

Beschleunigung Virtueller Privater Netze durch Netzwerkprozessoren

CeBIT 2003

Hannover, 18. März 2003

Stephan Groß <gross@rn.inf.tu-dresden.de>
Ralf Lehmann <lehmann@rn.inf.tu-dresden.de>

Technische Universität Dresden
Fakultät Informatik, Institut für Systemarchitektur
Lehrstuhl Rechnernetze
D-01062 Dresden, Germany

Inhalt

— Motivation

— Stand der Technik

— Probleme

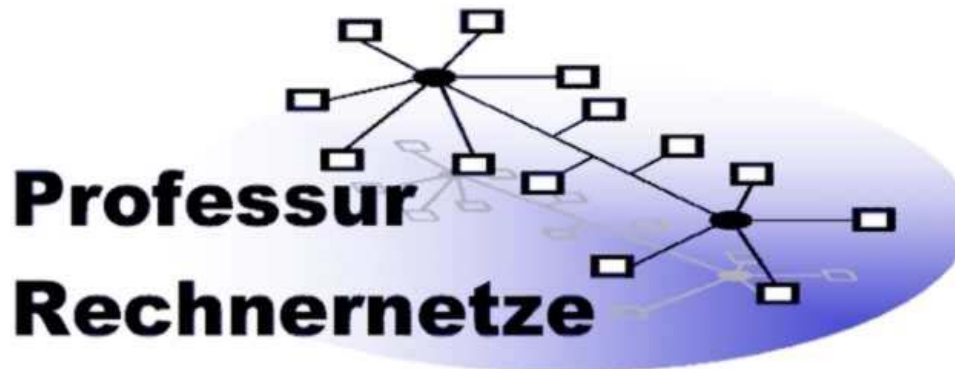
— Unsere Lösung

— Methodik

— Intel IXP

— Status

— Ergebnisse



- High Speed Networking und Multimedia
 - Flexible Kommunikationsplattformen für
 - Hardwarebeschleunigung von
- Middleware und Ubiquitous Computing
- Teleteaching and Teleworking



Inhalt

— Motivation

- Motivation

— Stand der Technik

- Stand der Technik

— Probleme

- Probleme

— Unsere Lösung

- Unsere Lösung

— Methodik

— Intel IXP

— Status

- Methodik
- Die Intel IXP Netzwerkprozessorfamilie
- Aktueller Stand der Arbeiten

— Ergebnisse

- Ergebnisse



Inhalt

— Motivation

— Stand der Technik

— Probleme

— Unsere Lösung

— Methodik

— Intel IXP

— Status

— Ergebnisse

Ungeschützte Datenübertragung im Internet

- Verlust der Vertraulichkeit
- Verlust der Datenintegrität
- Verlust Nutzerintegrität



Inhalt

— Motivation

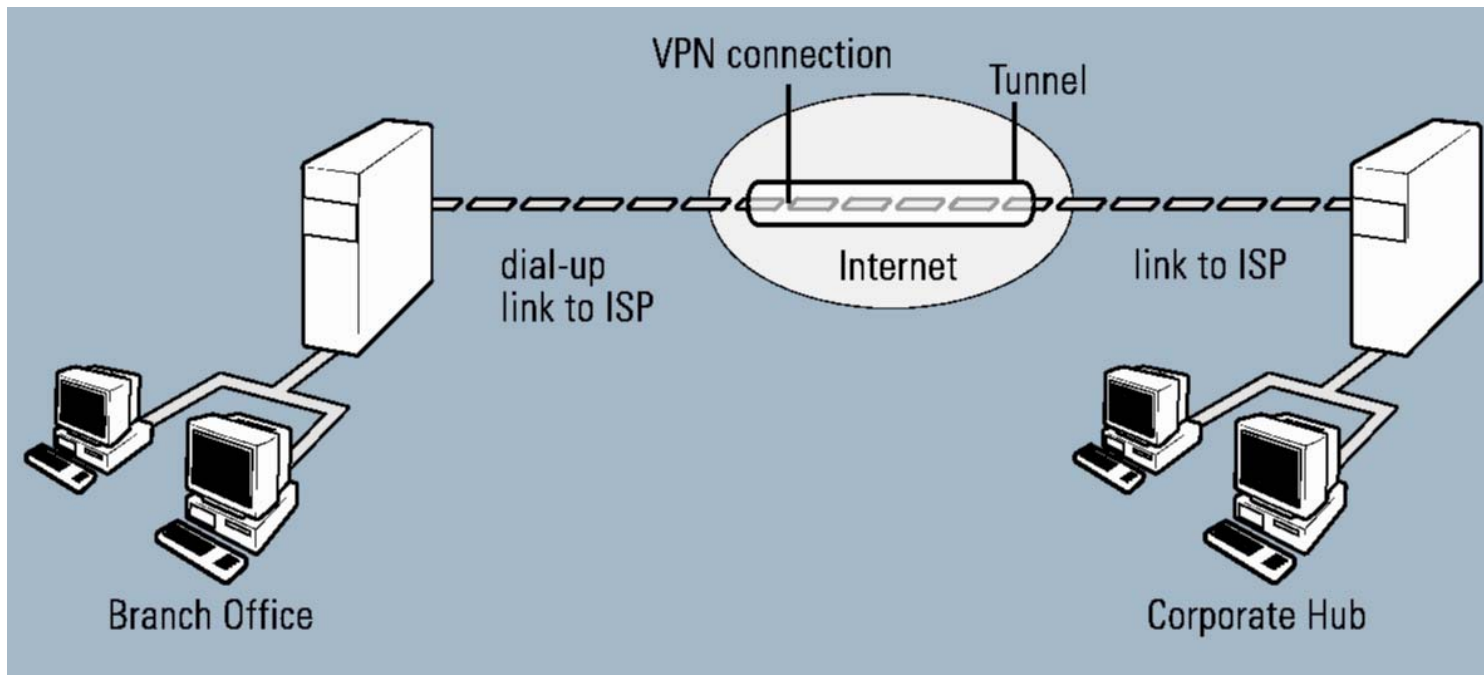
— Stand der Technik

— Probleme

— Unsere Lösung

- Methodik
- Intel IXP
- Status

— Ergebnisse



Inhalt

Motivation

Stand der Technik

Probleme

Unsere Lösung

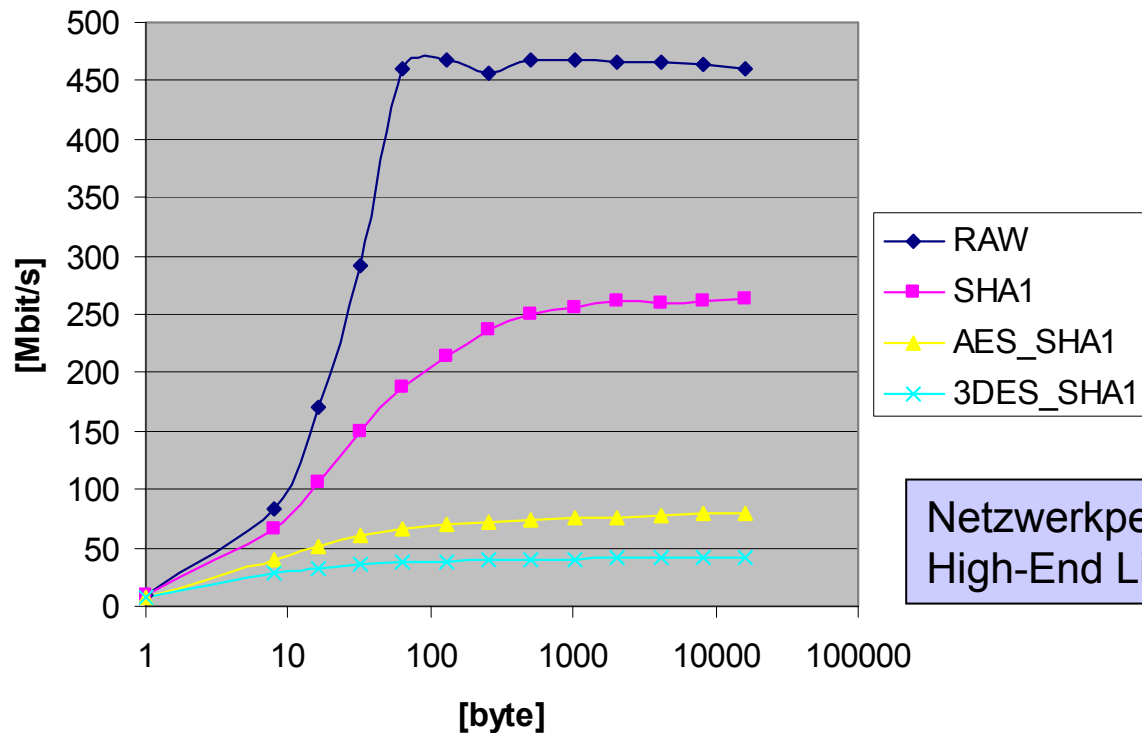
Methodik

Intel IXP

Status

Ergebnisse

- Schlechte VPN Performance mit reinen Softwarelösungen
- Hohe Kosten spezieller Hardware-Lösungen
- Fehlende Flexibilität reiner Hardware-Lösungen bei Anpassungen an neue Algorithmen und Techniken



Netzwerkperformance
High-End Linux



Inhalt

— Motivation

— Stand der Technik

— Probleme

— Unsere Lösung

— Methodik

— Intel IXP

— Status

— Ergebnisse

Netzwerkprozessorbasierte IPSec-Realisierung für VPN-Gateways

- **Zentrale Komponenten**
 - Intel IXP Netzwerkprozessor
 - Embedded Linux
 - IPSec-Implementierung
- **Ziele**
 - Unterstützung für MD5, SHA-1, 3DES, AES
 - Flexibel zu erweitern (z.B. IPv6)
 - Hochperformant und skalierbar bis 10 Gbit/s
 - Kosteneffektives Design



Inhalt

— Motivation

- Analyse der Linux IPSec Implementierung

— Stand der Technik

- Extrahierung des Datenpfades

— Probleme

— Unsere Lösung

- Portierung auf den IXP 1200 C Dialekt
- Optimierung der kryptographischen Algorithmen
- Integration in Linux IPSec Implementierung

— Methodik

— Intel IXP

— Status

— Ergebnisse



Inhalt

Motivation

Stand der Technik

Probleme

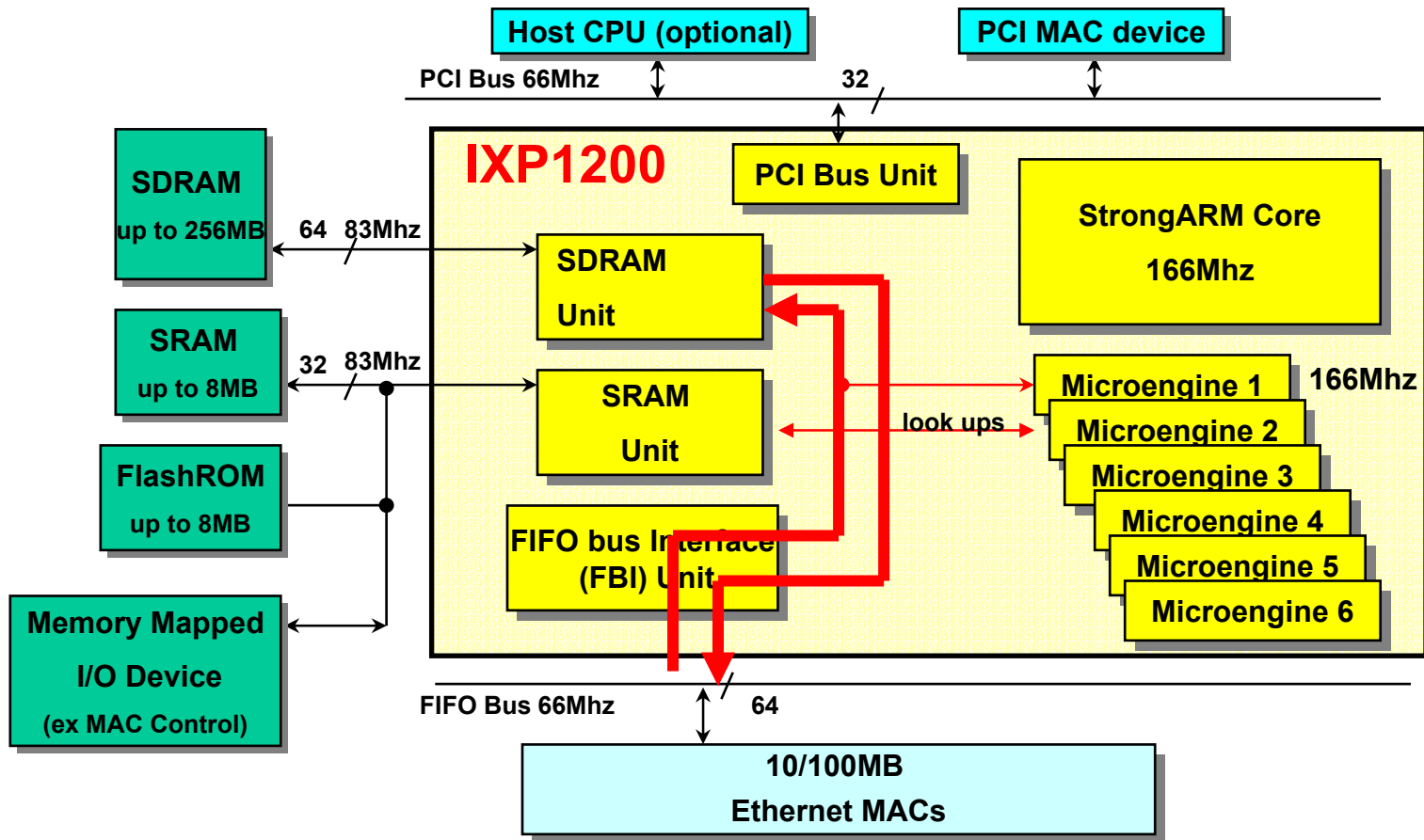
Unsere Lösung

Methodik

Intel IXP

Status

Ergebnisse





halt

- Motivation
- Stand der Technik
- Probleme
- Unsere Lösung
 - Methodik
 - Intel IXP
 - Status
- Ergebnisse

The screenshot displays the Intel IXP1200 Developer Workbench interface. The main window shows assembly code for a microengine, with instructions like `MD5STEP(F4, d, a, b, c, cin_r1[7] + 0x432aff97, 10);`. Below the code, there are comments in green: `/* context.buf[0] += a; context.buf[1] += b; context.buf[2] += c; context.buf[3] += d; */`. The bottom panel features a performance monitor with a table of microengine states and a timeline graph.

Microengine	PC	Condition Codes
Microengine 0	1723 [0]	I=0, <0, No carry
Microengine 1		
Microengine 2		
Microengine 3		
Microengine 4		
Microengine 5		

The performance monitor also includes a legend for threads (Thread0-7) and SDRAM access patterns (SDRAM Order, SDRAM Odd Bank).

Inhalt

— Motivation

— Stand der Technik

— Probleme

— Unsere Lösung

— Methodik

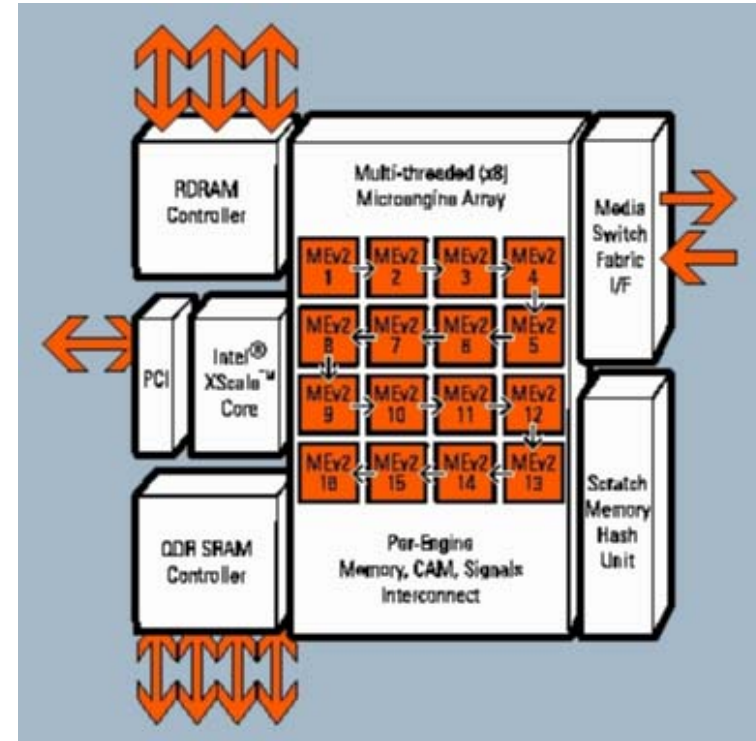
— Intel IXP

— Status

— Ergebnisse

Intel IXP2400 – Ausblick

- 8 Threads / 8 Micro Engines @ 600 MHz
- Lokaler Speicher 2560 Bytes
 - z.B. für S-Boxen moderner Verschlüsselungsalgorithmen
 - Ermöglicht die Implementierung von AES





Inhalt

— Motivation

— Stand der Technik

— Probleme

— Unsere Lösung

— Methodik

— Intel IXP

— Status

— Ergebnisse

- Analyse der Linux IPSec Implementierung **✓ OK**
- Extrahierung des Datenpfades **✓ OK**
- Portierung auf den IXP 1200 C Dialekt **Begonnen, AES und MD5**
- Optimierung der kryptographischen Algorithmen **Begonnen, AES und MD5**
- Integration in Linux IPSec Implementierung **Steht noch aus**



Inhalt

— Motivation

— Stand der Technik

— Probleme

— Unsere Lösung

— Methodik

— Intel IXP

— Status

— Ergebnisse

MD5

- Gute Performance
 - Single thread:
118 Mbit/s (MD5Transform)
 - Vergleich:
Pentium III, 1GHz: 250 Mbit/s
- Hohe Lokalität der Daten
- IXP1200 gut geeignet
- Ausblick:
weitere Optimierungen sollten
Performance verbessern

AES

- Erste Versuche problematisch
- IXP1200 ungeeignet
- Gründe:
 - Implementierung geht nicht
genügend auf Besonderheiten
der IXP-Architektur ein
 - Geringe Lokalität der Daten
verursacht hohe Kosten bei
Speicherzugriffen
- Ausblick: IXP2400



Fragen?



**Besuchen Sie uns
in Halle 11,
Stand D27 – S3**