
- Part 2 = IPSec configuration (see page 43)

Both parts provide details of corporate office to branch office No. 1 only. However, to add additional branch offices, repeat the procedures using the relevant details for the subsequent branch offices.

Part 1 - L2TP configuration

In order to establish IP connectivity, configure the systems using the IP addresses detailed in Figure 20 (see page 40).

Task	Description
Step 1 For IPO_CO create an L2TP tunnel (see page 30). Tunnel tab • Name = L2TP • Local Account Name = Administrator • Local Account Password = password • Remote Account Name = Administrator • Remote Account Password = password • Remote IP Address = 217.37.69.116 • Minimum Call Time = 60 • Encrypt Password = < selected>	A unique name for the L2TP tunnel is required. The Local Account name/password is used to authenticate the user at the remote end. The Remote Account name/password is used to authenticate the incoming user. The Remote IP Address is the tunnel endpoint. In this example it is 217.37.69.116, the IP address of Branch No.1. When Encrypt Password is selected, CHAP is used to authenticate the L2TP connection.
Step 2 For Branch No. 1,create an L2TP tunnel and apply the same parameter values as in the previous step except for the parameter shown below. • Remote IP Address = 217.37.65.126	The Remote IP Address is the tunnel endpoint. In this example it is 217.37.65.126, the IP address of the IPO_CO.
Step 3 For both the IPO_CO and Branch No. 1, perform the following: L2TP tab • Shared Secret = password • Sequence Numbers on Data Channel = <unselected> • Add Checksum on UDP packets = <unselected> • Use Hiding = <unselected>	Both tunnel endpoints must have the same-shared secret. All other settings are default settings.
Step 4 For both the IPO_CO and Branch No. 1, perform the following: PPP tab • CHAP Challenge Interval = <un-configured> • Header compression = <unselected> • Compression Mode = <Disable> • Multilink/QoS = <unselected> • Incoming Traffic = <selected> • LCP echo timeout = 6000	CHAP Challenge interval set if using CHAP. Header compression – IPHC, VJ Compression Mode – Disable, StacLZS, MPPC.

Task	Description
Step 5 Create the following two IP Routes on IPO_CO: (1) • IP Address = 192.168.50.0 • IP Mask = 255.255.255.0 • Gateway = <un-configured> • Destination = L2TP (2) • IP Address = <un-configured> • IP Mask = <un-configured> • Gateway = 217.37.65.123 • Destination = LAN2	(1) The default route pointing all traffic into the L2TP Tunnel. (2) A 32 bit route to the tunnel endpoint. A 32 route is only for a single IP address.
Step 6 Create the following two IP Routes on Branch No. 1: **(1)** • IP Address = 192.168.43.0 • IP Mask = 255.255.255.0 • Gateway = <un-configured> • Destination = L2TP (2) • IP Address = <un-configured> • IP Mask = <un-configured> • Gateway = 217.37.69.118 • Destination = LAN2	These routing entries will allow the tunnel to forward traffic, destined for the remote network, to the local VPN router.
Step 7 Checking to see if the Tunnel is up.	Using Ethereal, check packet exchanges are occurring in the L2TP Tunnel. L2TP Control Message - SCCRQ L2TP Control Message - SCCRP L2TP Control Message - SCCCN Use SysMonitor to view PPP packet exchanges. PPP echo Request /Reply packets will be see (if selected) when the L2TP tunnel is active. They will also be seen when the active L2TP tunnel is protected by IPSec.

Part 2 - IPSec configuration

With Part 1 completed (see page 41), perform the following:

Task	Description
Step 1 Install the IPSec Licence. Licence name – IPSec Tunneling.	An IPSec Licence is required per IP Office. Make sure the IPSec licences are valid on both PC's.
Step 2 For IPO_CO create an IPSec tunnel (see page 24). Main tab • Name = IPSec_Tunnel • Local IP Address = 217.37.65.126 • Local IP Mask = 255.255.255.255 • Gateway - <LocalInterface> • Remote IP Address = 217.37.69.116 • Remote IP Mask = 255.255.255.255 • Gateway = 217.37.69.116	A name for the IPSec tunnel is required. The Local IP Address/Mask is the range of IP addresses you want to secure through the tunnel. The Remote IP Address is the remote networks IP address range that we want to secure through the tunnel. The Remote IP Mask is the remote mask. The Gateway is the **tunnel endpoint**. Hence, for IPO_CO, the remote Gateway will be 217.37.69.116, which is the IP address of Branch No. 1.
Step 3 For IPO_CO perform the following in the IKE Polices tab: • Shared Secret = password • Exchange Type = ID port • Encryption = DES • Authentication = MD5 • DH Group = Group 2 • Life Type = Seconds • Life = 86400	Both tunnel endpoints must have the same-shared secret. Encryption set to DES. Authentication set to MD5 Diffie-Hellman Group = Group 2 This is the time period before a new key is generated (86400 represents one day in seconds).
Step 4 For IPO_CO, perform the following in the IPSec Policies tab: • Protocol = ESP • Encryption = DES • Authentication = MD5 • Life Type = Seconds • Life = 86400	Protocol set to Encapsulating Security Payload. Encryption set to DES Authentication set to MD5 This is the time period before a new key is generated (86400 represents one day in seconds).
Step 5 For Branch No. 1 create an IPSec tunnel. Main tab • Name = IPSec_Tunnel • Local IP Address = 217.37.69.116 • Local IP Mask = 255.255.255.255 • Gateway - <LocalInterface> • Remote IP Address = 217.37.65.126 • Remote IP Mask = 255.255.255.255 • Gateway = 217.37.65.126	A name for the IPSec tunnel is required. The Local IP Address/Mask is the range of IP addresses you want to secure through the tunnel. The Remote IP Address is the remote networks IP address range that we want to secure through the tunnel. The Remote IP Mask is the remote mask. The Gateway is the **tunnel endpoint**. Hence, for Branch No. 1, the remote Gateway will be 217.37.65.116, which is the IP address of IPO_CO.

Task	Description
Step 6 For Branch No. 1, use the parameters shown in Steps 3 and 4 to complete the IPSec form configuration.	In order for an IPSec SA to be established between two systems the IKE and IPSec Policies form must be identical for each peer.

Step 7
Checking to see if the tunnel is up.
	Using a protocol analyser check to see that the six ISAKMP Main Mode messages appear.
	Check to see that four Quick Mode messages appear.
	`ISAKMP Identity Protection (Main Mode)`
	`ISAKMP Identity Protection (Main Mode)`
	`ISAKMP Identity Protection (Main Mode)`
	`ISAKMP Identity Protection (Main Mode)`
	`ISAKMP Identity Protection (Main Mode)`
	`ISAKMP Identity Protection (Main Mode)`
	`ISAKMP Quick Mode`
	`ISAKMP Quick Mode`
	`ISAKMP Quick Mode`
	`ISAKMP Quick Mode`
	This Signifies that the IPSec Tunnel is up.
	
	When passing data through the tunnel you should see ESP packets on the protocol analyser.
	
	Use SysMonitor to view PPP packet exchanges. PPP echo Request /Reply packets will be see (if selected) when the L2TP tunnel is active. They will also be seen when the active L2TP tunnel is protected by IPSec.

For VoIP configuration refer to Part 3 VoIP Configuration on page 53.

IPSec encrypts all L2TP data, including the L2TP tunnel setup packets. This is an example of L2TP running inside IPSec.

IPSec Client Application (Dynamic Mode)

The following example shows a simple configuration that allows a client initiated IPsec connection to be terminated on IP Office.

Using this network, the homeworker is able to access the corporate office over a secure IPsec connection for both telephony and to access corporate resources. Internet access for both the homeworker and corporate network user is outside the established IPsec tunnel and is not be secured.

One of the key aspect to this application is that IP Office support Dynamic tunnels.

IP Office is able to create a Dynamic tunnel in the case were the IP address of the Remote tunnel end point is unknown. This may be the case for example if the Homeworker uses a-single-user-xDSL line or dialup via a local ISP.

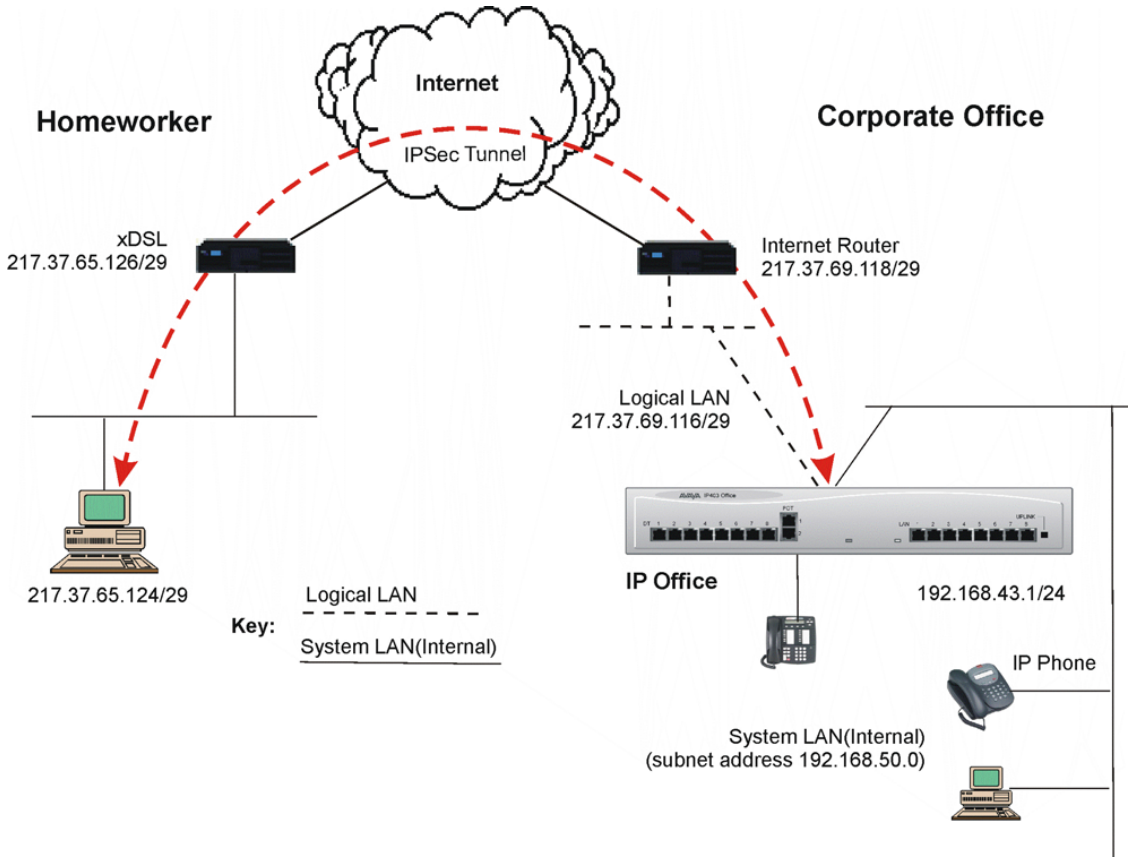

Figure 21. PC running IPSec Client Application

The procedure is divided into two parts:

- VPN Client Configuration (see page 46).
- IP Office Configuration (see page 47).

Part 1 - VPN Client Configuration

Install the NetScreen-Remote VPN Client application and create a new connection using the details shown in the table below. The information shown here is specific to NetScreen-Remote 10.0.0 (build 10).

NetScreen-Remote VPN Client
1- My Connection New Connection Connection Security: Secure Remote Party Identity & Addressing ID Type: IP subnet Subnet:192.168.43.0 Mask:255.255.255.0 Port: All Protocol: All Connect using: Secure Gateway Tunnel ID Type: IP address 217.37.69.116 My Identity Pre-shared Key: password Select Certificate: None ID Type: IP Address Port: All Virtual Adapter: Disable Internet Interface: <Local _NIC_Card_Name> IP Address: 217.37.65.124 Security Policy Select Phase 1 Negotiation Mode: Main Authentication (Phase1) Proposal 1 Authentication method: pre-shared key Encryp Alg: DES Hash Alg: MD5 SA life: Seconds Seconds: 86400 Key Group: Diffie-Hellman Group 1 Authentication (Phase2) Proposal 2 SA life: Seconds Seconds: 86400 Compression: None Encapsulation ESP: <selected> Encrypt Alg: DES Hash Alg: MD5 Encapsulation: Tunnel

Part 2 - IP Office Configuration

Task	Description
Step 1 Within Manager, create and configure a Logical LAN interface using the details below (see page 33). • Name = Logical_LAN • IP Address = 217.37.69.116 • IP Mask = 255.255.255.248 • Gateway IP Address = 217.37.69.118 • Gateway MAC Address (Internet Router) • Firewall Profile = none.	See Basic Internet access section - Internet Access using a Logical Interface on page 34. **Note:** It is not necessary to specifically use a Logical LAN. Alternatively, a LAN2 interface can be used (IP412 or SOE).
Step 2 Add an IP Route on IP Office: • IP Address = <un-configured> • IP Mask = <un-configured> • Gateway = <un-configured> • Destination = Logical_LAN	
Step 3 Install the IPSec Licence. Licence name – IPSec Tunneling.	An IPSec licence is required per IP Office. Make sure the IPSec licence is valid in the Manager.
Step 4 For IP Office create an IPSec tunnel: Main tab • Name = IPSec_Tunnel • Local IP Address = 192.168.43.0 • Local IP Mask = 255.255.255.0 • Tunnel Endpoint IP Address = <LocalInterface> • Remote IP Address = <unconfigured> • Remote IP Mask = <unconfigured> • Tunnel Endpoint IP Address = <unconfigured>	A discrete name for the IPSec tunnel is required. The Local IP Address/Mask is the range of IP addresses you want to secure through the tunnel, e.g. 192.168.50.1/24 will give a subnet address of 192.168.50.0. This single IPSec configuration supports all remote dial-up clients. In the case where the remote endpoint is unknown, the Remote IP Address, IP Mask and Tunnel Endpoint IP Address should be left <unconfigured>.
Step 5 For IP Office, perform the following on the IKE Polices tab: • Shared Secret = password • Exchange Type = ID port • Encryption = DES • Authentication = MD5 • DH Group = Group 1 • Life Type = Seconds • Life = 86400	Both tunnel endpoints must have the same-shared secret. Encryption set to DES. Authentication set to MD5 Diffie-Hellman Group = Group 2 This is the time period before a new key is generated (86400 represents one day in seconds).

Task	Description
Step 6 For IP Office, perform the following on the IPSec Policies tab: • Protocol = ESP • Encryption = DES • Authentication = MD5 • Life Type = Seconds • Life = 86400	Protocol set to Encapsulating Security Payload. Encryption set to DES Authentication set to MD5 This is the time period before a new key is generated (86400 represents one day in seconds).
Step 7 Check connection	Activate the Security Policy on the Windows PC by right clicking the SoftRemote icon in the task bar. Using a protocol analyser check to see that the ISAKMP Main Mode messages appear.

For VoIP configuration refer to Part 3 VoIP Configuration on page 53.

IPSec over the WAN

The IPSec Tunnel will be established over the WAN in order to secure all IP traffic between subnets. As an alternative, Frame Relay could be use instead of the dedicated WAN link. This section is split into two parts as follows:

1. A PPP numbered WAN Link.
2. An Un-numbered PPP WAN Link.

The difference between the two highlights the use of the Tunnel Endpoints IP Addresses. Both of these methods can be used on either the integral IP Office WAN interface or on a T1 interface when used in a non-channalized mode.

A Numbered PPP WAN Link

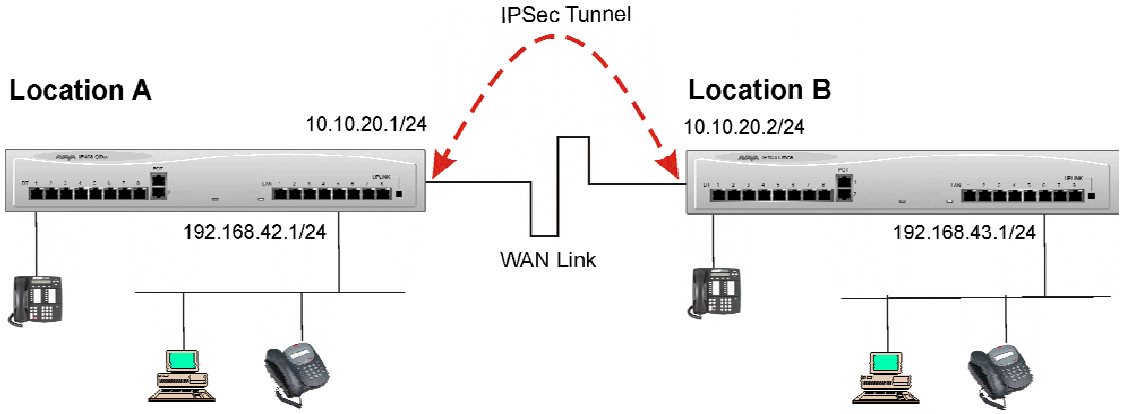

Figure 22. A Numbered PPP WAN Link

Task	Description
Step1 Configure the WAN link using the diagram above and check for correct operation. The following settings are required on the PPP tab of the WAN Service form for both systems. • Header Compression Mode = <unselected> • Multilink/QoS =<unselected> In support of numbered PPP interface mode add the following to IP tab of the WAN Service form. **Location A** • IP Address = 10.10.20.1 • IP Mask = 255.255.255.0 **Location B** • IP Address = 10.10.20.2 • IP Mask = 255.255.255.0	The IPSec tunnel will be established over the WAN in order secure IP traffic between the two subnets. Hence, the WAN link must be established before attempting security configuration. IPSec does not use the normal QoS facilities of IP Office. A PPP link that is configured and uses an IP address, is referred to as a numbered PPP link The addresses used to create the numbered PPP link will be used (later in this example) as the IP sec tunnel endpoint address.
Step 2 Install the IPSec Licence. Licence name = IPSec tunneling.	An IPSec Licence is required per IP Office. Make sure the IPSec licenses are valid on both systems.

Task	Description
Step 3 For IP Office **Location A** create an IPSec tunnel (see The IP Security Menu on page 24). **Main tab:** **Local Configuration:** • Name = IPSec_Tunnel • IP Address = 192.168.42.0 • IP Mask = 255.255.255.0 • Tunnel Endpoint IP Address = <10.10.20.1> **Remote Configuration:** • IP Address = 192.168.43.0 • IP Mask = 255.255.255.0 Tunnel Endpoint IP Address = <10.10.20.2>	A discrete name for the IPSec tunnel is required. The Local Configuration for the IP Address/Mask and Remote IP Address/Mask determines the range of IP addresses to be secured through the tunnel. The Local Tunnel Endpoint IP Address is the near end tunnel endpoint. Hence, for Location A, this will be 10.10.20.1, which is the WAN IP address of Location A. The Remote Tunnel Endpoint IP Address is the far end tunnel endpoint. Hence, for Location A, this will be 10.10.20.2, which is the WAN IP address of Location B.
Step 4 For IP Office **Location B** create an IPSec tunnel (see The IP Security Menu on page 24). **Main tab:** **Local Configuration:** • Name = IPSec_Tunnel • IP Address = 192.168.43.0 • IP Mask = 255.255.255.0 • Tunnel Endpoint IP Address = <10.10.20.2> Remote Configuration: • IP Address = 192.168.42.0 • IP Mask = 255.255.255.0 • Tunnel Endpoint IP Address = <10.10.20.1>	See notes in step 3 above. The Local Tunnel Endpoint IP Address is the near end tunnel endpoint. Hence, for Location B, this will be 10.10.20.2, which is the WAN IP address of Location B. The Remote Tunnel Endpoint IP Address is the far end tunnel endpoint. Hence, for Location B, this will be 10.10.20.1, which is the WAN IP address of Location A.
Step 5 For both IP Office Location A and Location B, perform the following: IKE Polices tab • Shared Secret = password • Exchange Type = ID port • Encryption = DES • Authentication = MD5 • DH Group = Group 2 • Life Type = Seconds • Life = 86400	These parameters set the Phase 1 negotiation for the SA.
Step 6 For both IP Office Location A and Location B,perform the following: IPSec Policies tab • Protocol = ESP • Encryption = DES • Authentication = MD5 • Life Type = Seconds • Life = 86400	These parameters set the Phase 2 negotiation for the SA.
Step 7 Checking to see if the tunnel is up.	Use the SysMonitor application to check if ESP packets are generated when ICMP ping requests are sent between the subnets.

For VoIP configuration refer to Part 3 VoIP Configuration on page 53.

An Un-numbered PPP WAN Link

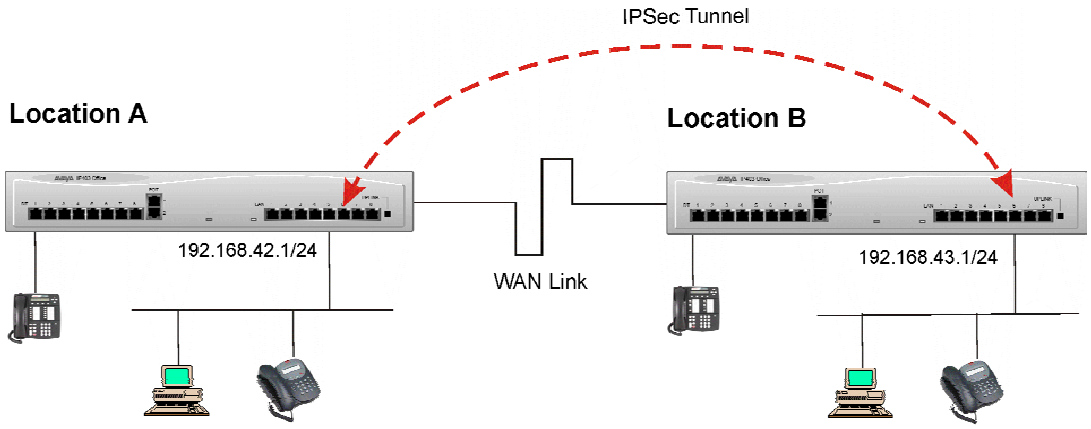

Figure 23. An Un-numbered PPP WAN Link

Task	Description
Step1 Configure the WAN link using the diagram above and check for correct operation. The following settings are required on the PPP tab of the WAN Service form: • Header Compression Mode = <unselected> • Multilink/QoS =<unselected>	The IPSec tunnel will be established over the WAN in order secure IP traffic between the two subnets. Hence, the WAN link must be established before attempting security configuration. IPSec does not use the normal QoS facilities of IP Office.
Step 2 Install the IPSec Licence. Licence name = IPSec tunneling.	An IPSec Licence is required per IP Office. Make sure the IPSec licenses are valid on both systems.
Step 3 For IP Office **Location A** create an IPSec tunnel (see The IP Security Menu on page 24). **Main tab:** **Local Configuration:** • Name = IPSec_Tunnel • IP Address = 192.168.42.0 • IP Mask = 255.255.255.0 • Tunnel Endpoint IP Address = <192.168.42.1> **Remote Configuration:** • IP Address = 192.168.43.0 • IP Mask = 255.255.255.0 • Tunnel Endpoint IP Address = <192.168.43.1>	A discrete name for the IPSec tunnel is required. The Local Configuration for the IP Address/Mask and Remote IP Address/Mask determines the range of IP addresses to be secured through the tunnel. The Local Tunnel Endpoint IP Address is the near end tunnel endpoint. Hence, for Location A, this will be 192.168.42.1, which is the LAN1 IP address of Location A. The Remote Tunnel Endpoint IP Address is the far end tunnel endpoint. Hence, for Location A, this will be 192.168.43.1, which is the LAN1 IP address of Location B.

Task	Description
Step 4 For IP Office **Location B** create an IPSec tunnel (see The IP Security Menu on page 24). **Main tab:** **Local Configuration:** • Name = IPSec_Tunnel • IP Address = 192.168.43.0 • IP Mask = 255.255.255.0 • Tunnel Endpoint IP Address = 192.168.43.1 **Remote Configuration:** • IP Address = 192.168.42.0 • IP Mask = 255.255.255.0 • Tunnel Endpoint IP Address = 192.168.42.1	 See notes in step 3 above. The Local Tunnel Endpoint IP Address is the near end tunnel endpoint. Hence, for Location A, this will be 192.168.43.1, which is the LAN1 IP address of Location B The Remote Gateway is the far end tunnel endpoint. Hence, for Location B, this will be 192.168.42.1, which is the LAN1 IP address of Location A.
Step 5 For both IP Office Location A and Location B, perform the following: IKE Polices tab • Shared Secret = password • Exchange Type = ID port • Encryption = DES • Authentication = MD5 • DH Group = Group 2 • Life Type = Seconds • Life = 86400	These parameters set the Phase 1 negotiation for the SA.
Step 6 For both IP Office Location A and Location B,perform the following: IPSec Policies tab • Protocol = ESP • Encryption = DES • Authentication = MD5 • Life Type = Seconds • Life = 86400	These parameters set the Phase 2 negotiation for the SA.
Step 7 Checking to see if the tunnel is up.	Use the SysMonitor application to check if ESP packets are generated when ICMP ping requests are sent between the subnets.

For VoIP configuration refer to Part 3 VoIP Configuration on page 53.

Part 3 VoIP Configuration

Once a VPN connection is established and working, VoIP configuration can be applied. For this reason it is important to have full IP connectivity before beginning VoIP configuration.

Because the VoIP configuration is transparent to the means of IP connectivity, the configuration procedure described here can be applied to any of the examples shown in earlier sections (see pages 34 and 37). However, for the sake of clarity, the following example is specific to the IP Office to IP Office via Logical LAN example shown on page 37.

On completion of the steps detailed in the table below it will be possible make calls between Site A and Site B using the IP hard phones, the IP soft phones and the on-switch phones.

Task	Description
Step 1 Check that the IPSec Tunnel is established between the two systems (see page 37).	Before beginning the VoIP configurations of this example it must be possible to perform the following tasks: Ping between the Internal LANs (through the established IPSec tunnel). Ping the remote internal system IP address and confirm that the resulting packet exchanges are shown using the SysMonitor/Interface decode options. Do not proceed until all tests are successful.
Step 2 Within Manager, for Office A create an IP Line and apply the following parameters. Using the Line tab of the IP Line form: • Line Number = 2 • OutGoing Group ID = 2	The IP Line is used to configure the VoIP Gateway for IP Office. IP Line number provides a discriminator to other line groups. No two line groups can share the same line number The Line Group ID as an absolute reference to a IP Line. It is permissible for 2 IP Lines to share the same Line ID in the case where redundancy is required. The IP Line number cannot exceed 240.
Step 3 Within Manager, for IP Office B create an IP Line and apply the following parameters. Using the Line tab of the IP Line form: • Line Number = 3 • OutGoing Group ID = 3	
Step 4 For IP Office A and IP Office B, apply the bandwidth restrictions using the Line tab of the IP Line forms. • Number of Channels = 5 • Outgoing Channels = 5 • Voice Channels =5 • Data Channels = 5 This must be done on **both** IP Office A and IP Office B	Under the IP Office (3.0+) implementation, the maximum bandwidth that can be used for IPSec encrypted VoIP calls is limited to either 512 (IP412) or 256Kbps (SMO, IP401, IP403, IP406). This is enough to allow up to five G729 calls. As the total bandwidth between the two xDSL lines is 512Kbps this will allow for 256Kbps (50%) for non-voice traffic between the two locations

Task	Description
Step 5 Within Manager, for Office A set the destination VoIP Gateway to the IP address of the internal interface address of IP Office B. Use the VoIP tab of the IP Line to set the following parameters. • Gateway IP Address = <192.168.50.1> • Compression mode = <G729>	The IP Line is used to configure the VoIP Gateway for IP Office. Although the LAN2 interface can be used to terminate a VoIP gateway. In this example The IP Office VoIP Gateway function residing on the internal LAN will be used. This because the IPSec Tunnel is already terminated on the External Interface G711 offers the best quality speech but uses the highest bandwidth. G711 should be used on LAN or WAN links were bandwidth availability is not an issue. G729 and 723 ultra low voice compression allows optimum use of slow speed WAN links.
Step 6 Within Manager, for IP Office B set the destination VoIP Gateway to the IP address of the Internal interface address of IP Office B Use VoIP tab of the IP Line to set the following parameters. • Gateway IP Address = <192.168.43.1> • Compression Mode = <G729>	See the notes in step 5.
Step 7 Select the required VoIP options • FAX Transport • Silence Suppression • Local Tones	Ensure that the following optional parameters are matched for **both** Office A and IP Office B.
Step 8 (Choose call routing method) IP Office is configured to use either Voice Networking or short codes for call route selection. Chose either Steps 8a or 8b to configure call route selection.	Voice networking Enables extension number sharing with the remote IP Office system. Extensions on the remote system can then be dialed from the local system. Voice Networking is sometimes referenced as Small Community Networking. Shortcodes Defines the rules and sets the condition under which the IP Office will invoke the IP Line.

Task	Description
Step 8a (optional) Voice Networking To enable Voice networking select the following option on the VoIP tab of the IP Line form. This must be done on IP Office A and IP Office B	Make sure that the telephone extension ranges on the two IP Offices are different.
Step 8b (optional) Short Code To enable route selection by Short Codes create a Short Code and add the following details: **For IP Office A** • Short Code = 8N • Telephone Number = N • Line Group ID = 2 • Feature = Dial **For IP Office B** • Short Code = 8N • Telephone Number = N • Line Group ID = 3 • Feature = Dial	
Step 9 Register IP Phones to the local IP Office units. Ensue the following parameters are configured Gatekeeper tab on the system form: • Auto-Create Extension = <selected> • Gatekeeper Enable = <selected> LAN1 tab on the System form: • DHCP Mode = <Server>	Ensure that the IP phones are registered to their local IP Office. If selected, H.323 terminals will automatically register themselves with the Gatekeeper thus creating a Extension in the configuration. IP Phones are connected to the LAN and therefore pick-up an IP address via the LAN1 DHCP Server. The Local IP Office provides the Gatekeeper function. In the IPSec Client Application example (see page 45), ensure that Phone Manager registration takes place through the tunnel. All registration traffic is encrypted.

Glossary

AH	Authentication Header. Within the IPSec architecture, the packet format for algorithms and general issues associated with authentication. See SA.
ARP	Address Resolution Protocol. A low level protocol within the TCP/IP suite that *maps* IP addresses to the corresponding Ethernet addresses.
ASN.1	Abstract Syntax Notation (1). A method for describing data that is used in many other standards.
CHAP	Challenge-Handshake Authentication Protocol. An authentication method that can be used when connecting to an ISP.
CO	Central Office. A common carrier switching centre in which trunks and/or loops are terminated and switched.
CPE	Customer Premise Equipment. Systems that are at a customer's site (as compared systems that are in a service provider's network, see CO).
DES	Data Encryption Standard. A cryptographic encryption algorithm that is part of many standards.
Diffie-Hellman	A cryptographic key-exchange algorithm that is part of many standards. See also X9.42.
Digital Signature	A method for proving that the holder of a private key is the originator of a message
DSS	Digital Signature Standard. A cryptographic signature algorithm that is part of many standards. Also called DSA (Digital Signature Algorithm).
DSL	Digital Subscriber Line. A generic name for a family of digital lines (also called xDSL) provided by the competitive Local Exchange Carrier and local telephone companies to their local subscribers.
ESP	Encapsulating Security Payload. Within the IPSec architecture, the packet format for algorithms and general issues associated with encryption. See SA.
HardPhone	The term HardPhone refers to a IP extension, a dedicated LAN attached H323 compliant device
IKE	Internet Key Exchange. The protocol used to exchange symmetric keys for performing IPSec.
ISDN	Integrated Services Digital Network. A set of international standards for a switched network that supports access to any type of service.
IPSec	IP Security. The protocol used to provide authentication and/or encryption to IP traffic.
IPSOE	IP Office - Small Office Edition. The smallest member of the IP Office family of phone systems.
ISP	Internet Service Provider.
ISAKMP	Internet Security Association and Key Management Protocol. The basis for IKE.
LAC	L2TP Access Concentrator.
L2TP	Layer 2 Tunneling Protocol. Provides a means for tunneling IP traffic in layer 2. Can be used with IPSec to provide authentication.
LDAP	Lightweight Directory Access Protocol. A simpler protocol for directory access than X.500.
LDP	Label Distribution Protocol.
LNS	L2TP Network Server.
LSR	Label Switching Router. A router that can read and respond to labeled layer 2 datagrams
MPLS	MultiProtocol Label Switching protocol.
NAS	Network Access Server is a device providing temporary, on-demand network access to users. This access is usually point-to-point using PSTN or ISDN lines.
Oakley	A protocol in which two authenticated parties can agree on secret keys.

Glossary (cont.)

PE	Provider Edge. The router that is on the provider's side of the customer-provider interface.
PKI	Public Key Infrastructure. The mechanisms used both to allow a recipient of a signed message to trust the signature and to allow a sender to find the encryption key for a recipient.
PPP	Point-to-Point Protocol. A layer 2 (data Link) protocol that allows two peer devices to transport packets over a single link.
PPTP	Point-to-Point Tunneling Protocol. Provides a means for tunneling IP traffic in layer 2.
PPVPN	Provider-Provisioned VPN. A VPN that is managed by a service provider, not the user of the VPN.
Public Key Cryptography	A method for creating two keys (also called a *key pair*) that can be used to encrypt and decrypt messages. One of the two keys, the *public key*, is widely published, while the other key, the *private key* is kept secret. When you want to encrypt a message for a recipient, you use that recipient's public key. Only someone with the private key can decrypt the message. When you want to digitally sign a message, you use your private key. Anyone with your public key can then check the signature and verify that only you could have signed the message.
QoS	Quality of Service. There are many meanings for this term, but they generally revolve around guarantees of service levels for Internet connections. With respect to VPNs, QoS generally means the amount of throughput and/or the number of simultaneous connections that can be sustained over a connection that uses IPSec.
RAS	Remote Access Server. Used by ISPs to allow customers access to their networks.
RFC	Request For Comments. The primary mechanism used by the IETF to publish documents, including standards.
RSA	Rivest-Shamir-Adelman. The name of a cryptographic key-exchange algorithm popular in many security protocols. Also the name of the company which controls the US patent on the algorithm.
SA	Security Association. A relationship established between two or more entities to enable them to protect data they exchange. The relationship is used to negotiate characteristics of protection mechanisms, but does not include the mechanisms themselves. IPSec usage: A simplex (uni-directional) logical connection created for security purposes and implemented with either AH or ESP (but not both).
SCCRQ	Start-Control-Connection-Request. Sent by the L2TP client to establish the control connection.
SCCRP	Start-Control-Connection-Reply. Sent by the L2TP server to reply to the Start-Control-Connection-Request message.
SCCRN	Start-Control-Connection-Connected. Sent in reply to a Start-Control-Connection-Reply message to indicate that the tunnel establishment was successful.
SoftPhone	The term SoftPhone refers to an IP extension, a dedicated LAN attached H323 compliant device, or a software program running on a multi-media PC. An example of a H323 software phone is MS-Netmeeting (3.x).
SSL	Secure Sockets Layer. A protocol for encryption and authentication of Internet connections. See TLS.
TCP/IP	Transmission Control Protocol/Internet Protocol. A networking protocol that provides communication across inter-connected networks, between computers with diverse hardware architectures and various operating systems.
TLS	Transport Layer Security. The standardized version of SSL.
UDP	User Datagram Protocol. Part of the TCP/IP protocol suite. UDP provides for exchange of datagrams with acknowledgements or guaranteed delivery. UDP is a transport layer protocol.
VPN	A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.
VPNC	Virtual Private Network Consortium. The trade association for manufacturers and providers in the VPN market.

Avaya
Sterling Court
15 - 21 Mundells
Welwyn Garden City
Hertfordshire
AL7 1LZ
England

Tel: +44 (0) 1707 392200
Fax: +44 (0) 1707 376933

Email: contact@avaya.com
Web: http://www.avaya.com.

IP Office Virtual Private Networking
Issue 3b (22nd June 2005)