

SEGURANÇA EM PROCESSADORES DE REDE

MUZZI, Fernando Augusto Garcia
TAMAE, Rodrigo Yoshio; ROSA
Adriano Justino

Docentes da Faculdade de Ciências Gerenciais e Jurídicas de Garça – FAEG/Garça
fagmuzzi@yahoo.com.br ; rytamae@yahoo.com.br; adriano@faef.br

RESUMO

Os processadores de rede têm fundamental importância para a comunicação de dados devido ao considerável aumento da velocidade de transmissão. No entanto, é necessária a implementação de segurança para os processadores de rede, ou seja, a criptografia de pacotes para garantir a segurança da informação.

Palavras-chave: Processadores de rede; segurança.

ABSTRACT

The network processors have fundamental importance for data communication by increase grow up transmission speed. However, it is necessary safety implementation for network processors to package's cryptography to safety information security.

Keywords: Network processor; security.

1. INTRODUÇÃO

A Internet está no dia a dia das pessoas, empresas e instituições de ensino. Seu uso tem acarretado um congestionamento dos links de transmissão. Os principais responsáveis são os gateways ("roteadores"), Os quais confinam o tráfego entre redes.

Os processadores de rede estão sendo objeto de estudo nas universidades e empresas. Estes processadores surgiram para melhorar a qualidade de serviços (*QoS: Quality of Services*) (TANEMBAUM, 1999).

O tempo de processamento dos pacotes de rede é mais rápido usando os processadores de rede (TANEMBAUM, 1999). É necessário aumentar a

capacidade de processamento dos pacotes para que não haja congestionamento e excessiva utilização da largura de banda.

A segurança da informação é importante para que os pacotes não possam ser lidos por pessoas não autorizadas. Assim, torna-se necessária a criação de mecanismos que possam impedir que o pacote seja lido. Existem padrões e normas de criptografia que podem ser implementadas em processadores de rede.

Os processadores geralmente foram baseados em propósito geral e sua arquitetura era parecida com a dos computadores pessoais. Ao invés disso, os processadores de rede foram projetados utilizando modelos de arquiteturas (PATTERSON, 1997), sendo o modelo mais utilizado o ASIP (*Application Specific Instruction Set Processor*) e o SoC (*System-on-Chip*) para agregar técnicas de projeto RISC (*Reduced Instruction Set Computing*) e ter um desempenho computacional maior.

Algumas empresas já desenvolveram processadores de redes, entre elas pode-se citar a Lucent e Agere (AGERE SYSTEM, 2001), Intel (INTEL, 2002), IBM (POWER NP, 2003).

Os processadores de rede têm fundamental importância para a comunicação de dados, já que a velocidade de transmissão de dados tem aumentado consideravelmente. No entanto é necessária segurança para os processadores de rede, ou seja, a criptografia de pacotes, para garantir a segurança da informação. Com a implementação de um módulo de criptografia o processador de rede poderá receber e transmitir pacotes criptografados.

Criptografia é a arte ou ciência de escrever em cifra, de forma a permitir normalmente que apenas um destinatário a decifre e compreenda. Quase sempre a descryptografia requer uma chave, uma informação secreta disponível ao destinatário.

No âmbito da tecnologia de informação, a criptografia é importante para que se possa garantir a segurança em todo o ambiente computacional que necessite de sigilo em relação às informações.

Existem também processadores de rede com módulo de segurança que realizam criptografia, entre eles podemos citar o IPX2800 da Intel.

O processador de rede IXP2800 é projetado para gateways, pontos de acesso wireless roteadores e switches SME, com suporte a criptografia.

2. IXP2800: PROCESSADOR DE REDE COM IMPLEMENTAÇÃO DE SEGURANÇA

Os projetos precedentes adicionaram a segurança à rede através de um co-processador ou de um processador de segurança. Os processadores de segurança podem realmente escalar as taxas de dados mais elevadas, mas devem executar muitas das mesmas funções que o processador de rede faz para conseguir a taxa de dados elevada.

O IXP2800 tem capacidade de processar pacotes da rede em até 10 Gigabits por segundo, com um baixo custo em relação consumo e potência.

Na figura 1 podemos visualizar dois módulos de responsáveis pela criptografia de pacotes no processador de rede IPX2800. O Crypto Unit 0 e o Crypto unit 1.

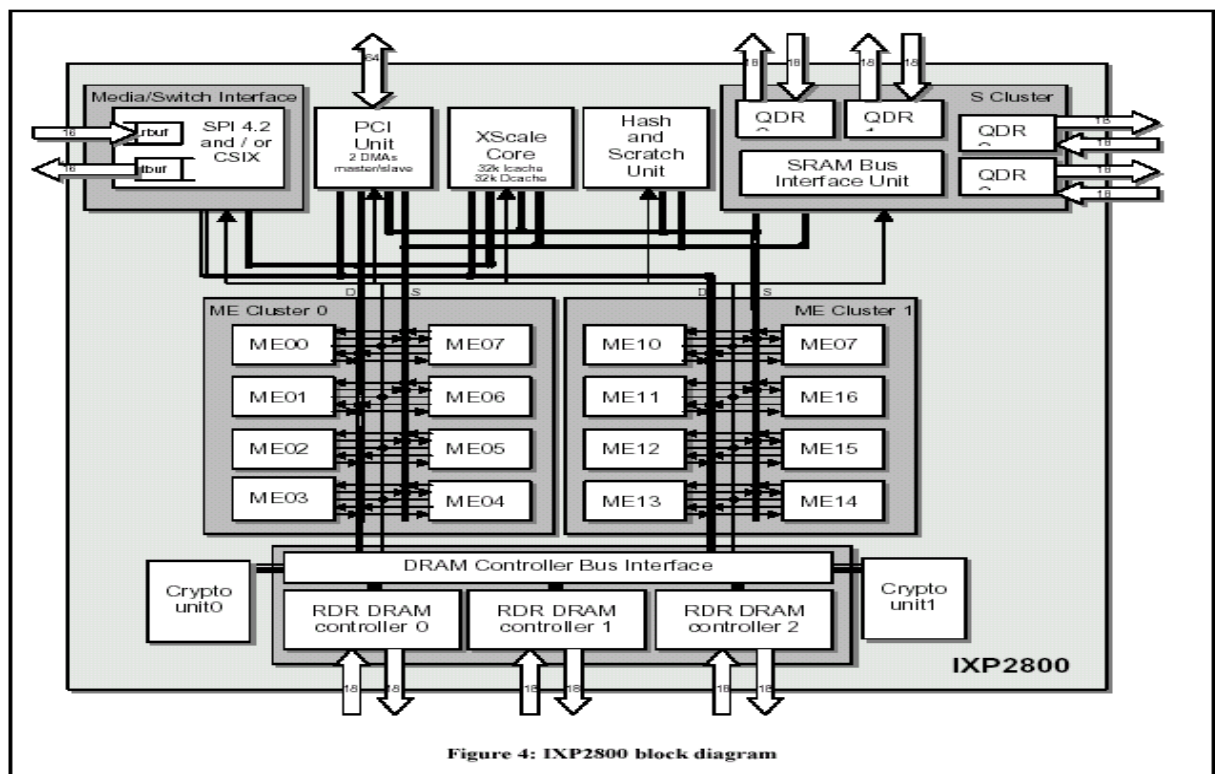


Figura 1 – Arquitetura do IXP2800 (INTEL, 2002)

3. CONCLUSÕES

Existem diversos processadores de rede para uso comercial e vários fabricantes e modelos específicos para trabalho em rede com a finalidade de melhorar o QoS (*Qualidade de serviços*), melhorar o tráfego e a transição de dados evitando assim gargalos, principalmente, em roteadores e switches que acabam sendo os principais componentes em uma rede. Os processadores de rede podem ser implementados em um SoC (*System on Chip*), um dispositivo reconfigurável, ou mesmo pode ser implementado diretamente em um chip em um roteador ou switch.

Os processadores de rede foram criados para eliminar o gargalo do tráfego da rede e efetuar o tratamento de pacotes. Os roteadores e switch ativos, por exemplo, são aqueles que verificam o cabeçalho do pacote e processam o mesmo analisando esse cabeçalho. Com o aumento do tráfego da rede e a Internet cada vez mais presente torna-se necessário à criação de processadores de rede com a finalidade específica de aumentar a performance da troca de pacotes.

Existem diversos processadores de rede comerciais, mas poucos com implementação de algoritmos de segurança usando criptografia no processamento de pacotes. Por isso a necessidade de criação de um módulo de segurança para processadores de redes.

3. REFERÊNCIAS BIBLIOGRÁFICAS

AGERE SYSTEM. **Fast Pattern Processor (FPP) Product Brief**, April 2001, Disponível em: <<http://www.agere.com>>. Acesso em: 20 de Set. 2003.

POWER NP. **PowerNP NP4GS3 Databook**. Disponível: <<http://www.ibm.com>>. Acesso em: 15 de Out. 2003.

INTEL IXP 1200. **IXP 1200 - Network Processor**. Datasheet, May 2000. Disponível em: <<http://www.intel.com>>. Acesso em: 18 de Dez. 2003.

INTEL. **Packet SONET excedente: Conseguindo o pacote de 10 Gigabit/sec que processa com um IXP2800** *jornal da tecnologia de Intel*. Edição 3 do Vol. 6. Agosto 2002. Disponível em:

<<http://developer.intel.com/technology/itj/2002/volume06issue03>>.
Acesso em: 20 de Set. 2003.

TANEMBAUM, A. S. **Redes de Computadores**. Editora Campus, 3º Edição. 1999.

PATTERSON, D.A. **Computer Organization and Design: The Hardware/Software interface**. Morgan Kaufmann Publisher, 1997.