

# IP Mobility vs. Session Mobility



*Securing wireless communication is a formidable task, something that many companies are rapidly learning the hard way. IP level solutions become extremely cumbersome when moving between networks and fail to provide many services necessary when acting in a fragmented wireless environment. By acting at the session level it is possible to create a powerful and flexible VPN capable of providing state-of-the-art security as well as a superior user experience.*

## Wireless VPN technology

As mobile computing is becoming increasingly popular, the demand for VPN access from mobile clients is rapidly increasing. This white paper identifies the critical functions of a wireless VPN and investigates how they are implemented at the IP and session level respectively. This paper argues that IP VPN solutions are inherently limited when it comes to wireless communication, and that a session level VPN presents a powerful and attractive alternative. The biggest challenge is handling movement between different networks without losing the VPN connection, so-called seamless network roaming. In order to facilitate discussion, two new concepts are introduced: IP mobility and session mobility.

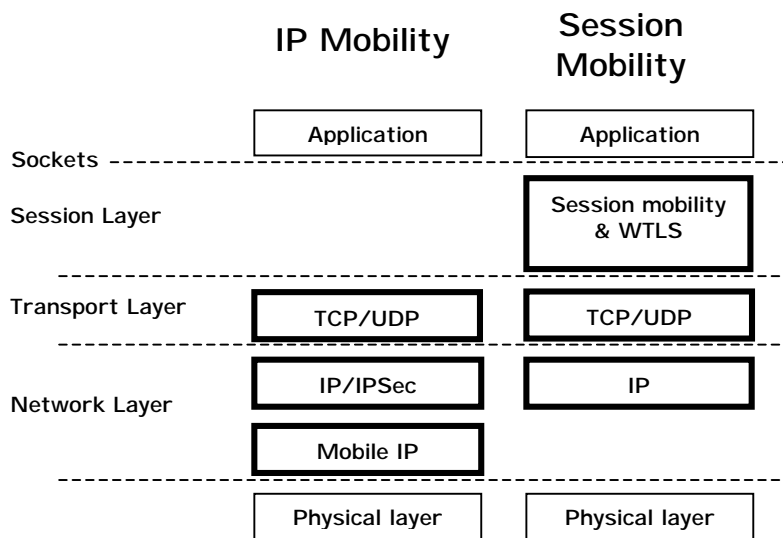
### IP mobility

The obvious IP level approach for the construction of a wireless VPN is to implement IPSec along with Mobile IP. The strategy is to provide transparency to the transport layer. Mobile IP effectively hides IP address changes allowing transport level connections to survive a network handover. This said, an IP level approach leaves the responsibility for flow control and session recovery to the transport protocol used, normally TCP. The use of IPSec introduces other problems as well, among which the NAT-problem is the most serious. This and other problems will be discussed later in this paper.

### Session mobility

A session level solution implements VPN and mobility functions at the session layer, as the name suggests. No attempts are made at keeping transport level connections alive during network roaming. Instead the solution relies on recovery mechanisms at the session layer for fast transport connection re-establishment.

Figure 1 shows a schematic overview of where in the protocol stack VPN and roaming functionality is implemented in an IP VPN and session level VPN respectively.



**Figure 1: Protocol stack overview**

In the following chapters we will perform a comparison between IPSec based VPNs and a WTLS based session level VPN, focusing on the following problem areas:

- Security
- Convenience and robustness
- Roaming
- Performance
- Interoperability and scalability

## Security

The most important function in a VPN is security. A wireless VPN must provide at least the same level of security as traditional wireline VPNs. Sensitive data is transmitted over public, insecure networks, which are fully accessible by third parties. Enterprise VPN solutions rely on their security mechanisms to provide privacy, data integrity and authentication. If any of these mechanisms fail, the VPN is vulnerable to attacks.

IPSec [1] has become the de facto security standard for IP VPNs. Since IPSec is a network level protocol, its security mechanisms are tightly connected to the IP address of the connecting host, an unfortunate characteristic that prevents smooth operation in a wireless environment with different networks hosted by different operators.

An alternative solution is to use WTLS (Wireless Transport Layer Security) [4], which is a wireless adaptation of the TLS protocol. At a first glance IPSec and WTLS present very similar services, such as strong encryption, authentication, signing and hashing. However, there are at least two important differences between the protocols, as will be described below.

WTLS can be used to enforce strong end-to-end security on an application-to-application level, which means that encryption is maintained past any corporate firewall or gateway all the way to the application if needed. If end-to-end security is not required, WTLS encryption can be terminated in a border gateway as is normally the case with IP VPN solutions. With end-to-end security, an application is able to differentiate its services depending on the security policy used by the accessing device. In a corporate email application for example, emails may be labeled for different levels of sensitivity. Only devices that use the strongest security mechanisms are allowed to download emails labeled confidential, while devices using weaker security may download emails with normal sensitivity.

IPSec is unable to maintain encryption past ordinary firewalls, gateways and Network Address Translators (NATs) without a large-scale network upgrade. This is due to the fact that traditional NAT servers expect transport level information rather than IPSec headers following the IP header. The so-called NAT problem has been attracting a lot of attention within the IETF community, but so far no standardized solutions are at hand.

## Convenience and robustness

In a wireless environment, network availability can never be guaranteed; connection instability is something a mobile user must cope with. Network services may be unavailable due to bad radio coverage, shortage of radio resources or during network roaming.

### Session resume

Secure connection establishment is a process that requires heavy computations and many messages need to be sent between the two communicating peers. If the communication device is a PDA with limited processing power, a session setup may take several minutes to perform. Therefore it is of paramount importance that the session is able to survive periods during which network services are unavailable.

To address these issues WTLS supports mechanisms for convenient and fast re-establishment of lost connections. The *session resume* functionality allows for long-lived WTLS sessions that are able to survive network failures. If a connection is lost, a new connection can be set up without any complex computations, at a fraction of the original setup time. Since the reconnection is performed in the background, no user interaction is required, i.e. the user does not have to re-logon after a session resume.

IPSec and WTLS perform very similar set up operations, normally called a handshake, but as IPSec lacks the session resume functionality, a full-scale handshake including key exchange mechanisms and capability negotiations must be performed each time the client reconnects. As connection instabilities are quite common in wireless communication, the user experience is dramatically improved with session resume functionality.

### Transaction recovery

One of the effects of implementing a wireless VPN at the session level is the possibility to implement a *transaction recovery* mechanism, providing reliable and seamless data transactions in a network environment with intermittent connectivity. For example, if a file transfer or an email download is in progress when the user enters an area without radio coverage, the transaction recovery mechanism can resume the transaction from where it was interrupted, without losing any previously transmitted data, as soon as the network is available.

A VPN solution based on IPSec has no inherent support for transaction recovery. In the scenario described above, the transaction must start all over again, losing all previously transmitted data. The only way to prevent data loss is to have every application implementing its own recovery mechanism. IP based solutions thus fail to provide an acceptable level of network transparency to the application layer.

## Network roaming

By network roaming we mean the general concept of movement between different networks. The networks may be constructed using different technologies and administrated by different network operators.

The proposed technology for providing network roaming in an IP VPN is called Mobile IP [2]. The idea is to prevent TCP sessions from breaking down during network handover. Network roaming often

results in a change of the device's IP address, which in turn causes the TCP connections to fail. Mobile IP uses IP tunnels to transparently route data to the wireless device, regardless of its current point of attachment. By using the combination of a care-of address (provided by the visited domain) and a home address (provided by the home network), network roaming is made transparent to TCP.

In reality a TCP session is unlikely to survive a network handover between different types of networks. A movement from a fast network, such as wireless LAN or Bluetooth, to a slow network, such as GPRS, will trigger multiple TCP timeouts from which the TCP connection may be unable to recover. When acting in a fragmented network environment with different types of networks interoperating, IP layer mechanisms fail to provide seamless roaming with continuity of services.

A different approach is to utilize the session resume functionality implemented in WTLS for network roaming. There is no point trying to keep the TCP sessions open when TCP itself is so vulnerable to the changing link environment. By using the session resume mechanism in WTLS, a new TCP session is opened and secured very quickly. Since all application connections are terminated locally on the computer, the establishment of the new TCP session is made totally transparent to the applications.

## Performance

One of the primary reasons for using IP VPN technology is the transparency to the upper layers, as this gives flexibility and applications do not have to be rewritten for wireless communication. This is also true for session level VPN solutions. By placing the VPN functionality underneath the operating system's socket API, all applications are wireless enabled by default. The difference between IP based solutions and session level solutions is that transparency in an IP VPN is achieved at the expense of performance while a session level solution is able to provide a high level of transparency and at the same time provide maximum performance.

In the reality of wireless communication, radio resources will always be scarce. This motivates the efforts for implementing wireless optimizations and compression.

## Compression

Compression is an optimization technique that has been widely used in most communication modems for many years. Common for all types of compression algorithms is that compressing encrypted data has no effect since the algorithms take advantage of structures in the data, something good encryption removes completely. Because of this it is vital to compress data before encryption if the data compression is to be effective. In general, more information about the data to be encrypted provides for better compression results. In a session level solution, compression and data reduction is performed close to the application layer ensuring high compression ratios.

IPSec implements compression mechanisms that may be applied to the data before encryption, but only on a packet-by-packet basis. First, there is no way finding out the nature of the data, which makes it impossible to use stateful compression techniques. Second, since every IP datagram is compressed separately, compression cannot be applied on a large stream of data. Because of this structural recurrence cannot be used in an effective way to increase compression efficiency.

## Data reduction

Data reduction is an effective way of increasing wireless performance. Protocol optimizations implemented at the session layer such as binary encoding and caching reduce latency as well as the amount of data sent between the communicating peers.

## Enhanced flow control

TCP recovery and flow control mechanisms are designed for a wireline environment with small delay variations, and where data loss is due to congestion in the network. Wireless communication however,

presents a totally different environment with low throughput and large delay variations, and data loss occurs mainly due to intermittent connectivity. When data is lost for reasons other than congestion, TCP flow control mechanisms result in an unnecessary reduction in end-to-end throughput and hence, in sub-optimal performance.

During network roaming it is extremely important that the flow control mechanisms are able to respond quickly to changes in link layer capacity. When moving from a fast network to a slow network, the flow control must respond immediately by decreasing its sending rate. Failure to do so will cause multiple TCP timeouts. Similarly, when moving from a slow network to a fast network, the flow control mechanism should react quickly for optimized link utilization.

Even though the end-to-end semantic of TCP is attractive when it comes to reliability, it presents a number of problems when used in a wireless setting. It is not possible to implement efficient wireless optimizations since part of the communication is actually taking part over a wireline network. In a session level VPN, the end-to-end TCP connection can be split into two connections, one over the wireline network and one over the wireless network. The flow control and recovery mechanisms can now be optimized for the specific environment in which the TCP implementation is used. Wireless optimizations are implemented on the wireless TCP connection, while the wireline connection is optimized for wireline communication. Even when using standard TCP implementations for both connections, there is a notable increase in performance. This is due to the fact that the connections can adapt their data flows independently of each other.

A split TCP solution is possible in a session level VPN since encryption is done at the session layer. IP VPNs on the other hand, do not allow for split TCP solutions since encryption is carried out at the network layer, making TCP optimizations unfeasible. Furthermore, session level VPNs rely on session layer mechanisms for loss recovery during network roaming and during periods of intermittent connectivity while IP based VPNs must rely on the recovery and flow control mechanisms implemented in TCP, resulting in instability and low reliability.

By implementing session layer management, the underlying transport protocol may be separated from the application protocols. Session management provides a channel to the application layer by multiplexing virtual connections on top of a reliable stream oriented transport protocol, for example TCP. By only having to maintain one TCP session, overhead and redundant retransmissions can be drastically reduced.

## **Interoperability and scalability**

As mentioned in the security discussion, IPSec does not interoperate well with existing NAT server solutions. Since most operators will be forced to use address translations, running Mobile IP without Foreign Agents will not be possible. Instead every operator and service provider must operate Foreign Agents inside their domains. This means maintaining a large number of security associations between Home Agents and Foreign Agents. Furthermore, Mobile IP requires Foreign Agents close to the radio access networks due to routing issues, leading to poor scalability and complex administration. When the Foreign Agent de-tunnels packets destined for a mobile terminal, a topologically incorrect destination address will be exposed, preventing normal IP routing. Forwarding data to the destination must therefore involve link layer mechanisms.

A session level VPN performs all its functions above the network layer, providing maximum interoperability with existing network infrastructure. A successful wireless VPN must be easily integrated into existing corporate solutions already deployed, extending rather than replacing them.

## The Columbitech solution

Columbitech Wireless VPN™ is a session level VPN architecture designed to eliminate the weaknesses of today's VPN solutions, while at the same time creating something as unique as a roamable, wireless VPN with true end-to-end security. The solution relies on WTLS and has been designed to meet the requirements for true mobile communication, i.e. secure corporate access anywhere, anytime, and with any device.

To improve the user perception further efforts have been made to improve compression capabilities. In wireless networks such as GPRS and GSM the area of compression is of great importance since it lowers the cost and the user experience faster communication.

Columbitech Wireless VPN™ is designed for seamless interoperability with existing corporate solutions. A company that is already using an 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™ 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 a wireline environment.

The Columbitech architecture is a client/server software based solution built on wireless technology for optimal performance. To ensure easy wireless enabling of corporate legacy applications, the software supports industry standard application programming interfaces on the client and server side.

## Conclusions

This white paper has described how wireline technology adaptations fail to solve many of the problems related to communication in a fragmented wireless environment. It has also described how a session level approach addresses the problems related to secure wireless communication.

The main reason behind the problems with IP level solutions is the fact that they rely on IPSec and TCP for handling flow control and session management. Both IPSec and TCP have been designed for a wireline environment, something that strongly affects their usefulness in a wireless setting. Using a session level approach, Columbitech Wireless VPN™ has been designed specifically for a wireless communication environment. The architecture combines seamless network roaming with an exceptional user experience in terms of security, performance and convenience.

## References

- [1] R. Atkinson and S. Kent, "Security Architecture for the Internet Protocol", RFC 2401, November 1998
- [2] C. Perkins, "IP Mobility Support", RFC 2002, October 1996
- [3] J. Postel, "Transmission Control Protocol Specification", RFC 793, September 1981
- [4] "Wireless Transport Layer Security Specification", WAP Forum, February 2000