Advance Information

SECURITYWP/D
Rev. 1, 3/2003

Securing the Smart Network with Motorola Security Processors

Author's Name
Neil Gammage
neil.gammage@
motorola.com

Geoff Waters
geoffrey.waters@
motorola.com

This document contains the following topics:

Part I Overview

End-customer demand for network security is growing at a tremendous rate. Governmental, commercial and public users of networking infrastructure are becoming aware that private communication via the Internet cannot be assumed. In fact, the likelihood of private information being stolen or altered is directly proportional to the value of that information.

While most members of the public can rely on their personnel communications being insufficiently valuable to draw the attention of a malicious outsider, that has not been the case for governmental and certain commercial users. Many government agencies are already sophisticated users of encryption and authentication technology, especially in areas of defense, intelligence, and finance. Some commercial enterprises have had IT security procedures in place for years, and others are rapidly upgrading their communications infrastructure to protect their data. There is a clear move to heighten security in all industries—migrating from unprotected networks to ones that support only encrypted or authenticated data.

Networking standards bodies have developed security protocols, such as Internet Protocol security (IPSec) and Secure Sockets Layer (SSL) to address the need for authentic and confidential communication in public networks. Network equipment vendors initially enabled security through software upgrades, wherein the customer could add IPSec or SSL to existing systems without changing hardware. While this allowed systems to claim VPN support, it quickly became apparent that customers actually intending to use their systems for terminating secure tunnels would be disappointed by security software running on general purpose hardware.

To meet the challenge of line rate security, a new class of integrated circuit was developed. Security processors are special purpose devices designed to accelerate the computationally intensive algorithms associated with encrypted and authenticated communications. Security processors are becoming near mandatory additions to various networking devices, especially in wireless networks, broadband access devices (such as cable-modem systems or xDSL systems), and remote access servers —key entry points into network infrastructures. Networking equipment vendors recognize that as the need for greater security increases, insecure solutions will not be able to compete with secure systems.

Motorola's first family of security processors, which targets customer premise equipment (CPE), broadband access, and network edge markets, was designed to be a cost efficient, easily integrated security solution for Motorola's popular PowerQUICC™ and PowerPC™ processor families.

Motorola's experience in data and communications security spans over 30 years, selling to the most sophisticated users of encryption technology—the aforementioned government agencies. In addition to the full communications systems produced for governmental customers, Motorola has applied its expertise in security technology to wireless handsets, smart cards, and cable set-top boxes. In 2000, Motorola brought its security technology and expertise to the commercial networking market via the introduction of the S1 Family of Network Security Processors. Designed to work seamlessly with Motorola communications processors, Motorola network security processors offer system designers an easy way to enhance the encryption and authentication performance of networking equipment.

This paper defines the technology behind network security and how that technology is applied to networks today. It also describes Motorola's full suite of security products available to solve your current security requirements. If you are already familiar with IPSec and SSL, you can jump right to learning about Motorola's security processor offerings on page 13.

Motorola plans to continue to secure the networks of tomorrow through future generations of security solutions that provide higher levels of performance and integration.

Part II What is Network Security?

In network communications, the term 'Security' covers the three related issues of ensuring the authenticity, integrity and confidentiality of data transmissions.

- Authenticity is ensured by authentication mechanisms, which provide the means for a data receiver to verify that a message was sent by the node that claims to have sent it
- Integrity is ensured by related authentication mechanisms, which also provide the means for a data receiver to verify that data has been received exactly as it was sent, and has not been modified in transit
- Confidentiality is ensured by encryption mechanisms, which provide the means to prevent unauthorized receivers of data from being able to read and use it.

The authentication and encryption mechanisms at the heart of security are provided by security protocols used in combination with suites of encryption and authentication algorithms. The three major security protocols are IPSec (Internet Protocol Security), SSL (Secure Sockets Layer) and TLS (Transport Layer Security). The last two are closely related and are often referred to jointly as SSL/TLS. The algorithms used by these protocols include bulk encryption algorithms, public key encryption algorithms, and message authentication algorithms.

2.1 IPSec

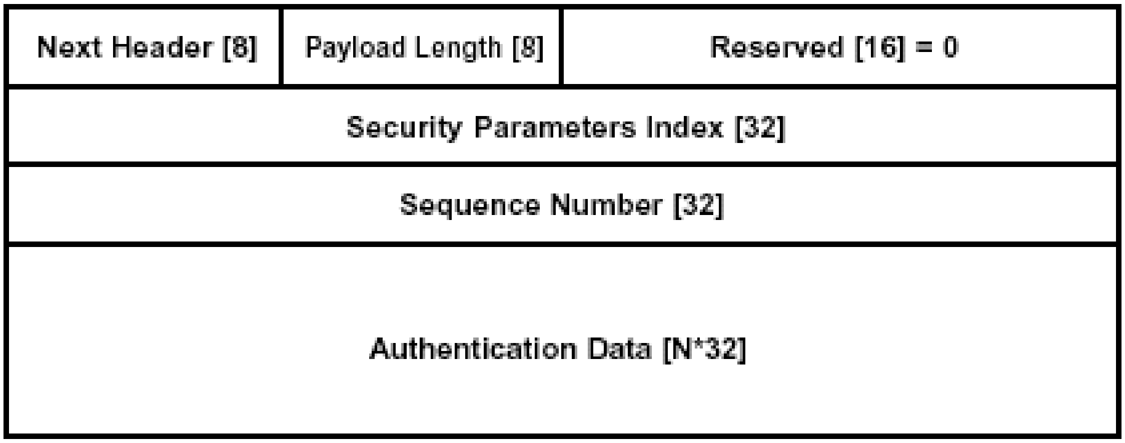
Internet Protocol Security is an extension of IP defined by IETF to provide security for all Internet traffic. A series of RFCs define the information to be added to IPv4 and IPv6 packets to ensure data security as well as specifying how encryption and authentication algorithms are to be used.

The architecture of IPSec, defined in [IPSEC], is based on setting up security associations between senders and receivers of data, which define the algorithms to be used for message encryption and authentication and the security keys to be used with these algorithms. IPSec defines the protocols that may be used for security, and also defines the mechanisms and protocols that may be used to establish security associations.

IPSec encompasses two packet transforms, Authentication Header (AH) and the Encapsulating Security Payload header (ESP). Each is described in the next sections. A packet may be secured via AH, ESP, or both, depending on the level of security required.

2.1.1 IPSec Authentication Header

The Authentication Header described in [AH] is used to permit authentication data to be transmitted with packet, and provides for authenticity and integrity, but not confidentiality. The authentication data is calculated by the sender and checked by the recipient to verify that the packet was transmitted by the sender, and has been received is as it was transmitted, without modification. The header format is as shown in Figure 2-1.



Next Header [8]	Payload Length [8]	Reserved [16] = 0
Security Parameters Index [32]		
Sequence Number [32]		
Authentication Data [N*32]		

Figure 2-1. Authentication Header

The fields are described as follows:

- Next Header – Defines the protocol of the next header in the packet. For IPv4 this will either be a UDP or TCP header, or no header if used in a raw IP packet. For IPv6 this may also define a further extension header after the AH and before the upper layer header.
- Payload Length – The length of the header in 32 bit words, minus 2.
- Reserved – The next 16 bits are reserved and must be set to 0.
- Security Parameters Index (SPI) – A randomly chosen number, which together with the destination IP address, identifies the security association (SA) to be used for authenticating the IP packet.
- Sequence Number – A counter incremented by the sender for every packet sent to the same destination. The destination should discard any packet received with a sequence number it has already processed.

- Authentication Data – The Integrity Check data used to authenticate the packet. Used as determined by the SPI to authenticate the packet.

The sequence number is incremented by the sender for every packet sent and may be checked by the receiver to detect lost or duplicated packets.

In the case of IPv4, the AH follows the IP header. In the case of IPv6, the AH follows the IP header and all extension headers except the ESP (if present). The authentication data is calculated by applying the authentication algorithm defined by the SPI to the entire packet, including immutable fields in the IP and IPv6 extension headers (for example, Source and Destination Address fields), as indicated in Figure 2-2.

The choice of:

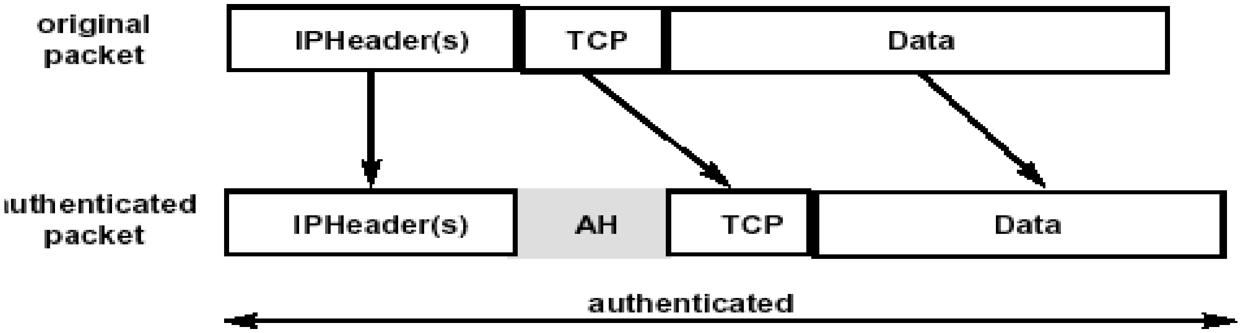


Figure 2-2. Authentication Header Coverage

2.1.2 IPSec Encapsulating Security Payload

The ESP transform described in [ESP] is used to send and received packets with encrypted payloads. Optionally, it also provides similar authentication capabilities to the AH and therefore covers the full set of security concerns—authenticity, integrity and confidentiality. The format of the header is as shown in Figure 2-3.

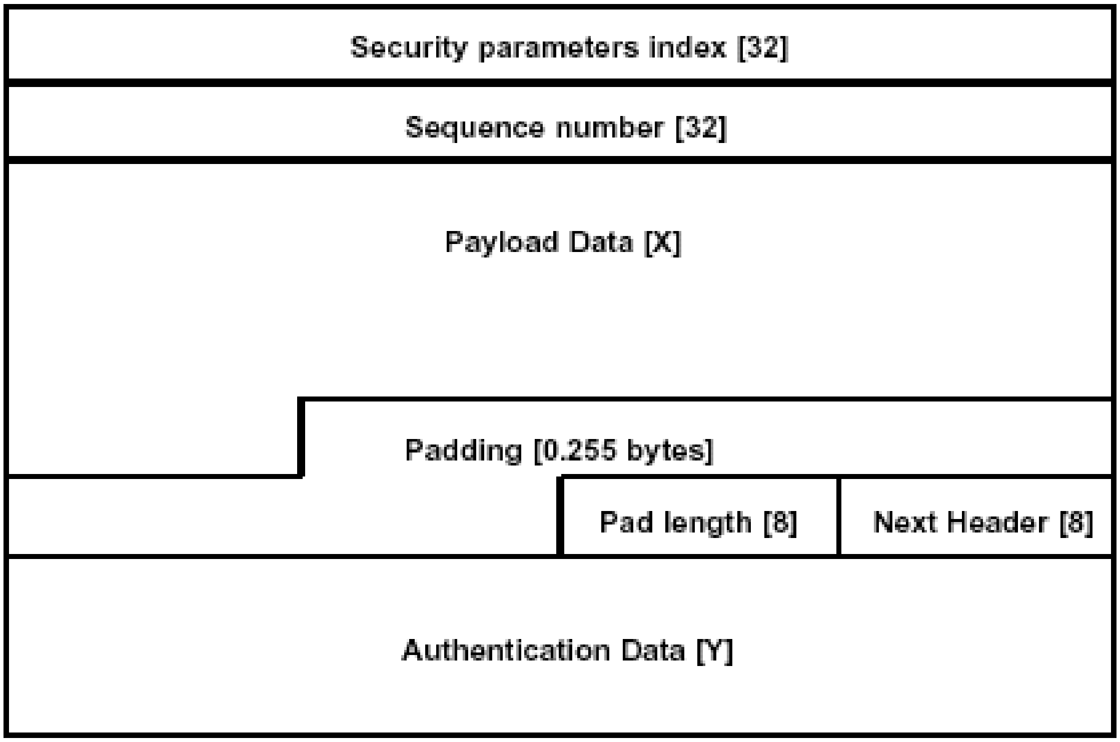


Figure 2-3. Encapsulating Security Payload Header

The fields of the header are as follows:

- Security Parameters Index (SPI) – A randomly chosen number, which together with the destination IP address, identifies the security association (SA) to be used for encrypting and authenticating the IP packet.
- Sequence Number – Used as for the AH.
- Payload Data – The encrypted payload along with any data required for decryption (for example, initialization data).
- Padding – Added to the header to ensure that the payload data ends on the appropriate byte boundary. This is required since the encryption algorithms are block ciphers operating on a fixed data block size.
- Pad Length – The number of padding bytes added
- Next Header – Used as for the AH.
- Authentication Data – If authentication is applied, is used in the same way to the Authentication Data field in the AH.

For IPv4, the ESP follows the IP header, and for IPv6 the ESP follows the IP header and all extension headers. In both cases, all packet data following the IP header (including any upper layer headers) is encrypted, and the authentication data is computed over the entire ESP header (including the enciphered data of the original packet), as shown in Figure 2-4.

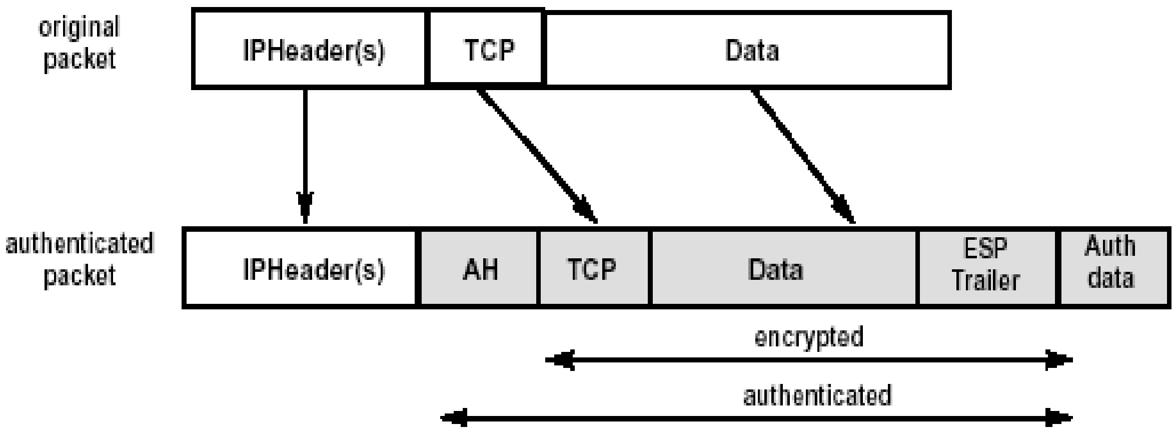


Figure 2-4. ESP Coverage

It is far more frequently used than the AH as the ESP is able to provide both authentication and encryption.

2.1.3 Transport and Tunnel Modes

IPSec can be used in two modes, Transport mode and Tunnel mode. The figures in the previous sections illustrated the AH and the ESP being applied in Transport mode. In Tunnel mode, the original packet is tunnelled by encapsulating the original message in a tunnel IP header before applying the AH or ESP.

When using the ESP in Transport mode, the IP header is neither encrypted nor authenticated. There is no protection against it being maliciously modified in transit nor against it being viewed and understood by an intermediate node even when an ESP is used. Although such a node will not be able to understand the message itself, it will be able to see which host sent it and which will receive it, and this information can be of significance in itself. When the ESP is used in Tunnel mode, both encryption and authentication are extended to cover the entire original packet, as shown in the figure below. In this figure, you can see that the entire original packet including the original IP header is authenticated and encrypted.

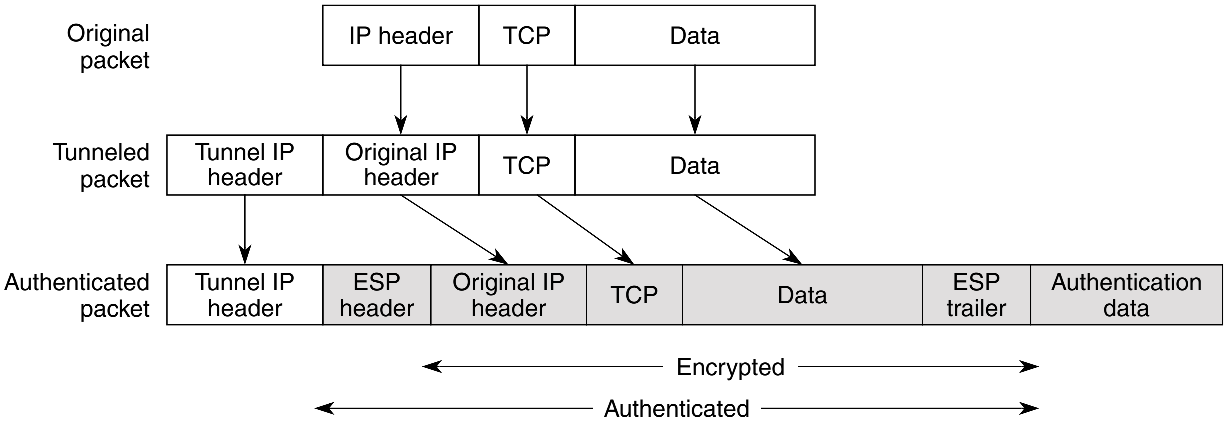


Figure 2-5. ESP Used in Tunnel Model

The process when an AH is used in Tunnel mode is shown in Figure 2-6. As you can see, use of the AH in Tunnel mode provides no additional coverage than that afforded in Transport mode.

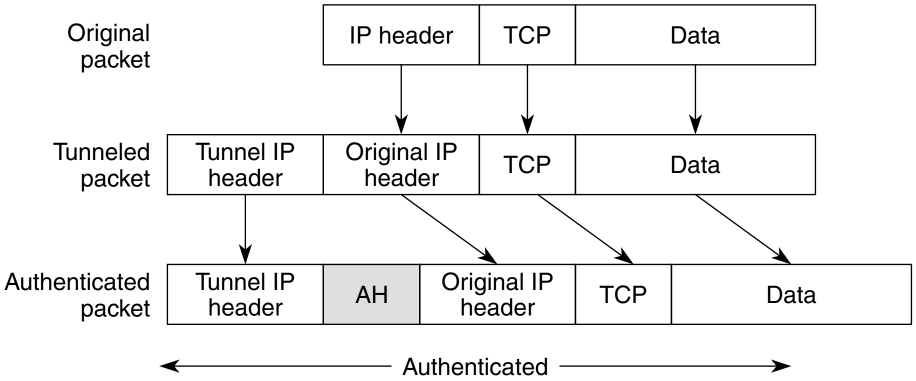


Figure 2-6. AH Used in Tunnel Mode

Transport mode can only be applied between two host systems – for example a workstation client and a network server. However, Tunnel mode can be applied not only between hosts but also between intermediate systems acting as security gateways. These might be devices such as firewalls or routers or specialized nodes providing a security service for the traffic flowing through them.

As shown in Figure 2-7, Transport mode may only be used between Host 1 and Host 2. Tunnel mode may be used between two Hosts, between a Host and a Gateway, or between the two Gateways. Because of the additional coverage when using the ESP and the ability to operate between security gateways, tunnel mode is far more frequently used than transport mode.

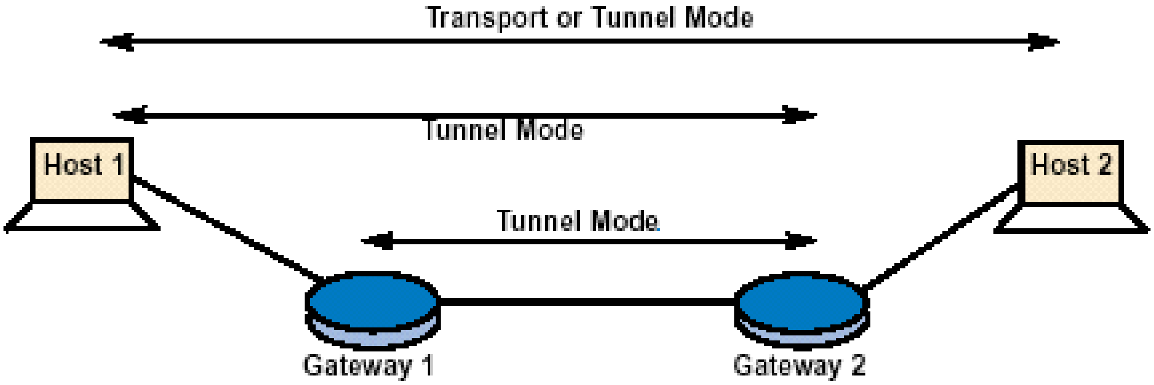


Figure 2-7. Transport and Tunnel Mode Coverage

2.1.4 Security Associations

A security association is a connection between an originator and receiver of encrypted or authenticated data. SAs are unidirectional, so that if a bi-directional flow of secure data is required between two nodes, two SAs must be set up, one for each direction. The SA determines whether an AH or ESP (or both) should be used, and defines the encryption and authentication algorithms and the encryption and authentication keys to be used to secure traffic. The cipher algorithms that may be used with the ESP are defined in [DES] and [CBC]. The inclusion of AES as a supported cipher algorithm within IPSec-ESP is expected in 2002. The message authentication algorithms which are used with the ESP and AH are defined in [HMAC], [MD5] and [SHA-1].

Every IPSec enabled node maintains two databases, a security policy database (SPD) and a security association database (SAD).

The SPD is used for outgoing packets, and is used to determine whether packets are to be processed by IPSec, and if so, how. The SPD is searched using a mask that may include the source and destination IP address of the packet, the source and destination port numbers, and the higher layer protocol (UDP/TCP) in use. Wildcard and number ranges are permitted in all fields of the key. If a matching entry is found in the database, the data returned determines:

- Whether an AH or ESP (or both) should be used
- Whether transport or tunnel mode should be used
- Which authentication and/or encryption algorithms are to be used.

The entry also contains a pointer to an entry in the SAD if one exists. If an SA does not exist, the SPD data contains all of the information required to set up a new one. The SAD entries contain all of the information required to construct the AH or ESP header and encrypt and/or authenticate the packet. Each entry includes:

- AH Authentication algorithm identifier and key (for AH SAs)
- ESP Authentication algorithm identifier and key (for ESP SAs)
- ESP Encryption algorithm identifier and key (for ESP SAs)
- Lifetime
- Sequence number counter
- Anti-replay window

The last two fields are used if the sequence number in the AH or ESP is to be used to detect lost or duplicated packets. The Lifetime is used to automatically limit the time that an SA can exist. When the lifetime expires, a new SA must be set up if necessary.

The SA data is used to encrypt and/or authentic the AH and/or ESP on outgoing packets. At the receiving IPSec node, the SA is lookup up using a key consisting of the Security Parameters Index (SPI) carried in the AH or ESP and the destination IP address of a packet. This provides the receiving node with all of the information required to decrypt and/or authenticate the packet.

2.1.5 Key Management

The Internet Security Association and Key Management Protocol defined in [ISAKMP] and [DOI] is a process for the creation of new security associations as required. The process is triggered by an attempt to send a secure packet between a sender and receiver who do not have an appropriate SA set up. ISAKMP defines a two-stage process for setting up an SA:

1. An authenticated connection is established between the sender and the receiver.
2. Key data is exchanged over the secure connection

ISAKMP does not specify the key exchange protocol to be used, but does recommend the use of Internet Key Exchange protocol, defined in [IKE] for the purpose.

The IKE connection may be authenticated in a variety of ways:

- Pre-sharing authentication keys and using MAC or HMAC as an authentication algorithm
- Exchanging data including public keys and using the RSA public key algorithm.
- Exchanging digital signatures using either the RSA public key algorithm or DSS/DSA

Once established, the Oakley (modified DH) protocol is used to exchange key data. At the completion of the key exchange, both parties to the SA will have agreed on the encryption and/or authentication algorithms and keys to be used.

2.2 SSL/TLS

Secure Sockets Layer is a protocol stack developed by Netscape for secure transmission of web pages. Transport Layer Security is an IETF protocol based on SSL, defined in [TLS].

SSL is built on a variety of security technologies, including

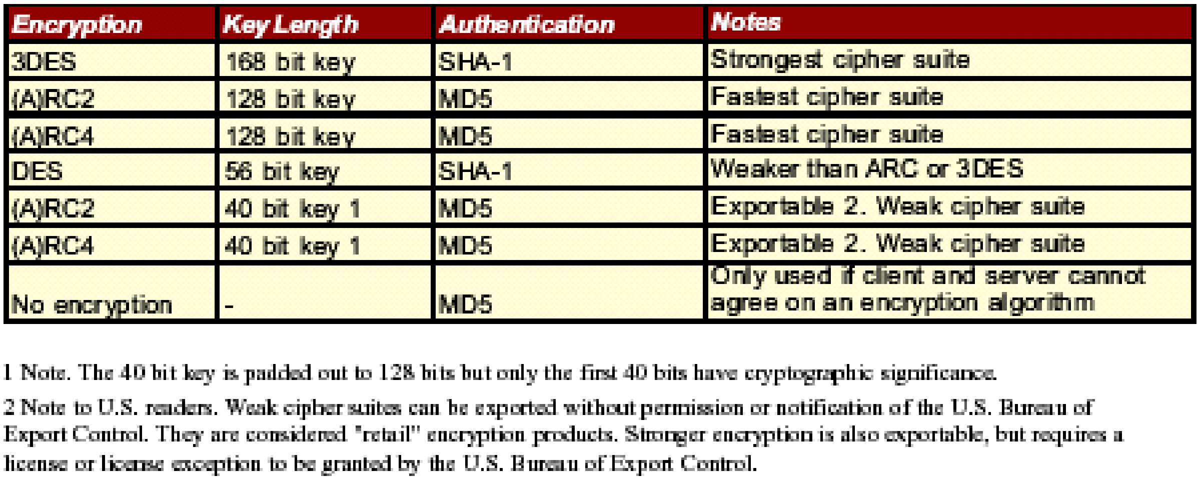
- Symmetric key algorithms such as DES, 3DES, and ARC-4 for bulk data encryption
- Message authentication algorithms MD5 and SHA-1
- User authentication algorithms such as RSA and DSA
- Key exchange algorithms such RSA key exchange and KEA

As can be seen there is a great deal of similarity between IPSec and SSL/TLS in the algorithms required to support them. Like IPSec, SSL defines both a secure message exchange protocol equivalent to the ESP protocol (the SSL record protocol), and a protocol similar to ISAKMP/IKE which is used to establish security associations and exchange session keys (the SSL handshake protocol).

2.2.1 SSL Cipher Suites

The two handshake protocols supported by SSL are one based on the RSA key exchange algorithm and one based on the KEA algorithm. Two sets of cipher suits are used with SSL. The first set uses the RSA key exchange algorithm in the SSL handshake that is shown in Table 2-1.

Table 2-1. SSL RSA Exchanged based Cipher Suites



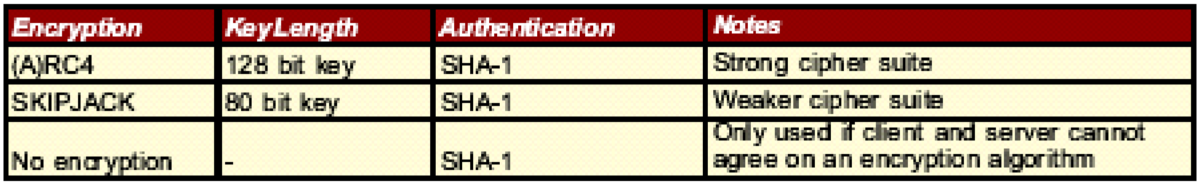
Encryption	Key Length	Authentication	Notes
3DES	168 bit key	SHA-1	Strongest cipher suite
(A)RC2	128 bit key	MD5	Fastest cipher suite
(A)RC4	128 bit key	MD5	Fastest cipher suite
DES	56 bit key	SHA-1	Weaker than ARC or 3DES
(A)RC2	40 bit key 1	MD5	Exportable 2. Weak cipher suite
(A)RC4	40 bit key 1	MD5	Exportable 2. Weak cipher suite
No encryption	-	MD5	Only used if client and server cannot agree on an encryption algorithm

1 Note. The 40 bit key is padded out to 128 bits but only the first 40 bits have cryptographic significance.

2 Note to U.S. readers. Weak cipher suites can be exported without permission or notification of the U.S. Bureau of Export Control. They are considered "retail" encryption products. Stronger encryption is also exportable, but requires a license or license exception to be granted by the U.S. Bureau of Export Control.

The second set of encryption and message authentication algorithms is the FORTEZZA cipher suites. FORTEZZA is an encryption system used by the U.S. government for sensitive but unclassified information. The KEA key exchange algorithm is used in the SSL handshake when these suits are in use. Table 2-2 shows the KEA key exchange:

Table 2-2. FORTEZZA Cipher Suites



Encryption	KeyLength	Authentication	Notes
(A)RC4	128 bit key	SHA-1	Strong cipher suite
SKIPJACK	80 bit key	SHA-1	Weaker cipher suite
No encryption	-	SHA-1	Only used if client and server cannot agree on an encryption algorithm

2.2.2 The SSL Handshake

The SSL handshake is used in the same way as ISAKMP in IPSec. That is, it first exchanges data, including digital certificates, between the client and server that enable the client to authenticate the identity of the server, and optionally to permit the server to authenticate the identity of the client. The second part of the handshake uses a key exchange algorithm to create the session keys which will be used to encrypt and decrypt subsequent SSL messages.

2.3 IPSec vs SSL

The major difference between these two protocols is the OSI layer at which they operate. IPSec is an enhancement to IP operating at the IP Datagram layer, and therefore does not recognize the concept of a TCP session or an end user. SSL/TLS operates on top of TCP/IP and is designed to provide security on a per TCP session and per user basis. Secondary difference is that whereas IPSec is based on peer-to-peer protocols, SSL is based on client-to-server protocols.

But why do we need two sets of security protocols at all? The reason is the usage for which each protocol suite was intended. IPSec was intended as a security protocol for all Internet traffic between any two nodes in the network. This makes it ideal for applications such as VPN, where traffic between two enterprises or between remote nodes and an enterprise need to be secured. This is the major use for IPSec Tunnel mode implemented on Security Gateways.

SSL, on the other hand, was intended to secure individual web interactions on a per user basis. As such it is defined exclusively as a host-to-host protocol – there can be no such thing as an SSL security gateway.

IPSec security associations are relatively long lived and are set up and terminated infrequently. In an IPSec implementation the rate at which secure data can be transmitted (ideally line rate) is far more important than the time taken to execute an IKE handshake.

By contrast, SSL sessions by definition carry the traffic of a single user and are relatively short lived, existing for access to a secure server typically for only part of a browser session. As a result at the server end of an SSL connection, the rate at which the SSL handshake protocol can be operated is a major issue for SSL implementations.

Part III Where is Security Required on the Network?

Security is needed, at some level, everywhere on the network. Whether or not a particular piece of networking equipment is a security gateway or end-point determines the volume of user traffic the system must be prepared to secure. The computational load added to a system performing frequent authentication is significant, but the load for authentication plus encryption is overwhelming. Systems capable of full duplex OC-3 routing without IPSec are brought to their figurative knees performing IPSec in software (less than 1Mbps!). Servers capable of thousands of insecure transactions per second see their performance measured in tens when running SSL. Hardware acceleration is not an option when encryption is more than an occasional activity.

Besides securing the data path, there is a growing requirement for control path security. Most network infrastructure uses the same physical connections for user data as control data. This means the control traffic is "in-band", which has serious implications for security. Previously, control traffic was "out of band", meaning control information travelled on dedicated, and presumably secure links. When out of band signalling exists, remote configuration of a router or server can only take place on that secure physical interface, and the other end of the link is known to be connected to an authorized administrator.

Where separate physical links are impossible (satellites) or uneconomical (everything else), in-band control traffic needs to take on the characteristics of a physical link between the authorized administrator and the remote equipment. Strong encryption and authentication can satisfy this requirement. Control traffic can be tunnelled through the data path via IPSec or SSL, and a control "port" in the remote equipment only sees the commands that pass through the secure tunnel termination point. Failure to secure a control port with a secure link (physical or encrypted tunnel) undermines any security applied to the data path. A malicious outsider, having failed in his attempt to read encrypted traffic, can attack the network infrastructure directly via an insecure control port, and command the router to turn off encryption of user data.

Control traffic is not just between a network administrator and a control port of a router, though. Routers exchange significant volumes of routing table updates, and other bindings, and this traffic can also be exploited by an attacker if it is not (at least) authenticated. Add to this customer billing information, and other "accounting" traffic, and the volume of in-band control traffic starts to add up.

Although control traffic is only a fraction of user data, the computational cycles taken away from the control plane of typical network infrastructure is sufficient to hurt overall system performance. System designers are adding hardware acceleration to network infrastructure not traditionally considered security end-points to ensure that the host spends its cycles running the operating system, rather than running 3DES.

Security Processors, such as Motorola’s S1 Family, provide the needed computational boost for handling both data path and control path security, which is especially critical in access and edge equipment.

Part IV What are Motorola’s Security Solutions?

With the introduction of the S1 Security Processor Family in 2000, Motorola effectively applied its years of expertise in governmental encryption solutions to the commercial networking market. Motorola’s first family of security processors, which targets customer premise equipment (CPE), broadband access, and network edge markets, was designed to be a cost efficient, easily integrated security solution for Motorola’s popular PowerQUICC and PowerPC architecture processor families. The S1 Family can also be used with the C-Port Network Processor Family in lower bandwidth, control plane applications.

With the addition of the MPC184 and MPC185 into the S1 Family, Motorola expands the price, performance, and interface options for system designers using Motorola processors, providing tremendous flexibility and enabling quick time to market of secure solutions. As Motorola introduces higher performance security processors, and integrates the security functionality into popular processor lines, the goal remains to meet customer security needs across all performance and integration levels.

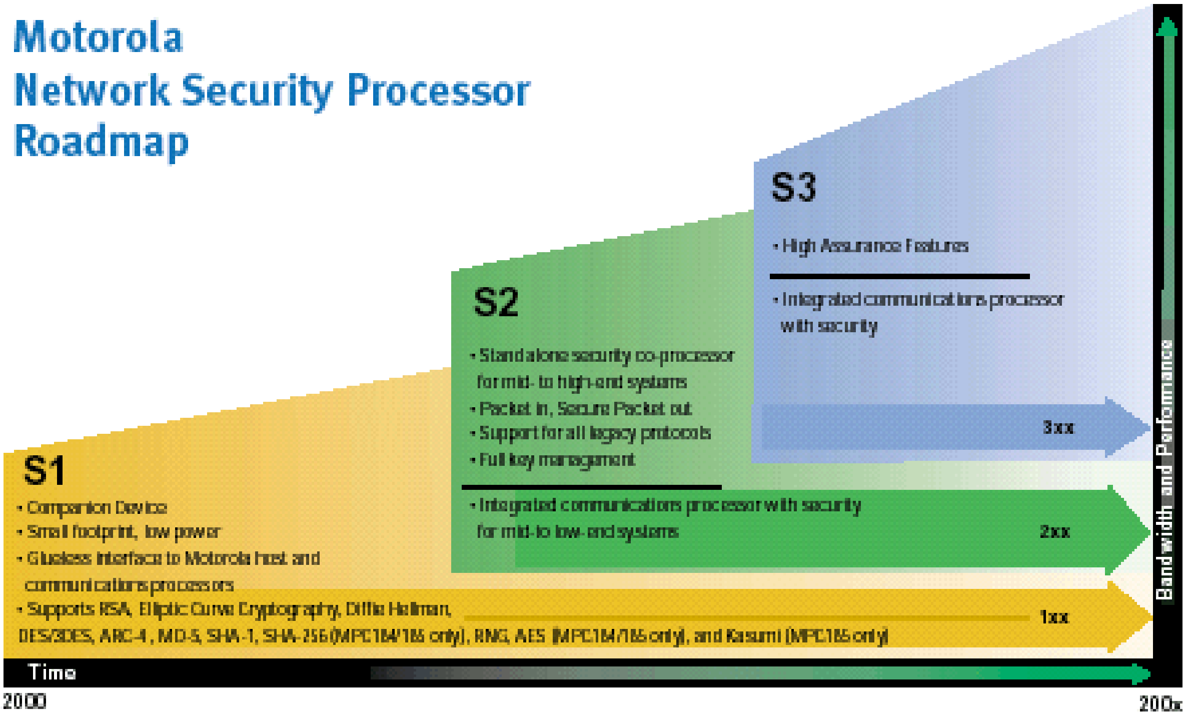

Motorola
Network Security Processor
Roadmap
S1
• Companion Device
• Small footprint, low power
• Glueless interface to Motorola host and communications processors
• Supports RSA, Elliptic Curve Cryptography, Diffie Hellman, DES/3DES, ARC-4, MD-5, SHA-1, SHA-256 (MPC184/185 only), RNG, AES (MPC184/185 only), and Kasumi (MPC185 only)
S2
• Standalone security co-processor for mid- to high-end systems
• Packet in, Secure Packet out
• Support for all legacy protocols
• Full key management
• Integrated communications processor with security for mid-to low-end systems
S3
• High Assurance Features
• Integrated communications processor with security
3xx
2xx
1xx
Time
2000
200x
Bandwidth and Performance

Figure 4-1. Motorola Security Roadmap

4.1 Motorola's S1 Family of Security Processors

Motorola's S1 Family was designed with the awareness that security has not been a driving force in system design, but that vendors will need to start migrating their designs to be more secure. For example, the growing importance of VPN services has made IPSec support almost mandatory in enterprise, access, and edge equipment. Systems that were more than adequate for insecure routing are unable to offer VPN services, even to select customers, without dramatically reducing system throughput.

By offering small footprint, low power coprocessors that gluelessly interface to Motorola host and communications processors already in many of these systems, Motorola offers system designers an upgrade path to significant VPN support. System software is similarly easy to upgrade. The S1 Family device drivers are supported under a number of third-party security stacks, and are also available directly to customers for porting into their current operating system (OS). The S1 Family of security processors is additional proof of Motorola's commitment to time-tomarket and time-in-market.

The family has four members: the MPC180, MPC184, MPC185 and MPC190. All members of this family are more accurately described as security coprocessors, in that the system host processor performs Security Policy conformance checking, and Security Association look-up. When the host determines that a packet requires security services, the host calls the device drivers of the security coprocessor, "waits" for the coprocessor to complete the security transformation, and then forwards the packet on-ward or upward.

NOTE

All performance estimates provided for these members are based on 3DES-HMAC-SHA-1, 1500 byte packets, and are measured from plaintext in memory to ciphertext + HMAC back in memory, and include all security processor set-up overhead, including key and context loading and unloading. Motorola includes all set-up and I/O overhead in its performance calculations to provide system designers with realistic system performance numbers, however host CPU loading (an application and operating system dependency) may effect actual results.

All members of the S1 family have an on-chip Random Number Generator, and support the following algorithms: DES, 3DES, ARC-4, MD-5, SHA-1, RSA, Elliptic Curve Cryptography, and Diffie-Hellman. The MPC184 and MPC185 additionally support AES (128, 192, 256-bit keys) and SHA-256. The MPC185 additionally supports the Kasumi security suite for 3G wireless equipment.

4.1.1 MPC180

The MPC180 is the first member of the S1 family. It is a low cost device, designed for use with the PowerQUICC and PowerQUICC II integrated communications processors. A PowerQUICC + MPC180 chipset is capable of up to 10Mbps, making it an ideal combination for SOHO routers with broadband connections. When used with the PowerQUICC II, the MPC180 interfaces to the 32-bit local bus, and the chipset can achieve 45Mbps.

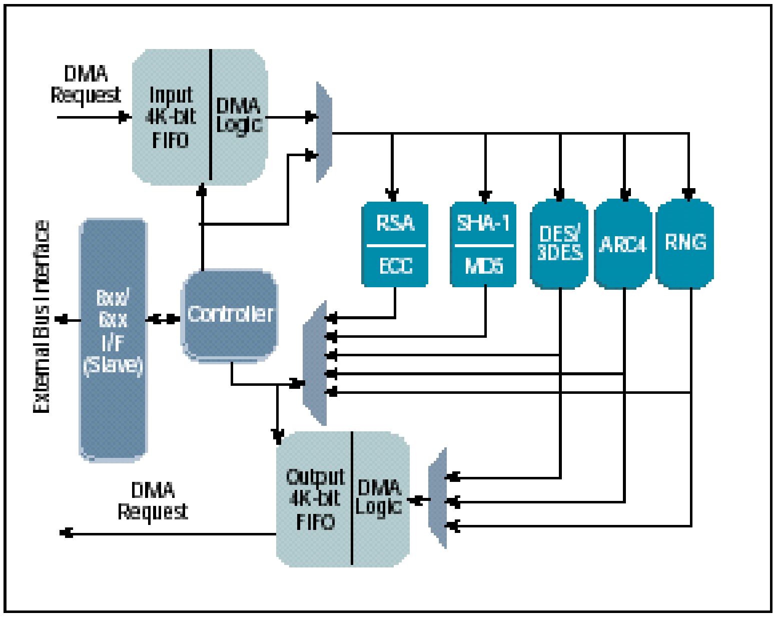


Figure 4-2. Motorola MPC180 Block Diagram

4.1.2 MPC184

The MPC184 security processor offers PowerQUICC customers a migration path to significantly higher performance (80Mbps), while also adding support for AES. The MPC184 has a mode-selectable interface to 32-bit PCI, allowing it to offer equivalent acceleration to systems with PCI, including systems built with Motorola host processors with integrated PCI, such as the popular MPC824x family, and new versions of PowerQUICC II (MPC8250/8265).

The MPC184 has bus mastering capability on both the PowerQUICC system bus and on PCI. When the host has a task for the MPC184, the host creates a descriptor and passes a pointer to that descriptor to one of four cryptochannels on the MPC184. Each channel maintains a descriptor ring, allowing four cryptographic processes to run in parallel. These channels have programmable prioritization levels, allowing the system designer to assign a packet to high, medium, normal, or low priority descriptor queues, and to define the relative weighting of each of those queues. This is an important feature for systems implementing differentiated services in a VPN environment.

The 8KB of on-chip general purpose RAM can be used for storage of ~250 keys, reducing the amount of bus traffic generated doing context switching. The gpRAM is actively zeroed on a hard reset of the MPC184, allowing for a degree of tamper protection.

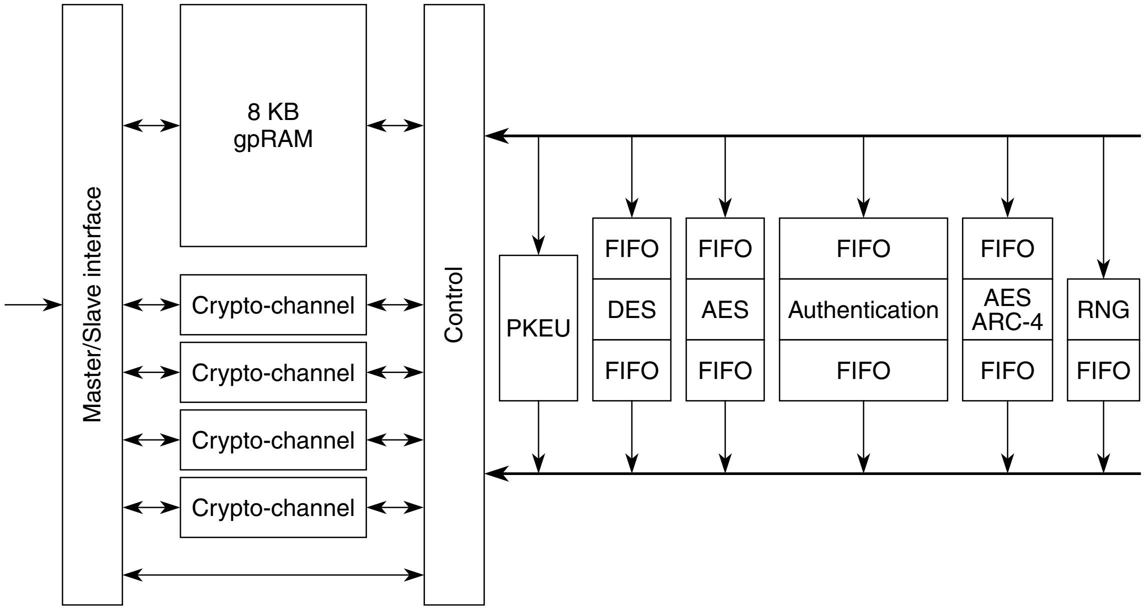


Figure 4-3. Motorola MPC184 Block Diagram

4.1.3 MPC185

The MPC185 has a PowerPC 60x bus interface, allowing it to gluelessly connect to the 64-bit CPU bus in systems built with PowerQUICC II communications processors and Motorola host processors implementing the PowerPC architecture, including the MPC755 and MPC7410. The MPC185 also has four channels with programmable arbitration, and 32KB of gpRAM. As the block diagram indicates, the MPC185 has multiple iterations of the execution units that perform the low-level algorithms. This, along with the 64-bit and up to 100MHz 60x interface, allows the MPC185 to provide performance of up to 400Mbps.

The MPC185 is unique in the industry for its acceleration of Kasumi, the 3G wireless security suite. Future 3G handsets will include Kasumi acceleration to enable the handset to accept encrypted data at up to 2Mbps. The MPC185 provides 3G infrastructure designers with a high-end solution for this emerging security requirement.

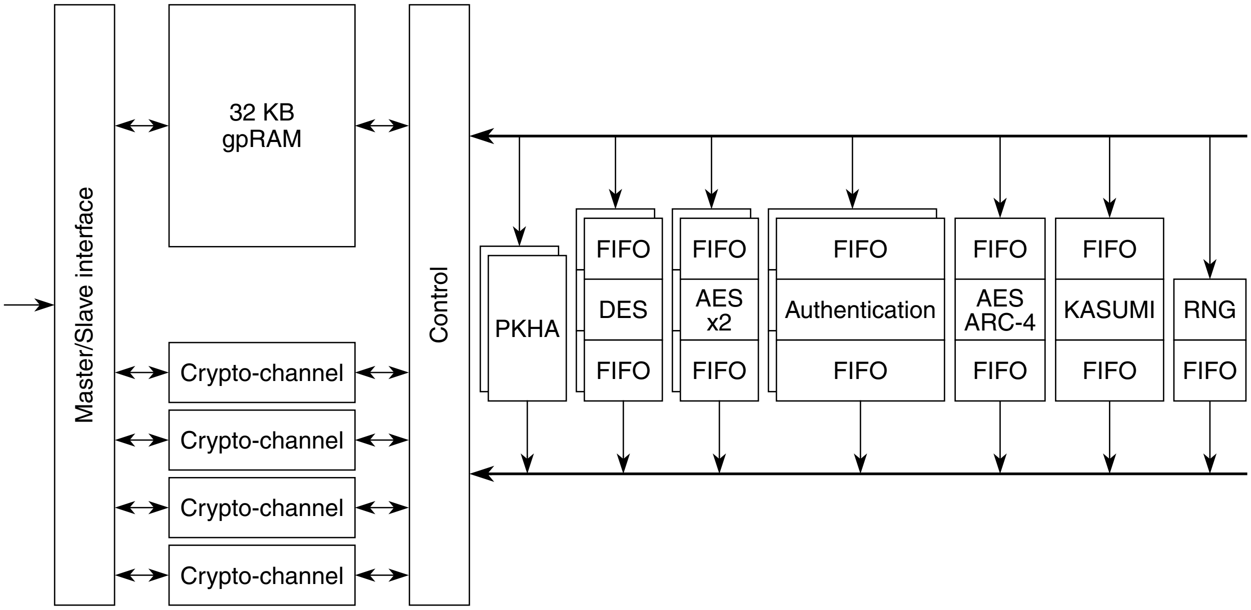


Figure 4-4. Motorola MPC185 Block Diagram

4.1.4 MPC190

The MPC190 is designed to off-load computationally intensive security functions, such as key generation and exchange, authentication, and bulk encryption from Motorola processors including the PowerQUICC II communications processors with integrated PCI (MPC8265, MPC8266), or from any processor through the use of a PCI bridge chip. The PCI interface is 32/64-bit, up to 66MHz, and the multiple iterations of each execution unit allow for all nine crypto-channels to perform concurrent cryptographic operations. This allows performance to reach 600Mbps. The MPC190 has significant key exchange capability, through use of six Public Key unit.

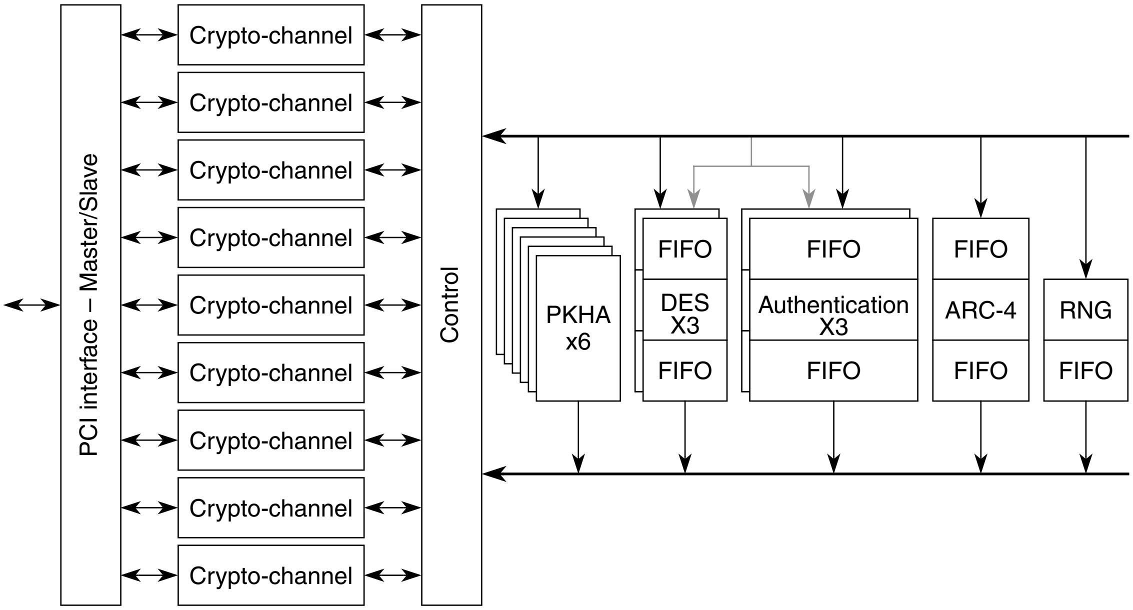


Figure 4-5. Motorola MPC190 Block Diagram

4.2 Motorola's S2 and S3 Families of Security Processors

Motorola's S1 Family enables a type of encryption architecture often referred to as "look-aside" encryption. Lookaside refers to the fact that the host processor is the first device to inspect the packet, and if the packet needs to be encrypted and authenticated, the host passes the packet to a coprocessor. As security applications require faster processing speeds (OC-12 and higher), this type of architecture is less effective.

An in-line security architecture, one in which a security device sits in the data path and makes encryption/authentication decisions without the assistance of an external host, enables security processing on the fast path, and can be used with higher-performance network processors. The goal of the S2 Family of Security Processors is to create a single chip, in-line security sub-system for high performance applications. Additionally, future Motorola communications processors with integrated security blocks will have many common features with S2 devices, but will act as a secure system-on-a-chip, rather than as a security sub-system. Until such devices are available, and in cases where a Motorola security processor does not meet the needs of a Motorola Network processor, Motorola is engaging with Smart Networks Alliance members to provide high-end, in-line security processing for the C-Port Network Processor Family.

S3 Family products will add high assurance features to the S2 family to help migrate networking equipment toward truly secure platforms. High assurance security processors provide protection against malicious insiders and against outside attacks that are able to get around other access controls. Motorola's significant heritage in assurance technology, along with a strong communications processor portfolio, uniquely positions us to introduce S3 products as market and legal conditions warrant.

Part V Motorola Security Processor Application Examples

As shown in Figure 5-1, Motorola's security processor solutions are compatible with the complete Smart Networks suite of communications processors. This section covers a few specific implementations including the communications processors and security processors.

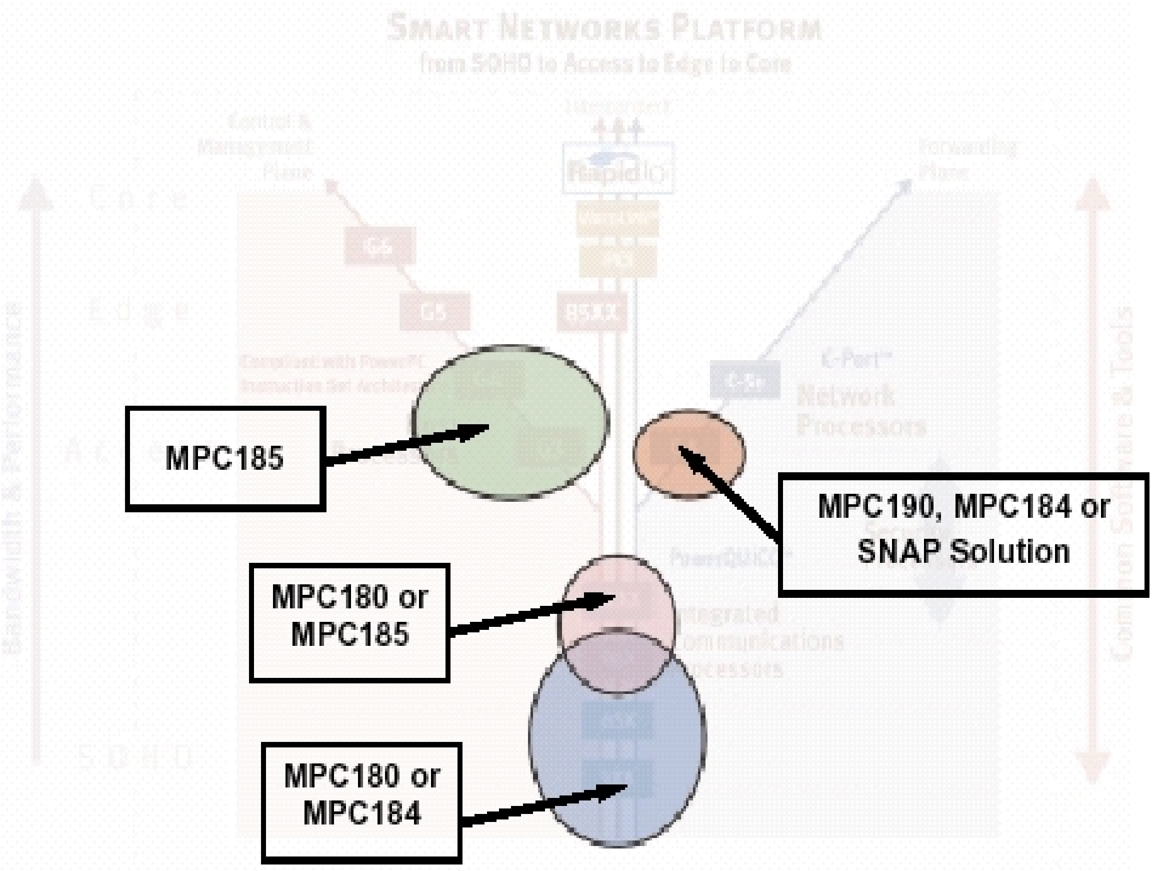

SMART NETWORKS PLATFORM
from SOHO to Access to Edge to Core
Interconnect
Control & Management Plane
RapidIO
Forwarding Plane
Core
Edge
Access
SOHO
G4
G5
85XX
Compliant with PowerPC Instruction Set Architecture
C-5e
C-Port™ Network Processors
PowerQUICC
Integrated Communications Processors
Bandwidth & Performance
Common Software & Tools
MPC185
MPC190, MPC184 or SNAP Solution
MPC180 or MPC185
MPC180 or MPC184

Figure 5-1.Smart Networks Communications Processors and Security Processors

5.1 PowerQUICC and MPC180 / MPC184

Motorola's MPC8xx PowerQUICC family moves the entire price/performance curve for SOHO routers to a new level with the MPC8xx + MPC180/184, which integrates Security, ATM, Ethernet, and USB functionality with a high-performance PowerPC ISA core for a very cost effective low-end VPN chipset. The proven PowerQUICC family architecture includes a versatile memory controller and a separate on-chip communications processor module, which offloads peripheral tasks from the core, such as the traffic handling of ATM via the UTOPIA port, Ethernet, and USB. In addition, the established code base and broad third-party support from Motorola's Smart Network Alliance members further enable cost-efficient solutions and accelerated time-to-market for low-end networking equipment suppliers.

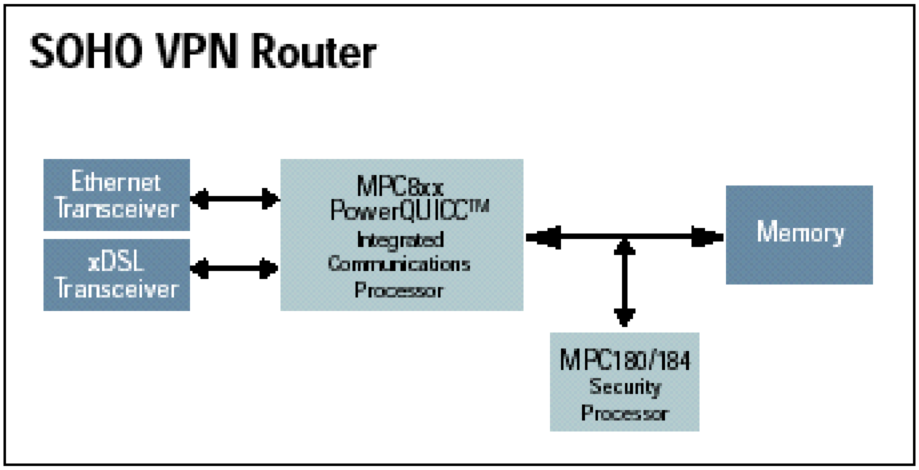

SOHO VPN Router
Ethernet Transceiver
xDSL Transceiver
MPC8xx PowerQUICC™ Integrated Communications Processor
Memory
MPC180/184 Security Processor

Figure 5-2. PowerQUICC and MPC180/MPC184 Board Design

The MPC180 Security Processor is easily integrated into systems already using Motorola's processors, and uses existing system memory, resulting in significant savings of both board space and system cost. The MPC184 provides a significant performance boost with the inclusion of 8xx bus mastering, and single pass processing for bulk encryption plus authentication. Both the MPC180 and MPC184 include Public Key acceleration and include on-chip random number generators, making them the most full featured security solutions for SOHO VPN applications.

5.2 MPC824x and MPC184

Wireless gateways connect wireless users into the wired LAN, an access point that requires a security solution. The MPC824x family can provide a streamlined wireless gateway solution, and when combined with the MPC184, a secure one. The MPC184 easily integrates with the PCI bus of the MPC824x to process the sophisticated security protocols, such as WEP, IPSec, SSL and Wireless Transport Layer Security (WTLS). By accelerating both wireless and wireline security protocols, the MPC824x + MPC184 chipset can enable 802.11 Wireless Access Points to include WAN interfaces, and secure those WAN interfaces with IPSec.

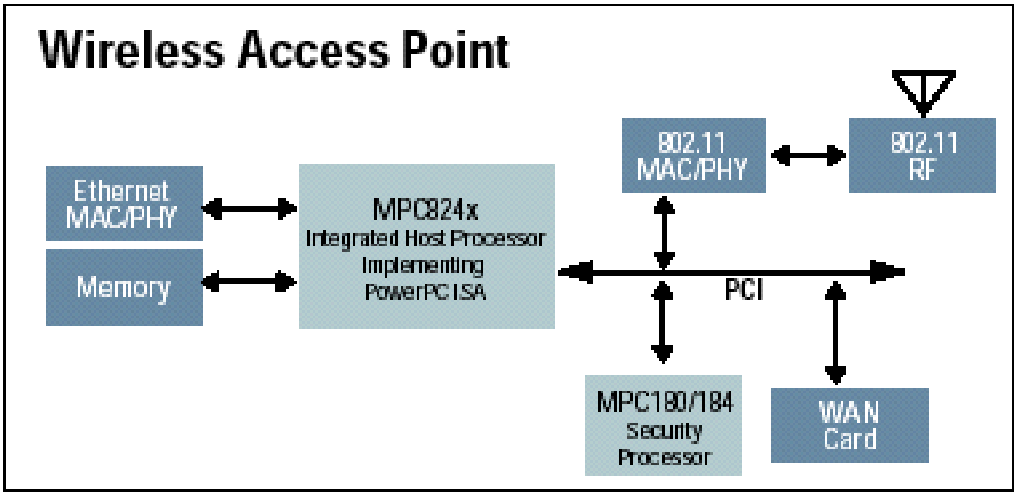

Wireless Access Point
Ethernet MAC/PHY
Memory
MPC824x Integrated Host Processor Implementing PowerPC ISA
802.11 MAC/PHY
802.11 RF
PCI
MPC180/184 Security Processor
WAN Card

Figure 5-3. MPC8245 and MPC184 Board Design

5.3 PowerQUICC II and MPC185

In this example, the MPC8260 PowerQUICC II can support OC-3 ATM rates, T3/E3, or four T1 framers on the Time Division Multiplexing (TDM) side, while connecting to several 10/100BASE-T Ethernet interfaces on the LAN side. Its powerful Communications Processor Module (CPM) can be programmed to support several other popular protocols, and also provides a direct interface to most physical layer (PHY) devices. In ATM mode, the local bus is used to store connection tables for active ATM connections. Additional ports remain available for system management functions.

The MPC185 Security Processor is easily integrated into PowerQUICC II systems via the 60x bus. The MPC185 achieves its high performance through 60x bus mastering, and immediate access to system memory. By avoiding data transfers across bridges and secondary buses, the MPC185 provides PowerQUICC II system designers with the ultimate security chipset for mid-range VPN applications.

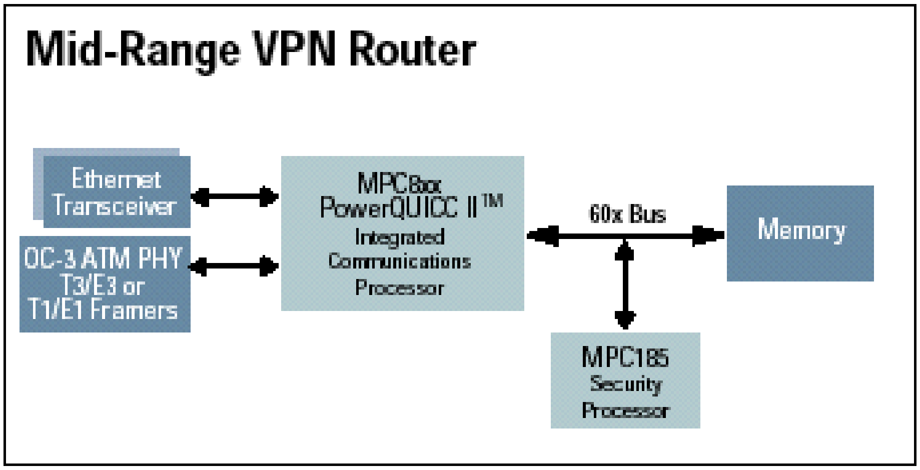

Mid-Range VPN Router
Ethernet Transceiver
OC-3 ATM PHY T3/E3 or T1/E1 Framers
MPC8xx PowerQUICC II™ Integrated Communications Processor
60x Bus
Memory
MPC185 Security Processor

Figure 5-4. PowerQUICC II and MPC185 Board Design

5.4 C-Port Network Processor Family and MPC190 / MPC184

When the only encryption requirement is related to control traffic, it is possible to interface the low-cost, small footprint MPC190 or MPC184 security processor to a C-Port Family network processor. This configuration works well when the data rate of secure traffic is relatively low because the PCI interface will also be carrying all host to NP traffic. Future generations of Motorola security processors will be more optimized for in-line security processing with the C-Port Family.

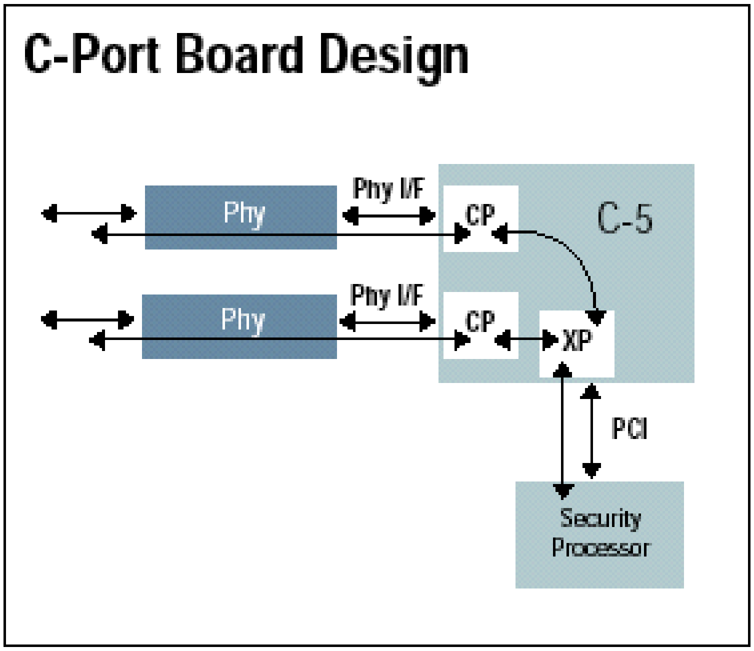


Figure 5-5. C-Port Network Processor and MPC190/MPC184 Board Design

Through the Motorola Smart Networks Alliance program, Motorola continues to build alliances where it makes sense. The performance requirements of a security solution for the C-Port Network Processor Family has led to an alliance with Corrent, the developers of high-performance, standards-based network security silicon chips for the high speed internet. Through this alliance, vendors can be assured of interoperability between the C-Port Network Processor Family and Corrent's Socket Armor™ CR7020 SSL Security Processor Family, providing fast in-line security processing.

Part VI Summary

IPSec and other security protocols are nearly impenetrable barriers to thieves and vandals, and other malicious parties that openly prowl the public network. Proper application of encryption and authentication can greatly reduce the very real threats associated with transmission of confidential user and control traffic. The greatest barrier to the application of network security, however, is the tremendous performance degradation encountered when running security protocols on general-purpose hardware. The end user should not be forced to chose between an insecure broadband Internet experience and a secure "dial-up" experience. Similarly, system designers should not be expected to re-architect their systems to accommodate security acceleration.

Motorola is delivering to its customers the S1 Family of full-featured security processors that provide glueless interfaces to Motorola host and communications processors. These security processors offer the smallest board footprint, the lowest power, and the easiest to integrate software, making adding security to network devices a painless process. And Motorola's strategy of seamless integration of security into Smart Networks will continue into the future.

Part VII References

[HMAC] RFC 2104 'HMAC: Keyed-Hashing for Message Authentication'

[IPSEC] RFC 2401 'Security Architecture for the Internet protocol'

[AH] RFC 2402 'IP Authentication Header'

[MD5] RFC 2403 'The Use of HMAC-MD5-96 within ESP and AH'

[SHA-1] RFC 2404 'The Use of HMAC-SHA-1-96 within ESP and AH'

[DES] RFC 2405 'The ESP DES-CBC Cipher Algorithm With Explicit IV'

[ESP] RFC 2406 'IP Encapsulating Security Payload (ESP)'

[DOI] RFC 2407 'The Internet IP Security Domain of Interpretation for ISAKMP'

[ISAKMP] RFC 2408 'Internet Security Association and Key Management Protocol (ISAKMP)'

[IKE] RFC 2409 'The Internet Key Exchange (IKE)'

[TLS] RFC 2246 'The TLS Protocol Version 1.0'

[CBC] RFC 2451 'The ESP CBC-Mode Cipher Algorithms'

[RIPE] RFC 2851 'The Use of HMAC-RIPEMD-160-96 within ESP and AH'

Part VIII Revision History

Table 8-1 summarizes the revision history of this document.

Table 8-1. Revision History

Revision No.	Substantive Change(s)
0	Initial release.
1.0	Added revision history Updated with new template. Diagrams—2.5, 2.6, 4.3,4.4, and 4.5 are corrected.

THIS PAGE INTENTIONALLY LEFT BLANK

THIS PAGE INTENTIONALLY LEFT BLANK

HOW TO REACH US:

USA/EUROPE/LOCATIONS NOT LISTED:

Motorola Literature Distribution
P.O. Box 5405, Denver, Colorado 80217
1-480-768-2130
(800) 521-6274

JAPAN:

Motorola Japan Ltd.
SPS, Technical Information Center
3-20-1, Minami-Azabu Minato-ku
Tokyo 106-8573 Japan
81-3-3440-3569

ASIA/PACIFIC:

Motorola Semiconductors H.K. Ltd.
Silicon Harbour Centre, 2 Dai King Street
Tai Po Industrial Estate, Tai Po, N.T., Hong Kong
852-26668334

TECHNICAL INFORMATION CENTER:

(800) 521-6274

HOME PAGE:

www.motorola.com/semiconductors

Information in this document is provided solely to enable system and software implementers to use Motorola products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits or integrated circuits based on the information in this document.

Motorola reserves the right to make changes without further notice to any products herein. Motorola makes no warranty, representation or guarantee regarding the suitability of its products for any particular purpose, nor does Motorola assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. “Typical” parameters which may be provided in Motorola data sheets and/or specifications can and do vary in different applications and actual performance may vary over time. All operating parameters, including “Typicals” must be validated for each customer application by customer’s technical experts. Motorola does not convey any license under its patent rights nor the rights of others. Motorola products are not designed, intended, or authorized for use as components in systems intended for surgical implant into the body, or other applications intended to support or sustain life, or for any other application in which the failure of the Motorola product could create a situation where personal injury or death may occur. Should Buyer purchase or use Motorola products for any such unintended or unauthorized application, Buyer shall indemnify and hold Motorola and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Motorola was negligent regarding the design or manufacture of the part.

MOTOROLA