Columbitech Wireless VPN™

Technical Description

Updated 2007-10-22

DuraTech USA Inc.
A Certified 8(a), SDB, DBE, SBE, MBE, WBE firm.
Phone: (714) 898-2171 Fax: 866-704-9132
Email: sales@DuraTechUSA.com www.DuraTechUSA.com

Abstract

Not to long ago the workplace was an office and only an office. Mobility has given today's workforce a new level of efficiency in production, logistics and customer relations.

Wireless technology is finally getting mature enough to be useful in corporate data applications. The reason for this is, among other things, the public high-speed wireless networks emerging in metropolitan areas, enabling traveling employees to access corporate data just as easily as if they were at the office. This, in combination with the commercial rollout of public GPRS and 3G services and the new high-capacity wireless devices, is a milestone for corporate wireless data applications.

However, large enterprise and service providers have until today been unable to successfully launch their corporate wireless services. One major showstopper has undoubtedly been the lack of security. Communicating sensitive data in a public wireless environment requires a security framework that is strong enough to resist any unauthorized access to the data or to the corporate network, while still being convenient for end users. The lack of convenience combined with relatively poor wireless performance is another issue that prevents a successful commercial rollout. There is clearly a demand for new wireless solutions.

This white paper presents Columbitech's Wireless VPN solution, a system that enables secure and convenient remote access to the corporate network. The architecture is developed for use in a wireless network environment where network resources are limited and connections are unstable. The solution has been designed to overcome the three main obstacles in wireless communications, namely the lack of security, the poor wireless performance, and the low level of transparency to the end user.

Contents

Introduction

Columbitech Wireless VPN™ is a client/server based software architecture for secure remote access to corporate data. The architecture enables mobile users to be continuously and securely connected to their corporate intranet, using any public network available. The Wireless VPN lets the user work normally, as if connected directly to the office LAN. Data is transferred within an encrypted and authenticated WTLS session, over a public network, to the VPN server residing on the corporate network. Columbitech Wireless VPN™ is network-agnostic and transparent to the applications. This means that a remote user can use any network provider to securely access any enterprise service or application.

As the name suggests, Columbitech Wireless VPN™ is a VPN architecture developed for use in a wireless environment. Various mechanisms are used to create a high-quality wireline-like experience over unreliable, low-bandwidth wireless networks. Columbitech's solution protects the secure session in case the wireless network fails. Automatic connection re-establishment mechanisms make sure that the user automatically gets logged back on to the corporate network as soon as any access network is available. The VPN session may be established over one type of network and later resumed over another, depending on current network availability.

Columbitech Wireless VPN™ is not just another VPN solution. By using standards and protocols especially adopted for wireless communication, Columbitech has been able to create a VPN with exceptional reliability. The VPN architecture is implemented as a middleware and can be seen as a wireless communications platform, not only providing a very high level of security, but also providing high performance through efficient adaptive compression and various protocol optimization techniques. Furthermore, the peculiarities of wireless data communication are made transparent by providing the end user with a robust, convenient and hassle-free single sign-on environment.

Columbitech Wireless VPN™ is designed for seamless interoperability with existing corporate solutions. Columbitech Wireless VPN™ can make use of existing services for authentication, authorization and network management. A company that is already using another IP VPN solution may deploy Columbitech's wireless VPN as a wireless extension and still benefit from their existing IP VPN for wireline services. If a company is not currently operating an IP VPN, the Columbitech Wireless VPN™ solution is able to provide traditional wireline VPN services in addition to the wireless functionality. Many of the wireless optimizations implemented in the Columbitech architecture are just as applicable to wireline environments.

Technology Overview

VPN products can roughly be divided into three groups: Site-to-site VPNs, fixed client-to-site VPNs and mobile client-to-site VPNs. Site-to-site VPNs are based on IPSec and are used to securely connect different branch offices together over insecure networks. Fixed client-to-site VPNs are used to connect remote users to a corporate network, preferably by connecting a VPN client to the corporate firewall. Fixed VPNs do not have support for mobility; if the user moves to a different network provider or to a different subnet, the VPN session will terminate. Mobile client-to-site VPNs include functions for enabling a user to move between different networks and service providers without losing the VPN session. A user is thus able to change access network without having to re-logon to the VPN server and also without having to restart any application.

There are numerous ways to implement a VPN. The following paragraphs describe three different approaches as well as the pros and cons for each approach

Layer 2 Solutions

Layer 2 solutions operate beneath the IP stack to secure the link layer. Examples of such technologies are PPTP [1] and L2TP [2]. Although Layer 2 solutions provide a high level of transparency to the applications, they suffer from not being network transparent; a PPTP session cannot be carried over a packet based network, such as the Internet. Instead the remote user has to dial up to a secure location inside the corporate premises, thus making the remote access service expensive and inefficient. This problem is solved by the L2TP protocol; PPP frames are tunnelled inside an L2TP tunnel to a remote access server. The L2TP tunnel is carried on top of UDP/IP and can thus traverse standard packet based networks.

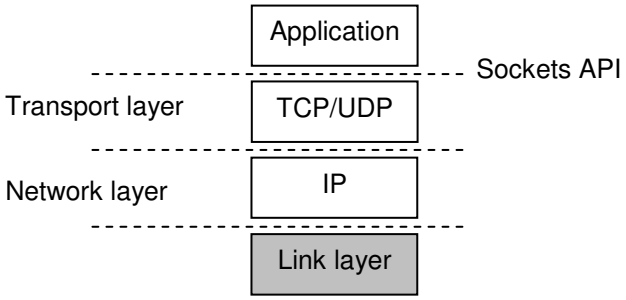

Figure 1: *Protocol stack for a link layer solution*

However, L2TP is suffering heavily from the tunnelling overhead as can be seen in Figure 2. The original IP packet, including IP header and transport header, is transported inside an IPSec tunnel, which in turn is carried within PPP and L2TP.

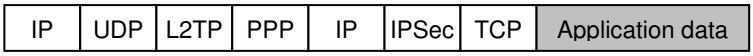

Figure 2: *Data transport using a L2TP based VPN (TCP based appl.)*

The PPTP and L2TP protocols do not have inherent support for mobility. Solutions based on these technologies could however implement Mobile IP or any other IP based mobility protocol to achieve mobile VPN functionality.

IP Level Solutions

The obvious IP level approach is to implement IPSec [3] along with Mobile IP [4]. The strategy is to provide transparency to the transport layer by hiding the change of IP address, allowing transport level connections to survive roaming between different networks.

IP level solutions operate on the network layer, thus leaving the responsibility for flow control and session recovery to the transport protocol used, normally TCP. However, both IPSec and TCP are protocols initially developed for fixed networks characterized by high bandwidth, low delay and jitter and where data loss mainly occurs due to congestion. Wireless networks present a totally different environment; bandwidth is limited, connections are unstable, delay varies and data loss occurs due to intermittent connectivity and bit error. Applying wireline technology to such an environment will undoubtedly lead to sub-optimized performance.

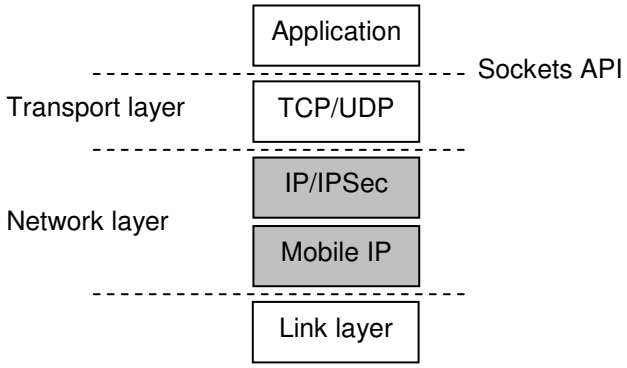

Figure 3: *Protocol stack for an IPSec/Mobile IP solution*

Mobile IP

Mobile IP tries to hide movements to the upper layers, i.e. IP, UDP and TCP, by maintaining two IP addresses on the client; one address that reflects the client's current point of attachment and one address belonging to the home domain, that remains constant during the whole session.

The Mobile IP architecture defines three network entities; *Mobile IP Client, Home Agent,* and *Foreign Agent*. The Home Agent resides on the corporate network and is responsible for intercepting data on behalf of the Mobile IP client. The Home Agent adds a new IP header to the original IP datagram and forwards it to the client using normal IP routing. Two different modes can be used to forward the data to the client: *Foreign Agent mode* and *co-located mode*. In Foreign Agent mode, the Home Agent tunnels the data to a Foreign Agent residing on the visited network. The Foreign Agent removes the outer IP header and forwards the original data to the client. Regular IP forwarding cannot be used to route data between the Foreign Agent and the Mobile IP client since the destination IP address does not belong to the visited domain. Packets will instead be routed using link layer forwarding mechanisms, the Foreign Agent must therefore reside on the same subnet as the Mobile IP clients. Thus, Mobile IP in Foreign Agent

mode introduces scalability issues; a large number of Foreign Agents is required as well as a large number of security associations between Home Agents and Foreign Agents.

Therefore, most Mobile IP implementations use co-located forwarding as the normal mode of operation. In co-located mode, the Home Agent tunnels the data all the way to the client without using a Foreign Agent. The Mobile IP client removes the outer IP header and passes the original datagram to the IP layer. This technique solves the scalability issue related to the use of Foreign Agents, but then another problem presents itself: The Mobile IP tunnelling adds extra overhead to the communication over the wireless link, where bandwidth is already scarce.

IPSec

IPSec has become the de facto standard for IP VPNs. IPSec operates on the network layer and its security mechanisms are tightly connected to the IP address of the connecting host, an unfortunate characteristic that prevents smooth operation in a fragmented network environment with different networks hosted by different providers.

One of the most serious problems with IPSec is that the protocol does not support network address translation, a technology that virtually every enterprise and service provider use in order to increase its public address space. NAT servers expect transport level information rather than IPSec headers following the IP header. The common solution is to append a transport protocol header between the IP header and the IPSec header on each data packet. One problem has been solved, unfortunately by introducing another: The extra transport protocol header introduces additional overhead to the data transmission. Using IPSec together with Mobile IP will lead to a substantial performance degradation related to extensive protocol overhead.

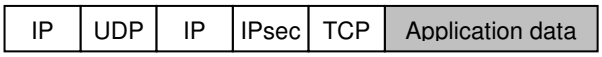

Figure 4: *Data transport for an IPSec/Mobile IP based VPN (TCP based appl.)*

Another serious shortcoming of IPSec is its lack of session resume functionality. In a fixed network environment, connections are rarely dropped , which is why session resume was never an issue when designing the protocol. A wireless connection on the other hand, presents a much higher demand on the protocols used. Wireless networks are unstable and connections will be dropped. Without session resume, the user will have to log on again every time a connection is lost, including heavyweight functions, such as key exchange and user authentication.

Session Level Solutions

The third approach to implementing a mobile VPN is to use protocols implemented at the session layer. It is important to distinguish solutions implemented at the session level from application layer solutions. The session layer is the 5th layer in the OSI model, while applications reside on layer 7. Application layer solutions do often use a standard web or WAP browser for accessing internal information, such as email or internal web content, through a standard SSL session. The upside of this approach is that a user does not have to install VPN client software on the device. The downside is that an application level solution is not transparent to the application layer, thus not allowing transparent access to internal applications and services.

A session level approach however, is implemented below the application layer, as depicted in Figure 5. Any standard application can be used to access internal information. By implementing the functionality below the application layer, the VPN connection will remain transparent to the users, the corresponding nodes, and their applications.

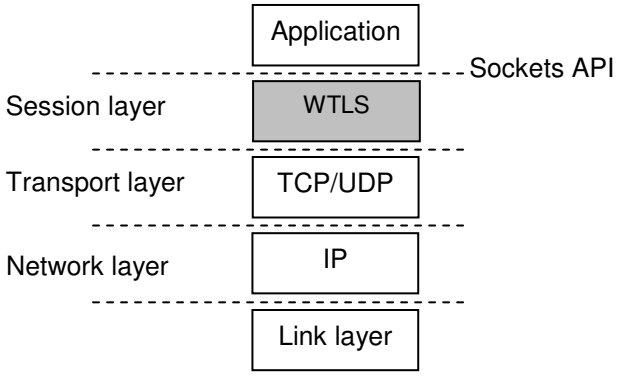

Figure 5: Protocol stack for Columbitech's session level solution

The main difference between a session based VPN and an IP based VPN is that a session based solution is implemented above the transport layer. As stated before, TCP is not designed for networks with large variations in bandwidth and delay. TCP's flow control and recovery mechanisms fail to respond to the rapid change in link quality and its congestion control algorithm leads to sub-optimized link utilization. Roaming from a high bandwidth network to a low bandwidth network, i.e. from wireless LAN to GPRS, will most likely trigger multiple TCP timeouts from which the TCP connection may be unable to recover.

Since most applications are using TCP for data transport, TCP cannot simply be replaced by a different protocol without a major impact on the Internet community. The only viable solution would be to hide the shortcomings of TCP to the application layer by implementing recovery mechanisms at the session level. The session based approach allows for implementations of transport proxy mechanisms at the VPN server for maintaining active application connections if a user experiences momentary network problems, e.g. due to lack of radio coverage or due to TCP breakdown.

Furthermore, a session layer approach can take advantage of the application data characteristics for data reduction. Session level compression can be made extremely efficient since the compression algorithm can be applied on large streams of data. IP layer compression however, can only be applied on a per packet basis and can thus not take advantage of recurrent patterns in the data stream.

Traditional interoperability issues related to NAT and firewall traversal with IP level based security do not apply to a session-based architecture. Since the mobility protocol is based on a session ID instead of an IP address, standard NAT and NAPT traversal is supported.

System Overview

Columbitech Wireless VPN™ architecture consists of a client software component, the Columbitech Wireless VPN™ Client, and one or more server components. Columbitech Wireless VPN™ Server is a server software component residing inside the corporate network. Columbitech Wireless VPN™ Server acts as the VPN terminator; it handles encryption, authentication, compression and session management. A second server component, Columbitech Gatekeeper, may be installed in the corporate demilitarized zone (DMZ) to further increase security, to simplify firewall configuration and to enable load balancing. The Gatekeeper is not a mandatory component in the Wireless VPN architecture. However, to meet strict corporate security policies, the Gatekeeper component may be required.

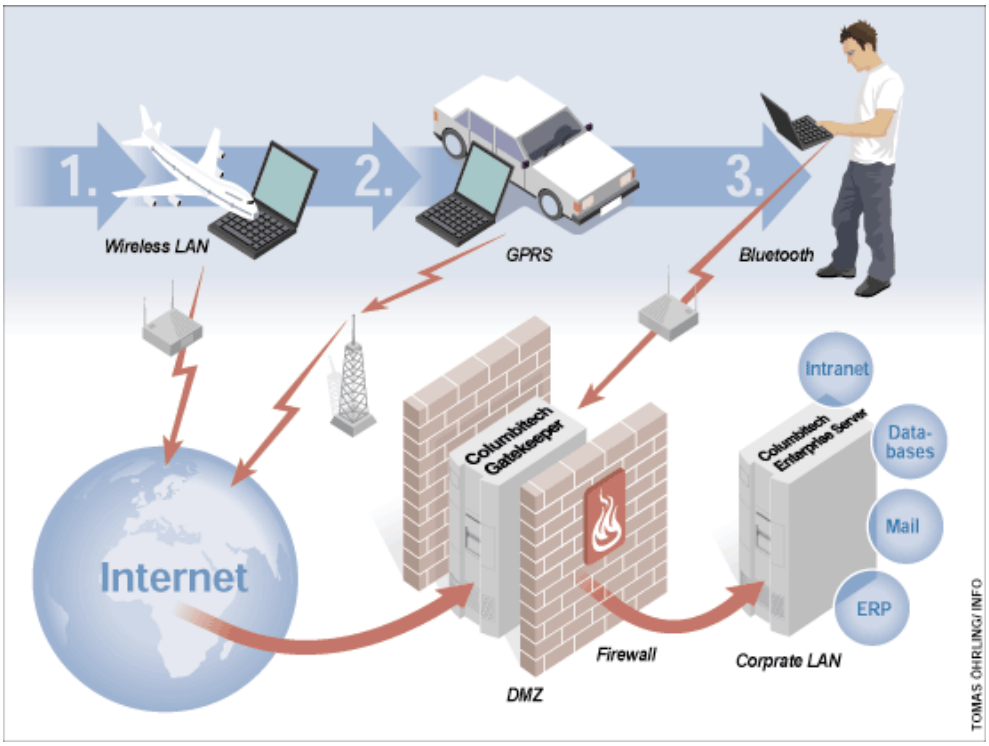

Figure 6: *Imagine a salesman at an airport, connected to his corporate LAN through a hot spot WLAN access point (1). When leaving the airport, the connection will be lost and the VPN client will switch over to a GPRS network (2), making it possible to remain connected, without any new logon procedures. When visiting the customer, the salesman could connect to his corporate server using the customer's Bluetooth network (3). Each network switch is performed automatically, totally transparent to the user.*

Columbitech's Wireless VPN solution is implemented at the session layer, totally transparent to the applications as well as to the underlying network infrastructure. Transparency to network operator or service provider is achieved since no software or hardware needs to be installed

outside the corporate domain. However, the wireless VPN architecture includes components that may be installed by an operator or service provider to enable outsourcing of the corporate wireless data services.

Columbitech Wireless VPN™ Server

Columbitech Wireless VPN™ Server consists of several software modules that can be installed either on the same machine or on separate machines. The modules are described below:

Columbitech Wireless VPN™ Server

Columbitech Wireless VPN™ Server is the core component responsible for handling the VPN connections. Columbitech Wireless VPN™ Server is installed on a server residing on the corporate network inside the firewall, as depicted in Figure 7. Wireless VPN Clients may connect directly to Columbitech Wireless VPN™ Server or via a Gatekeeper located outside the firewall, in the DMZ. Regardless of which, the secure tunnel is always terminated by Columbitech Wireless VPN™ Server. No data will ever be revealed outside the firewall.

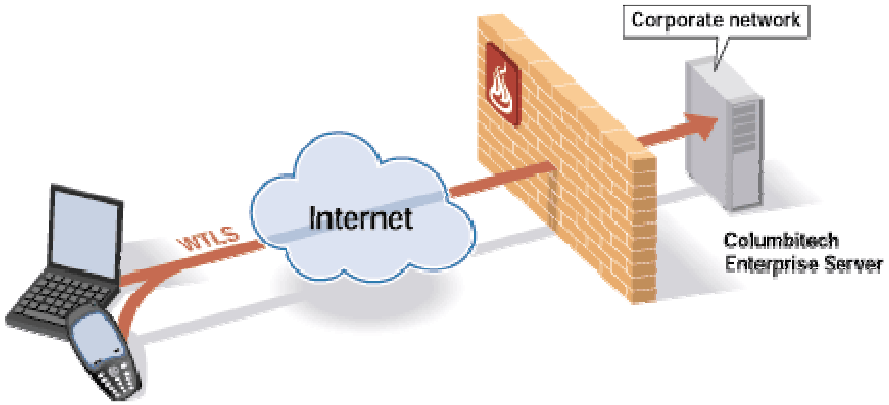

Figure 7: Columbitech Wireless VPN™ Server

When a client initiates a VPN session, the user is required to authenticate to Columbitech Wireless VPN™ Server. Authentication can be done by using one or a combination of the following authentication mechanisms:

- Client certificate (X.509 and WTLS formats supported)
- Windows username/password.
- RADIUS (challenge/response or username/password)
- RSA SecurID one-time-password
- Smartcard / CAT card
- Biometrics

When the user has been properly authenticated, the WVPN Server enables the VPN session and assigns a corporate domain IP address to the client. Data to a Wireless VPN client is intercepted by Columbitech Wireless VPN™ Server for compression and encryption before it is sent to the client. For any corresponding host or node, the VPN client appears to be connected directly to the corporate network, the fact that the client may be remotely connected to the WVPN Server is totally transparent.

Administrative Tool

The Columbitech Wireless VPN™ Server Tool is implemented as an MMC (Microsoft Management Console) snap-in. The management console is using Com+ objects for communication with the WVPN Server. This enables the system administrator to install the

management console on a different machine for remotely managing the WVPN Server. It is possible to connect to multiple WVPN Servers from the same management console, a useful feature in large installations with distributed servers. As an option, the communication between the management consol and the WVPN Server may be encrypted and authenticated.

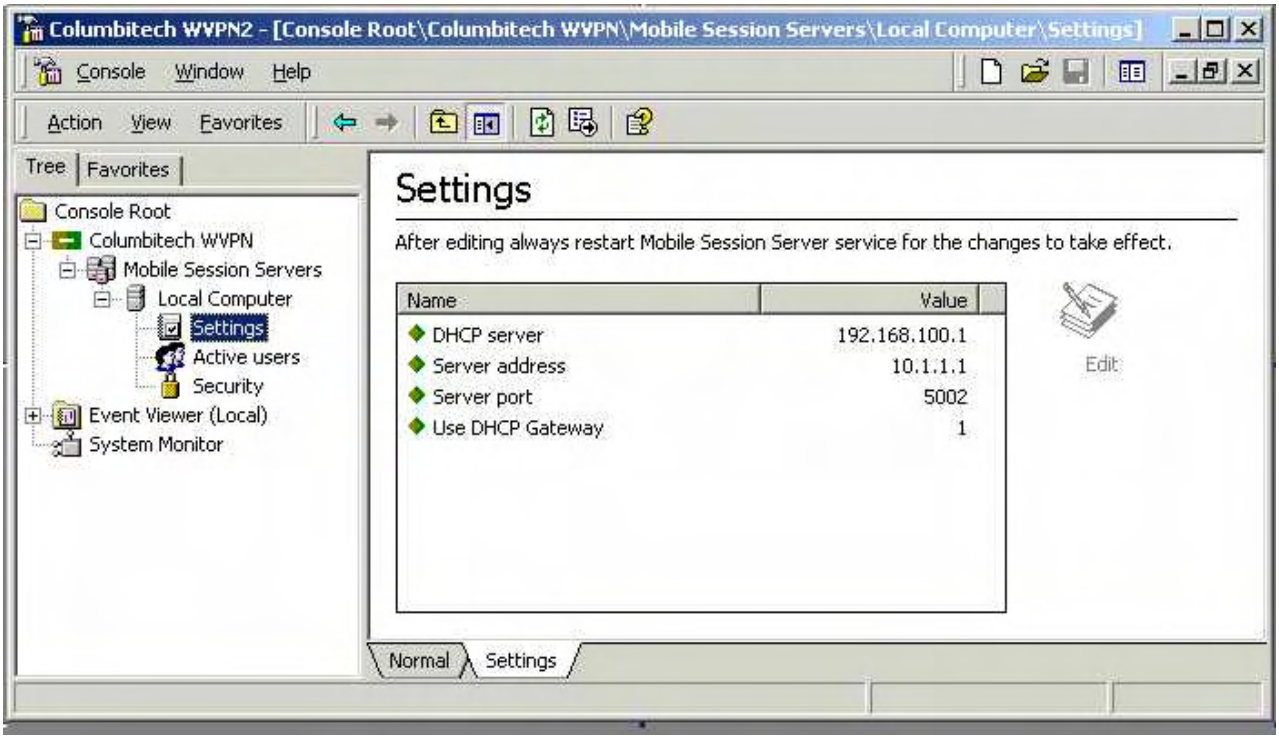

Figure 8: Columbitech Wireless VPN™ Server management consol

Columbitech Certificate Manager

Included in Columbitech Wireless VPN™ Server is an application for creating and managing certificates. An enterprise is thus not dependent on an external PKI solution or provider for enforcing certificate authentication in Columbitech Wireless VPN™ with the Certificate Manager, a system administrator can easily create CA certificates, client certificates and server certificates according to the x.509 or the WTLS standard. Certificate revocation lists can be imported or created in order to revoke invalid certificates.

For large installations, the Columbitech Wireless PKI Portal can be used to automatically create a large number of client certificates. The PKI portal connects to the corporate Windows domain controller and creates a client certificate for each domain user, or for a group of users, as configured in the Certificate Manager. Furthermore, the PKI portal supports automatic distribution and installation of client certificates on the client devices.

Columbitech Gatekeeper

Columbitech Gatekeeper is an additional server component designed to be installed on the corporate DMZ. The main purposes for deploying the Gatekeeper is to:

- Increase the security through strong authentication outside the firewall.
- Simplify firewall configuration.
- Prevent exposure of the WVPN Server on the Internet.
- Enable load balancing and failover.

If the system is configured to use a Gatekeeper, the WVPN Server connects to the Gatekeeper when the server starts. The connection is established from inside the corporate network to the DMZ, something most corporate security policies allow. The VPN clients connect to the Gatekeeper, they do not connect directly to the WVPN Server. The Gatekeeper connection is totally transparent: The VPN client does not explicitly have to be configured to use the Gatekeeper, this is taken care of by the WVPN protocol.

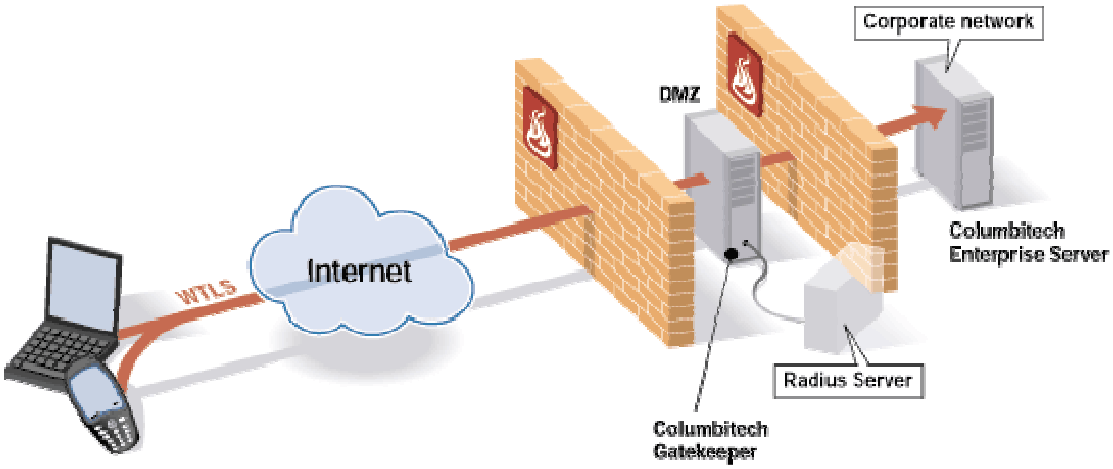

Figure 9: *Gatekeeper deployment*

When a WVPN Client initiates a handshake, the Gatekeeper authenticates the user before allowing the connecting client to continue the handshake with the WVPN Server. Data from WVPN Client is intercepted by the Gatekeeper and multiplexed over the TCP session that was initially created by the WVPN Server. Thus the firewall does not have to be opened for incoming TCP connections. The Gatekeeper supports the following authentication mechanisms:

- Client certificate (x.509 or WTLS format)
- RSA SecurID
- RADIUS (challenge/response or username/password)

By deploying Columbitech Gatekeeper, strong user authentication can be enforced before any traffic is allowed inside the firewall, still without breaking the end-to-end encryption between the VPN client and the VPN server.

Columbitech Gatekeeper can also be used to seamlessly and dynamically scale up the system, while at the same time provide the WVPN Server with load balancing and failover. Several WVPN Server can be grouped into one logical server by using a server group identifier. Large enterprises with different branch offices or isolated departments may deploy a Gatekeeper inside their corporate DMZ and have one WVPN Server group per branch office or department connecting to the same Gatekeeper.

The Gatekeeper is responsible for distributing WVPN Clients evenly on the available WVPN Servers within one server group. If one WVPN Server is going down, only the users connected to that particular WVPN Server would be disconnected. When the WVPN Client reconnects, the Gatekeeper will allocate another WVPN Client from the server group to the client.

Administrative Tool

Using the Gatekeeper Administrative Tool, a system administrator can configure the Gatekeeper service and monitor connected WVPN Servers and users. The functionality is very similar to the WVPN Server Administrative Tool.

Columbitech Wireless VPN™ Client

The Columbitech Wireless VPN™ Client is implemented as a virtual network interface. When the client connects to the WVPN Server, the virtual interface gets an IP address allocated from the corporate domain. The WVPN Client reconfigures the routing tables to force all applications to send data through the virtual interface. Functions at the session layer compress and encrypt the data before it is passed down to the virtual interface for address translation. The data is then multiplexed over one of the physical network connections for further transport to the WVPN Server.

The WVPN Client runs as a Windows service and uses the following components to interface the user:

Client Monitor

The client monitor is an icon on the system tray menu. The monitor displays the current connection status, available connections, and the currently used bearer. In expanded mode, the WVPN Client Monitor can be used to change connection state, profile and bearer.

Figure 10: *Wireless VPN Client Monitor (expanded mode)*

WVPN Client Control Panel

The control panel is used to change the settings of WVPN Client, including connection settings, connection preferences and user profiles. Administrative privileges are required to change the WVPN Client settings or to allow for the personal firewall to be switched off. A normal user can thus not bypass the VPN by disabling the Wireless VPN client or by changing the security configuration.

GINA Module

The Columbitech GINA (Graphical Identification and Authentication) module is a kernel module for integrating the WVPN Client login with the standard Windows login mechanism. When a VPN user logs on to the computer, the Columbitech GINA intercepts the user's credentials and the user gets transparently logged on to the WVPN Server before the Microsoft GINA logs on to the windows domain.

Client API

Columbitech Wireless VPN™ Client includes a software API with which an application developer can integrate the wireless VPN functionality into a user application in order to make the Wireless VPN functionality transparent to the end user. By using the client API, an application can connect and disconnect to the WVPN Server, change profile and trigger network roaming. The application can also retrieve status information regarding data rate and the type of bearer through the API. This feature opens up new possibilities for creating adaptive applications where the behaviour and information is adapted according to the currently used bearer type.

Functional Description

Security

Many wireless network technologies are using various mechanisms to prevent third parties to eavesdrop and tamper with transmitted data. Examples of such mechanisms are frequency hopping and the WEP link layer encryption system. Although those techniques make eavesdropping more complicated, they are not to be seen as secure solutions. With the appropriate equipment and knowledge it is fully possible to listen in on traffic transmitted over e.g. GSM, DECT, 802.11 W-LAN and Bluetooth. Also, the data is protected only when transmitted over the wireless link. Most wireless network providers are using the Internet to transport data from its backbone to the end customers, thus the data will be transmitted in clear. There is obviously a need for end-to-end secure VPN solutions.

Not only is it important to make the data transmissions impossible to eavesdrop on, it is equally important to protect the corporate network from unauthorized access and a good VPN must be able to handle both requirements. Transmitted data is effectively hidden by the use of encryption and the corporate network is protected by enforcing strong user authentication. Columbitech Wireless VPN™ implements the latest standards and algorithms for securing the transmitted data, the corporate network and the client device, as will be described in the following paragraphs.

Columbitech Wireless VPN™ is FIPS 140-2 certified and is in the process of becoming Common Criteria evaluated.

Securing Traffic

To secure the transmitted data, a virtual encrypted tunnel is created between the WVPN Client and the WVPN Server. Columbitech Wireless VPN™ is using the WTLS [5] standard to encrypt, authenticate and validate the transmitted data. WTLS is a wireless implementation of TLS, which is an enhanced version of SSL 3.0. The reason for using WTLS instead of IPSec is mainly that IPSec suffers heavily from sub-optimized performance when applied over wireless, low-bandwidth networks.

The WTLS framework defines a set of protocols and algorithms for encryption, signing and hashing; Columbitech Wireless VPN™ uses DES (56 bit), 3DES (112 bit) and AES (up to 256 bit) for the symmetric encryption of the payload data. RSA (up to 15360 bit) is used for asymmetric encryption during the initial handshake, and MD5 (128 bit) or SHA (up to 512 bit) is used for validating the data integrity. Columbitech Wireless VPN™ can be configured to use a combination of the algorithms mentioned above to achieve a desired level of security.

Securing Network Resources

To protect the corporate network from unauthorized access, Columbitech Wireless VPN™ enforces strong authentication mechanisms. User authentication may be performed by the WVPN Server inside the corporate network, by the Gatekeeper residing outside the firewall, or

by both the WVPN Server and the Gatekeeper. Typically, a corporate security policy might state that no unauthorized data is allowed inside the corporate network. In such a scenario, the Gatekeeper could be configured to enforce client certificate authentication or one-time-password authentication before the VPN session is handed over to the WVPN Server. The VPN handshake will then be continued by the WVPN Server, possibly asking the user for a Windows NT or RADIUS password, a client certificate, or a one-time-password.

Columbitech Wireless VPN™ has been designed to interoperate with the existing corporate authentication mechanisms. With the Columbitech GINA module, a user will be transparently logged on to the WVPN Server as soon as he or she logs on to the computer. Furthermore, a system administrator does not have to maintain two different sets of user accounts for each user; existing user databases may be used for Wireless VPN authentication. Columbitech Wireless VPN™ Server and Columbitech Gatekeeper can be configured to utilize any standard RADIUS server, Windows Active Directory server, or RSA ACE server. Columbitech Wireless VPN™ has full PKI support to ensure for maximum scalability and to provide for reliable authentication of servers and clients. Certificates are easily created, maintained and distributed with the included Wireless PKI Portal and the certificate management application.

To further secure the network side, Columbitech Wireless VPN™ Server includes a firewall to enforce packet filtering and inspection. Enabling strong user authentication in combination with firewall protection at the network edge is the most effective defense against intrusion. In most organizations, access to network resources is based on user and group policies. To enforce group based access control, Columbitech Wireless VPN™ can be configured to allocate IP addresses that belong to different IP subnets, depending on which user groups the connecting user belongs to. Access can then be controlled by a firewall or policy router. The Enterprise Server can also be configured to allocate different IP addresses depending on if the user connects directly to the Enterprise Server or via a Columbitech Gatekeeper. This allows the system administrator to set up different access policies depending on whether the user connects remotely or directly from the office.

Securing Clients

Employees often bring their laptops home and connect them to the Internet through their home broadband connections. As soon as the computer is connected to the Internet it is exposed to attacks. The corporate firewall is no longer there to protect the computer from viruses, trojan horses and other exploits. Later, when the computer connects to the internal network, the malicious code could easily spread to the whole network and cause substantial damage.

Columbitech Wireless VPN™ Client ensures that all data is processed by the virtual VPN interface. The WVPN Client software protects every network interface on the computer, including dial-up connections, by applying IP filters that only accept properly encrypted data that has been sent through the VPN tunnel. This functionality is part of Columbitech personal firewall and the main goal is to protect the computer from malicious attacks when exposed to public networks as well as to prevent client applications from bypassing the VPN connection.

Managing devices is perhaps one of the biggest challenges with a mobile workforce. It is important that the mobile devices run the latest security patches and other appropriate security software, as specified by the corporate IT policy. To make sure that the connecting device does not compose a security threat, Columbitech Wireless VPN™ contains built-in Network Admission Control (NAC). This means that the client can check the integrity of the client computer before allowing it to connect to the corporate network. When the Wireless VPN Client requests a connection, the Columbitech Wireless VPN™ Server sends an encrypted script, or program, that executes on the client computer. The script can verify that security patches, anti virus programs, personal firewalls and other security software is running and up-to-date. Depending on the return value of the script, the client is accepted by the server,

rejected by the server, or as a third option, placed in quarantine. When placed in quarantine, the client gets limited access to the network, just enough to download e.g. virus definition updates or OS patches.

Wireless PKI

In order to establish an encrypted WTLS tunnel, a shared secret key must be agreed upon by both communicating peers. To exchange the secret key, asymmetric encryption is used. In asymmetric encryption, each party has a key pair consisting of one *public key* and one *private key*. The public key is publicly available to anyone, while the private key remains private. A message encrypted with the public key can only be decrypted using the private key (and *not* using the key that encrypted the message, as is the case in symmetric cryptography). Asymmetric encryption is extremely processor heavy and thus not feasible for encrypting large amounts of data. Instead, symmetric encryption is used for the actual data transfer and asymmetrical encryption is only used to exchange the shared secret key used for the session.

Public Key Infrastructure (PKI) is the infrastructure for managing a trusted matching between public keys and their owners. One of the fundamental components of PKI is the digital certificate. A digital certificate has many similarities with a passport. It contains information about its owner, or subject, and about the entity that issued it. The public key of the subject is also included, as well as a *digital signature* that proves the authenticity of the certificate.

To handle certificates, Columbitech Wireless VPN™ includes a Certificate Manager with which a system administrator can create and manage digital certificates, i.e. it lets you operate a simple certificate authority. A wireless PKI portal included in Columbitech Wireless VPN™ Server allows easy certificate management in large installations. The PKI portal connects to the Windows user account database and automatically creates and distributes client certificates for all users in the corporate domain. Columbitech Wireless VPN™ is fully x.509 compliant, any public certificate authority can be used to create and manage certificates for the Columbitech Wireless VPN™ architecture.

Convenience

Automatic Session Resume

Intermittent connectivity is unfortunately a characteristic closely related to wireless communication. Connections go up and down due to bad radio coverage, shortage of radio resources or due to interference. One of the design goals for the WTLS standard was to address these issues by implementing mechanisms for fast session re-establishment after a network failure. The result, called *Session Resume*, allows for a very fast VPN reconnection without any user interaction. The user does not have to go through any extra logon or authentication procedures. As soon as the radio link is re-established, the client and the server are authenticated and the WTLS session is resumed from where it was suspended. This technique of resuming an old session is sometimes referred to as a lightweight handshake. It is done in a background process very efficiently.

The Session Resume functionality in Columbitech Wireless VPN™ also allows for a seamless and automatic activation of the VPN session when a device resumes from hibernation. This is a very important feature, especially when using mobile devices with limited battery power. If the device cannot enter hibernation, the battery power on a standard PDA will not last longer than a couple of hours. With standard VPN solutions, resuming from hibernation often means that the VPN Session has to be re-established and the user has to log on again to the VPN server.

Data Transaction Recovery

Even though the secure session is re-established automatically, (this may also include automatic dial up of a dial-up connection), it is very frustrating to lose a network connection, especially if data was being transferred. In order to make life easy for the mobile user, *Columbitech Wireless VPN*™ implements a function called *Transaction Recovery*. Transaction Recovery allows a data transfer to pick up from where it was interrupted. The user does not have to restart the transfer, nor the application. All applications will survive a lost connection and all interrupted data transfers will automatically continue from where they were interrupted, as soon as data can be transferred again. Retransmission mechanisms at the session layer make sure that lost data segments get retransmitted before the data transfer resumes. In the eyes of an application, this short re-establishment period will just be viewed as a period of lower-than-usual bandwidth.

Seamless Network Roaming

Seamless network roaming is a delicate task and a great technical challenge. With seamless network roaming we mean the general concept of moving between different networks, possibly of different types, without loosing any open connections. Columbitech Wireless VPN™ uses the session resume functionality implemented in WTLS to create a seamless, always-connected experience for the mobile user. During network roaming, the secure session is instantly resumed over the new network and the flow control and transaction resume mechanisms guarantee that no data is lost in the process. The seamless network roaming functionality is totally transparent to the application layer, i.e., the applications believe they are still using the same connection.

Since the roaming functionality is implemented at the session level, the client applications are not dependent on TCP for retransmissions and flow control during the handover. This is particularly important when roaming from a fast network, e.g. wireless LAN or LAN, to a slow network, e.g. GPRS, GSM or CDPD, since TCP will most likely fail to adapt to the drastic change of bandwidth and delay.

Single Sign-On

The Wireless VPN logon can be made transparent to the user. By integrating the VPN logon into the standard Windows domain logon, the Wireless VPN user gets transparently logged on to the WVPN Server when he or she logs on to the computer. Standard Windows clients are supported as well as Novell Netware clients.

Internet service providers and wireless hotspot providers often require the user to logon before gaining Internet access. The most common way to authenticate a user is to redirect the user's Internet browser to the ISP's authentication server. The users must then enter a username and password before they can be allowed to enter external networks. By defining a network access policy in the Wireless VPN Client, the hotspot login can be performed entirely in the background by the WVPN Client, without any user interaction. A user is thus able to logon to the access network, the WVPN Server, and the corporate Windows domain with one single login.

Performance

Since radio frequencies are a limited natural resource, wireless capacity will always be limited. Therefore, wireless networks will always be significantly slower than wired networks. This motivates the efforts for implementing wireless optimizations.

Adaptive Data Compression

Compression is probably the most widely used optimization technique for data reduction. A characteristic that all types of compression algorithms have in common is that they take advantage of recurring structures or patterns in the data in order to compress it. In contrast, good encryption is designed to distort and remove patterns. Therefore, if both compression and encryption is applied to a data stream, it is vital to compress the data *before* encrypting it, in order for the compression to be efficient. Columbitech Wireless VPN™ implements data compression at the session layer, before the data is encrypted. This way, the compression algorithm may be applied on large blocks of data, ensuring very high compression ratios. IP level compression on the other hand is applied on individual IP datagrams. Therefore, the compression algorithm cannot exploit recurrences in the data flow, since the datagrams are compressed separately.

When using thin clients, such as handheld devices, over fast networks such as wireless LAN or fixed networks, the device's memory and CPU load may be the critical bottleneck, not the bandwidth. Therefore, compression is applied on a per connection basis. When roaming between fast and slow bearers, the Wireless VPN Client can be configured to dynamically switch the compression on and off, according to the current user profile.

Adaptive Encryption (Trusted Zones)

Trusted Zone is the term used for any network where the client can access the WVPN Server directly without going through a Gatekeeper. This is typically the local wired network. It is possible to configure the WVPN Server to allow clients to bypass the VPN if connecting from a Trusted Zone to further increase performance. The user is still subject to full authentication and the client computer will be subject to integrity check prior to bypassing the VPN. The VPN client is still running to detect change of network, from a trusted to a non trusted network.

Transmission Protocol Optimization

Other schemes for data reduction are also applied; Optimizations at the transport level, such as TCP connection multiplexing, prevent flooding the wireless link with redundant TCP retransmissions during handover. In short, the available bandwidth will be used to transport actual user data instead of redundant TCP retransmissions. If the entire link capacity is utilized for retransmissions, TCP will eventually break down due to lack of new user data on the link. However, if all data were multiplexed over one TCP Session, there would be plenty of room for new data to reach the receiver and the applications would be more likely to survive a bad connection.

When communicating over networks with large delays, such as most cellular wireless networks, the standard TCP flow control mechanism leads to poor link utilization. A TCP sender will not be able to fully utilize the available link bandwidth. This is caused by a combination of a large delay-bandwidth product and a badly configured TCP transmission window size. The standard setting of the TCP buffers causes the TCP connection to stall because it takes to long for the receiver's acknowledgments to return to the sender. A TCP sender is dependent on the returning acknowledgments as well as on the size of the sending window for increasing its sending rate. A small sending window and a long acknowledgment delay will undoubtedly prevent the connection from reaching the maximum link speed. To prevent this from happening, the Columbitech Wireless VPN™ Client continuously monitors the current round-trip time in order to dynamically configure the TCP buffers for optimal transmission performance.

Data Encapsulation

Columbitech Wireless VPN™ Client software uses Windows routing mechanisms for capturing, encrypting and forwarding traffic. By creating a virtual network interface card (NIC) and forcing all application data to be routed through it, the VPN client is able to encrypt all

outgoing traffic without requiring any changes to existing applications. The virtual NIC intercepts the data and sends it to the VPN client software for processing. After compression, encryption and address translation, the data is sent to the currently used physical interface. By using address translation mechanisms rather than standard tunnelling, Columbitech Wireless VPN™ is able to reduce the data overhead to less than 10%, as compared to over 25% for standard IPSec. Session based data compression and transport optimization reduces the overhead to a minimum.

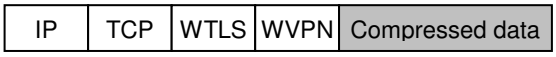

Figure 11: Data transport in Columbitech Wireless VPN™

The local termination of connection-oriented traffic makes the client resistant against temporary loss of network connections. Even though the real network connection may go up and down, the virtual NIC is always enabled and is always accepting traffic. The effect of the virtual NIC being constantly enabled is that if a network connection goes down, the locally terminated application connections will not be affected and the applications will still believe that they are online. A network failure immediately triggers the VPN client software to start reconnecting to the VPN server. The client software starts scanning for available networks and connects through the best available network, according to a defined user profile. When the client succeeds to connect to the VPN server, the WTLS session is instantly resumed and all data transfers are synchronized and continued.

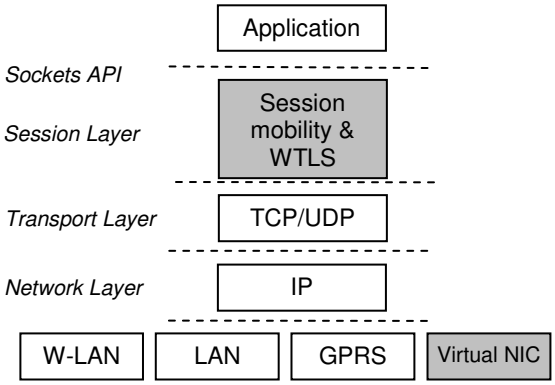

Figure 12: *The wireless VPN client protocol stack*

When a VPN client connects to the corporate network, the WVPN Server allocates an IP address from the corporate domain to the virtual VPN interface. The WVPN Server allocates the IP address by making a DHCP request to an existing DHCP server on behalf of the client. If there is no DHCP server on the network, the WVPN Server may be configured to allocate IP addresses from a specified IP address range. In practice this means that each VPN client actually has two IP addresses; one on the physical interface, allocated from the access network provider and one on the virtual interface, allocated by the corporate domain. The IP address on the physical interface will change when the client moves between different networks. The IP address on the virtual NIC will however remain constant during the whole session.

The fact that the client keeps the same IP address on the virtual interface enables seamless roaming with continuation of services. All applications and communicating peers use the corporate IP address on the virtual interface when communicating with the client. The IP address on the physical interface is hidden from the applications and is only used for transporting the data between the client and the VPN server. Inside the corporate network, the

WVPN Server translates all incoming and outgoing traffic to hide the physical interface's IP address from the applications.

A connection between a VPN client and a server application is terminated locally inside the Wireless VPN client. In order to establish the connection all the way to the application server, the client requests the WVPN Server to establish a connection on its behalf. Once the connection has been properly established, the client and the server may start forwarding traffic between each other. The client application as well as the server application is totally unaware of the WVPN Server, they believe that they are connected directly to each other.

A server application connects to a remote VPN client exactly the same way as if the client had actually been physically connected to the corporate network. The connection request is intercepted by the VPN Server and forwarded to the VPN client through the WTLS tunnel. If the client has an active application listening on the specified port, a connect message is reported back to the WVPN Server and the WVPN Server accepts the connection to the application server and data can be sent to the client. However, if the client was not listening on the specific port, the VPN client software sends a reject message to the WVPN Server, which in turn sends the appropriate ICMP message to the connecting application.

Connectionless data is handled the same way; a UDP datagram sent from a corresponding node is intercepted, encrypted and re-encapsulated by the WVPN Server for further transport to the client.

The use of split TCP connections adds robustness and flexibility to the system. If the TCP connection between the client and the WVPN Server would break down for any reason, the application connections will be maintained and the communication may continue as soon as a new physical connection is established. The split TCP connection approach also allows for further optimization of the communication between the VPN client and the WVPN Server, since the applications are actually unaware of this connection. TCP may be re-implemented or replaced by another protocol that is optimized for wireless communication.

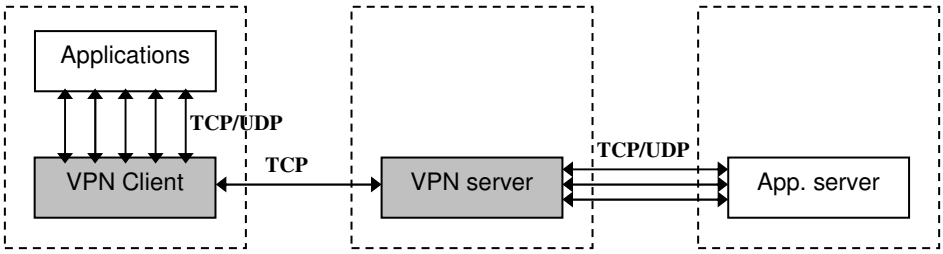

Figure 13: Data transport overview. The application connections are terminated locally on the client and the data is tunneled to the WVPN Server over one single TCP connection. The WVPN Server performs address translation and forwards the data to the destination.

However, since the TCP end-to-end semantic is violated, it is vital that the architecture implements mechanisms for end-to-end flow control and retransmission. To prevent data loss in case the connection between the VPN client and the WVPN Server would fail, the Columbitech architecture uses standard TCP mechanisms to stop the sending application from transmitting more data. In case of network failure, the WVPN Server will immediately send a TCP control message to the sender, stating that the WVPN Server has no more receiving buffers available. When the connection to the VPN client is re-established, the WVPN Server commands the TCP sender to continue transmitting. This approach is to be preferred before a solution where the VPN server buffers data in memory. Eventually the server will run out of

memory and start dropping packets. The former of these two TCP flow control mechanisms is implemented in both the WVPN Server, the Gatekeeper and in the Wireless VPN client.

To avoid loosing packets that were being transmitted when the connection broke down, the WVPN Server stores the few last transmitted packets for each client connection. When the VPN client reconnects, the WVPN Server and the VPN client synchronize their data flows and if any packets were lost in transit, they are retransmitted.

Scalability

Columbitech Wireless VPN™ includes support for server load balancing and fail over. Expensive third-party solutions are thus not required to provide server redundancy. By using Columbitech Gatekeeper, several WVPN Servers can be clustered into one WVPN Server group, as depicted in Figure 14. When a user connects to the corporate network, the Wireless VPN Client will establish a connection to the Gatekeeper. After initial user authentication, the Gatekeeper will hand over the client to one of the WVPN Servers belonging to the server group specified by the client. It is possible to cluster as many as 15 WVPN Servers in one server group and one Gatekeeper can handle a large number of server groups. A large enterprise with different branch offices or departments in separate administrative domains may deploy a Columbitech Gatekeeper in the corporate DMZ to centrally manage the remote access. When a client connects to the Gatekeeper, the Wireless VPN session will be handed over to one of the WVPN Servers belonging to the accessing user's administrative domain.

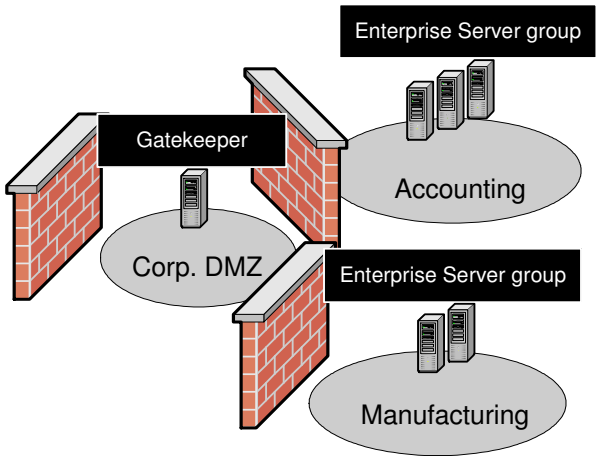

Figure 14: Example of WVPN Server clustering

If one WVPN Server within the server group were to fail, only the users connected to that particular server would be disconnected. In this case, the Wireless VPN Client will prompt the user to log in again and the Gatekeeper will now allocate another WVPN Server from the client's server group. A server failure will thus only cause a limited and temporary disruption of the Wireless VPN service.

The server group functionality allows for seamless system up-scaling; WVPN Servers and server groups may be added without any interruption of the service. New WVPN Servers will automatically connect to a Gatekeeper and send information about the server group they belong to. The WVPN Server also sends information to the Gatekeeper regarding its processing capabilities to ensure for efficient load balancing

Technical Data

Authentication Mechanisms

Columbitech Wireless VPN™ solution can be configured to use one or more of the following authentication methods:

- Windows AD username/password
- Radius (username/password or challenge/response)
- X.509 certificates
- WTLS certificates
- RSA SecurID
- Smartcard
- Biometrics

* Some authentication mechanisms are not supported by the embedded client.

Encryption Algorithms

Columbitech follows the WTLS standard and supports the following algorithms:

Encryption:

- DES (56 bit)
- Triple DES (112 bit)
- AES (up to 256 bit)

Key exchange:

- RSA (512-15000 bit)

Hashing and signing:

- MD5 (40-128 bit)
- SHA-1 (40-512 bit)

Software Requirements

Columbitech Wireless VPN™ Client

Windows 2000 professional + SP2 or higher
Windows XP
Windows Vista
Pocket PC 2002
Windows Mobile 2003, Mobile 5, Mobile 6
Windows CE 3.0*
Windows .Net*
Embedded

Columbitech Wireless VPN™ Server

Windows 2000 Professional + SP2 or higher

Windows 2000 Server + SP2 or higher
Windows 2003 Server
Wireless Switch (customized installations)
Linux (different distributions)

Columbitech Gatekeeper

Windows 2000 Professional + SP2 or higher
Windows 2000 Server + SP2 or higher
Windows 2003 Server

* Special restrictions apply. Contact Columbitech for more information

Hardware Requirements

Columbitech Wireless VPN™ Client for Windows

CPU	Any CPU capable of running Windows 2000/XP
Memory	128 MB required

Columbitech Wireless VPN™ Client for Pocket PC

CPU	StrongARM

Columbitech Wireless VPN™ Server for Windows and Columbitech Gatekeeper

CPU	Any CPU capable of running Windows 2000/2003
Memory	256 MB required, 512 MB recommended

Network Interface Cards

Columbitech Wireless VPN™ supports any standard NDIS compliant network interface card that supports Windows Media Sense. To verify if your network card supports Windows Media Sense, unplug the LAN cable or move out of W-LAN radio coverage. The card supports Windows Media Sense if the network connection status changes to "Network cable unplugged".

All standard non-NDIS compliant network interface cards are supported as long as there is a valid interface driver present. The same is true for all data enabled mobile phones.

Conclusions

Columbitech Wireless VPN™ has been created with the mobile user in mind. By enabling secure data access over any wireless IP network, Columbitech's Wireless VPN solution brings remote access to a new level. With inherent support for seamless roaming between different networks and subnets, the mobile user gets the final say about when to disconnect. If networks go down or become unavailable, the software will automatically and smoothly re-establish live connections, without any need for cumbersome login procedures.

In this white paper we have argued that wireless communication is so vastly different from wireline communication that VPN solutions built on wireline technology will fail to provide a seamless end user experience when used in a wireless environment. This we believe is mainly due to:

- **Lack of performance** - due to extensive protocol and processing overhead introduced by IPSec and Mobile IP

- **Lack of robustness** - IPSec does not cope well with low-bandwidth, large-delay networks. Although some instability issues are not directly related to IPSec or Mobile IP protocols, they make no effort to protect the user from these shortcomings.

Columbitech Wireless VPN™ is developed especially for mobile devices and wireless networks. Large effort has been made to reduce the processing and data transport overhead to a minimum as well as to create a robust communications platform on which any wireless-unaware application can operate. By only using standards and protocols developed and optimized for wireless communication, Columbitech has been able to provide a VPN architecture with exceptional robustness and end user experience, still maintaining the highest possible level of security.

References

[1] Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W. and G. Zorn, "Point-to-Point Tunneling Protocol (PPTP)", RFC 2637, July 1999.

[2] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn, G. and B. Palter, "Layer Two Tunneling Protocol "L2TP"", RFC 2661, August 1999.

[3] Kent, S., and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[4] Perkins, C., “IP Mobility Support”, RFC 2002, October 1996.

[5] Wireless Application Protocol Wireless Transport Layer Security Specification, February 2000. (http://www.wapforum.org.)