DOI: 10.36910/6775-2524-0560-2020-40-24
УДК 004.272.4
Христинець Наталія Анатоліївна, ст.викладач
https://orcid.org/0000-0002-4836-7632
Чернящук Наталія Леонідівна, д.п.н., професор,
http://orcid.org/0000-0002-3178-8377
Міскевич Оксана Іванівна, асистент
https://orcid.org/0000-0002-5009-2391
Повстяна Ю.С., к.т.н., доцент
https://orcid.org/0000-0001-5426-4157
Довгонюк Микола Вікторович.
Луцький національний технічний університет.

ТЕХНОЛОГІЇ АПАРАТНОЇ ВІРТУАЛІЗАЦІЇ МІКРОПРОЦЕСОРІВ INTEL

Христинець Н.А., Чернящук Н.Л., Міскевич О. І., Повстяна Ю.С., Довгонюк М.В. Технології апаратної віртуалізації мікропроцесорів Intel. Розглянуті особливості структури мікропроцесорів архітектури Nehalem: контролер пам'яті, ієрархію кешу, TLB та організацію доступу до пам'яті. Подано технічні характеристики процесорів на сокеті LGA1156 в межах одного модельного ряду як результати тестів даної архітектури та досліджено методи організації віртуальної пам'яті.
Ключові слова: архітектура мікропроцесорів, Nehalem, Conroe, кеш, доступ до пам'яті, LGA1156, віртуалізація пам'яті.

Христинец Н.А., Чернящук Н.Л., Мискевич О. И., Повстяна Ю.С., Довгонюк Н.В. Технологии аппаратной виртуализации микропроцессоров Intel. Рассмотрены особенности структуры микропроцессоров архитектуры Nehalem: контроллер памяти, иерархию кэша, TLB и организации доступа к памяти. Подано технические характеристики процессоров на сокете LGA1156 в пределах одного модельного ряда как результаты тестов данной архитектуры и исследованы методы организации виртуальной памяти.
Ключевые слова: архитектура микропроцессоров, Nehalem, Conroe, кэш, доступ к памяти, LGA1156, виртуализация памяти.

Khrystynets N., Cherniashchuk N., Miskevych O., Yu. Povstiana., Dovgonyuk M. Technology of hardware virtualization of microprocessors Intel. The features of the Nehalem architecture of microprocessors are considered: memory controller, cache hierarchy, TLB and memory access organization. The technical characteristics of the processors on the LGA1156 socket within one model range are presented as the results of tests of this architecture and the methods of virtual memory organization are investigated.
Keywords: microprocessor architecture, Nehalem, Conroe, cache, memory access, LGA1156, memory virtualization.

Постановка проблеми:

У сучасній стрімкій індустрії IT велика кількість досліджень присвячена перспективним технологіям, що дозволяють забезпечити енергоощадність комп'ютерної техніки, тим більше питання екології і збереження енергоресурсів сьогодні є дуже популярним і актуальним.

Однією з технологій, яка сьогодні набула широкого використання та має позитивні відгуки світової спільноти як в комерційній сфері, так і у навчальному процесі, є віртуалізація. Досліджено розробку компанії Intel, яка включає в себе на даний час можливість віртуалізації ЦП, віртуалізації пам'яті, функції віртуалізації введення-виводу, технології Intel GVT, віртуалізації систем безпеки та мережевих функцій на прикладі тестового стенду . На даний момент, це потрібні та корисні інструменти для користувачів ПК.

Аналіз досліджень.

Серед вбудованих технологій мікропроцесорів явище віртуалізації висвітлене у багатьох сучасних і зарубіжних дослідженнях [1-3], обговорюється на світових форумах та конференціях [4-5]. Американські IT-фахівці Werner Fisher, Thomas Krenn у своїх роботах зазначають, що сучасна віртуалізація Intel здійснює абстрагування обладнання, що має спільний доступ до ресурсів комп'ютерної системи у випадку робочого навантаження. Офіційно компанія Intel заявляє, що «на загальному віртуалізованому обладнанні можна поєднувати різні робочі навантаження при збереженні повної ізоляції один від одного, вільної міграції по інфраструктур і масштабування в міру необхідності.

Розріязняють програмну, апаратну та серверну віртуалізацію.

Прикладом програмної віртуалізації може бути усім відома пісочниця антивірусних програм, яка фактично використовується для захисту локальної системи під час виконання невідомого або шкідливого коду. Вона забезпечує цей захист, блокуючи критичні операції, або виконуючи підозрюваний код у віртуальному середовищі. Таке віртуальне середовище дозволяє користувачу безперешкодно контролювати зловмисне програмне забезпечення і запобігати його наслідків.

З ростом прогресуючих серверних технологій багато компаній досліджували роботу серверних процесорів. Вони виявили, що переважаюча частина серверів використовують процесор та пам'яті менше 20%. Таким чином, у IT-світі назріло питання віртуалізація сервера. Ця технологія надає можливість запускати декілька ізольованих операційних систем на одній частині серверного обладнання, що дозволяє підняти рівень розумного і ощадного використання ресурсів усієї мережі.

Для роботи апаратних технології віртуалізації, які саме і розглянуті у роботі, важливі параметри комп'ютерної системи (обов'язкова наявність):

- процесор
- набір мікросхем
- BIOS
- операційна система
- драйвери пристроїв.

Технологія обробки віртуальної пам'яті в процесорі призначена для багатозадачності операційних систем [6]. Коли ця методика використовується для кожної програми, застосовується незалежна схема адресації пам'яті для відображення її за фізичною адресою в пам'яті ПК. Організувавши набір незалежних адресних просторів, можна підвищити ефективність використання пам'яті кількома програмами, що працюють одночасно, та забезпечити захист пам'яті між різними програмами. Завантажуючи невикористані сторінки на вторинний накопичувач, можна використовувати більше пам'яті, ніж встановлено на комп'ютері.

Використання повної потужності центрального процесора із злагодженою безперебійною роботою прикладного програмного забезпечення – це важливий напрямок досліджень, які можна проводити на процесорах різних архітектур, починаючи від Nehalem.

Виклад основного матеріалу й обґрунтування отриманих результатів.

Найяскравіше, на нашу думку, можна продемонструвати апаратну віртуалізацію Intel VT можна від архітектури Nehalem на ядрах Conroe, бо вона бере початок саме з цього покоління процесорів.

Процесори сімейства Core i Series працюють у виконанні Socket LGA1366 в той час, як більш масові моделі призначені для установки в Socket LGA1156. Для підтримки Intel VT ці моделі містять інтегрований двоканальний контролер пам'яті DDR3, графічний інтерфейс і інтегрований відеоадаптер. Оскільки базова функціональність північного моста у них вже інтегрована, процесори у виконанні Socket LGA1156 використовують для взаємодії з південним мостом на системній платі більш повільну версію інтерфейсу шини DMI з пропускною спроможністю 2 Гбайт/с. Представниками сімейства Core i Series є процесори Core i5 і Core i7. Надалі до них «приєдналися» процесори Core i3 і Core i9, що дозволило охопити весь діапазон від початкового до високого рівня. У цих процесорах міститься до трьох контролерів пам'яті DDR3. Якщо встановити пам'ять DDR3-1333, яку також підтримує Nehalem, в деяких конфігураціях вона забезпечить пропускну здатність до 32 ГБ/с. Але, перевагою вбудованого контролера пам'яті є не тільки пропускна здатність. Це значно скорочує затримку доступу до пам'яті, що не менш важливо, оскільки для кожного доступу потрібні сотні циклів. У разі використання настільних ПК скорочена затримка вбудованого контролера пам'яті вітається, наявна повна перевага масштабованої архітектури в конфігурації багатостороннього сервера. Раніше, при додаванні процесорів (ядер), доступна пропускна здатність залишалася незмінною, а з цією технологією кожен новий додатковий процесор збільшує пропускну здатність, оскільки кожен процесор має свою пам'ять. Схема апаратної віртуалізації подана на рисунку 1:

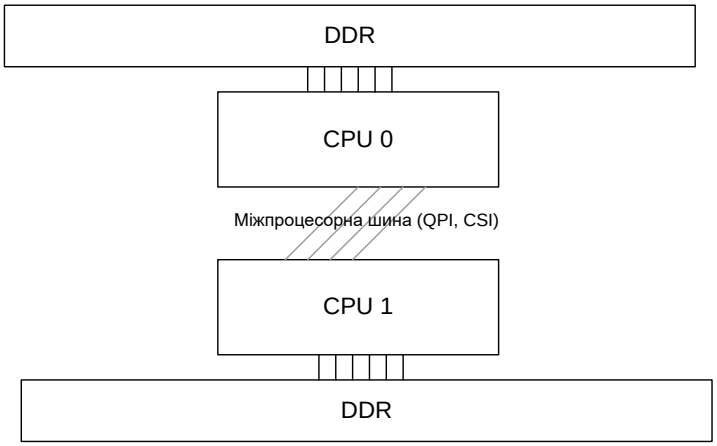

Рисунок 1 – Віртуалізація при зверненні до пам'яті

Вплив на продуктивність кожної архітектури передбачити важко, оскільки він повністю залежить від ППЗ та операційної системи. Intel стверджує, що порівняно з локальним доступом погіршення продуктивності віддаленого доступу затримує приблизно на 70%, а пропускна здатність зменшується вдвічі. За даними Intel [6], навіть віддалений доступ через інтерфейс QPI має меншу затримку, ніж попередні покоління процесорів, де контролер розташований на Північному мосту. Однак, це стосується лише серверних додатків.

Щодо пам'яті, то Intel зосереджується на роботі спільних кешів L2, і це стає найкращим рішенням для архітектур, які спрямовані на багатоядерні конфігурації. Але, що стосується Nehalem, інженери почали з нуля і прийшли до того ж висновку, що і їхні конкуренти (маємо на увазі конкуруючу компанію AMD): весь кеш L2 не дуже підходить для чотирьохядерної архітектури. Ядра часто «стирають» дані, необхідні для інших ядер, що призводить до надмірних проблем із внутрішньою шиною та арбітражем, намагаючись забезпечити достатню пропускну здатність для всіх чотирьох ядер, зберігаючи при цьому достатньо низьку затримку. Щоб вирішити ці проблеми, інженери обладнали кожне ядро власним кешем другого рівня (рис. 2). Оскільки він виділений кожному ядру, він може забезпечити дуже високоефективний кеш, зокрема, затримка була значно покращена.

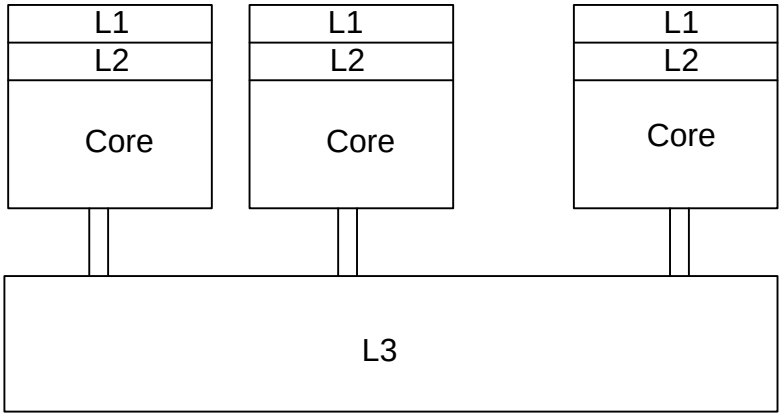

Рисунок 2 – Трирівнева ієрархія кешу

З перенесенням контролера пам'яті з північного моста в тіло CPU зменшилася залежність процесора від постійного збільшення обсягу кеш-пам'яті. Ієрархія кеша в Core i7 цілком підпорядкована багатопотоковим обчислень: уніфікований L2 кеш урізаний на кожне ядро, а основний акцент зроблений на кеш третього рівня. Останній містить всі інструкції і дані з L1/L2 cache для зменшення трафіку запитів.

Протягом багатьох років процесори використовували не фізичну адресу пам'яті, а віртуальні адреси. Серед інших переваг, цей метод дозволяє програмі виділяти більше пам'яті, ніж комп'ютер, зберігати лише ті дані, які в даний час необхідні у фізичній пам'яті, а також зберігати все інше на жорсткому/твердотільному диску. Це означає, що кожен доступ до віртуальної пам'яті повинен бути переведений на фізичну адресу, і для підтримки відповідності потрібно використовувати величезні таблиці структури пам'яті. Проблема полягає в тому, що таблиці занадто великі, а щоб більше зберігати їх на мікросхемі – вони поміщаються в основну пам'ять і навіть можуть бути скинуті на жорсткий диск (втратитися в пам'яті та скинутись на HDD може тільки частина таблиці).

Якщо кожна операція з пам'яттю вимагає такого етапу перекладу адреси, то все буде працювати занадто повільно. Тому, згодом інженери повернулися до принципу фізичної адреси та безпосередньо додали невеликий кеш до процесора, який підтримував кореспонденцію декількох нещодавно запитуваних адрес. Цей кеш називається трансляційним буфером перегляду (TLB).

Доступ до пам'яті призводить до багатьох обмежень продуктивності. Процесор оптимізований для доступу до пам'яті, вирівняної по 64-байтовій межі, що є розміром рядка кешу. Для нестандартних даних доступ не тільки повільний, але і дорожчий у виконанні (розробці). Причина полягає в тому, що ці інструкції призводять до декількох мікрооперацій на декодері, що зменшує пропускну здатність таких інструкцій. В результаті компілятор уникає створення такого типу інструкцій, а замість цього використовує низку більш повільних інструкцій. Інженери Intel оптимізували це, щоб зробити доступ

швидшим. Реалізовано підхід, коли дані вирівнюються в пам'яті, продуктивність не знижується при використанні нерівних інструкцій читання чи запису. В інших випадках, Intel також оптимізувала дозволи доступу та зменшила погіршення продуктивності порівняно з архітектурою Core.

В архітектурі Intel на ядрах Conroe суттєвим є апаратне прогнозування. Як відомо, блок прогнозування є механізмом моніторингу характеру доступу до пам'яті. Він передбачає, які дані знадобляться за кілька циклів. Мета його – попередньо завантажувати дані в кеш, який буде розташований ближче до процесора, при цьому максимізуючи наявну пропускну здатність, коли процесор не потрібен.

Ця технологія може забезпечити відмінні результати в більшості настільних додатків, але в серверному середовищі вона зазвичай викликає погіршення продуктивності. Причин цієї неефективності багато. По-перше, часто важко передбачити доступ до пам'яті в серверних додатках. Наприклад, доступ до бази даних ніколи не є лінійним – якщо елемент даних запитується в пам'яті, це не означає, що наступним буде наступний елемент. Це обмежує ефективність роботи попереднього відбору проб. Але головна проблема – пропускна здатність пам'яті в конфігурації декількох слотів. Як ми зазначали раніше, це вже «вузьке місце» для декількох процесорів, і крім того, блок попередньої вибірки викликає рівень додаткового навантаження. Якщо мікропроцесор не має доступу до пам'яті, зазвичай вмикається блок попереднього відбору проб і використовується пропускна здатність, яку вони вважають непрацюючою. Однак, ці блоки не можуть знати, чи потрібен другий процесор цієї пропускної здатності. Це означає, що блок попередньої вибірки може «займати» пропускну здатність процесора, що в цій конфігурації вже є «вузьким місцем». Для вирішення цієї проблеми Intel не знайшла кращого способу, ніж відключення блоку попередньої вибірки. Хоча, в літературі зустрічаються міркування, що це навряд чи найкраще рішення.

За даними Intel, це питання було вирішено, але компанія не надала жодних деталей щодо роботи нового механізму попереднього відбору проб. Однак, навіть якщо Intel не вніс жодних змін, переваги нової організації пам'яті та більша пропускна здатність повинні компенсувати негативний вплив попереднього зразка.

Conroe стало міцною основою для нових процесорів, і Nehalem заснований на ньому. Він використовує таку ж ефективну архітектуру, але тепер він має більш високу модульність та масштабованість, що має забезпечити успіх у різних ринкових секторах. Е можна напевно 100% стверджувати, що Nehalem змінив архітектуру Core, але зрозуміло, що новий процесор з технологією віртуалізації змінив платформу Intel.

Глобальний підхід до віртуалізації Intel призвів до створення декількох технологій апаратної підтримки на платформі, які спрощують віртуалізацію та роблять її більш надійною та, як правило, зменшують витрати на програмне забезпечення, пов'язані з віртуалізацією.

Удосконалена технологія Intel Virtualization (забезпечує апаратну підтримку для керування таблицею сторінок, що полегшує гостьовій ОС доступ до обладнання. Це зменшує кількість запитів на програмне забезпечення, бо перетворення, здійснені менеджером VM, споживають багато ресурсів процесора.

Програмний метод віртуалізації вводу-виводу забезпечує гнучкість у прозорості вводу-виводу та прозорості обладнання. Віртуалізація програмного вводу/виводу (I/O) не дозволяє контролювати прямий доступ пристроїв вводу-виводу до фізичної пам'яті, що може спричинити проблеми при ізоляції віртуальних машин та їх пристроїв вводу-виводу. Однак, поєднання апаратної підтримки та системного програмного забезпечення може забезпечити необхідні засоби ізоляції операцій прямого доступу до пам'яті.

Апаратна підтримка віртуалізації вводу-виводу (рис. 3) дозволяє системному програмному забезпеченню безпечно призначати конкретні пристрої вводу-виводу безпосередньо віртуальним машинам. Прямий розподіл за допомогою апаратної підтримки дозволяє позбутися рівня емуляції VM, тим самим збільшуючи пропускну здатність віртуальної машини. Коли задіяти пристрої, які можуть розподіляти свої ресурси серед декількох віртуальних машин, функція прямого розподілу буде додатково розширена, оскільки на один пристрій може бути виділено більше віртуальних машин.

Технологія Intel VT-d забезпечує необхідну апаратну підтримку, щоб зробити віртуалізацію вводу-виводу більш безпечною, простою та надійною.

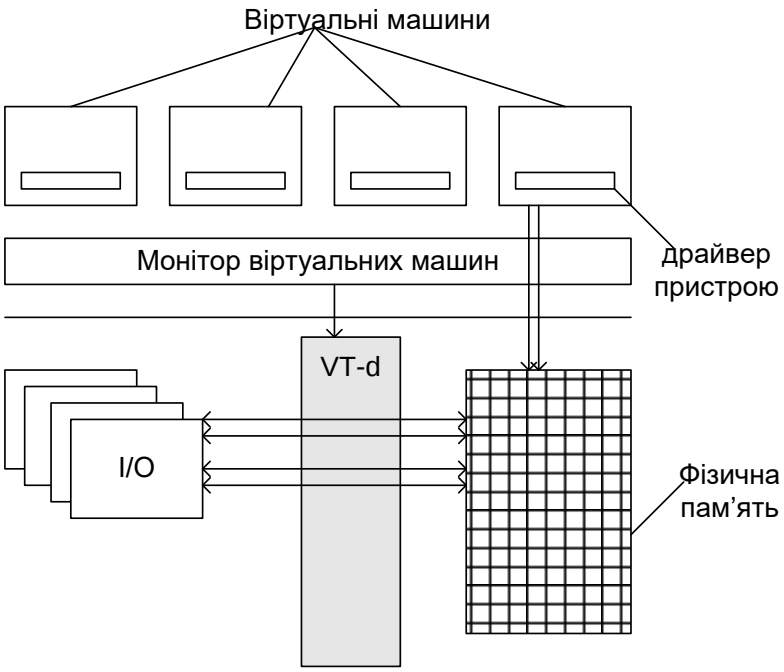

Рисунок 3 – Схема віртуалізації вводу-виводу

Технологія віртуалізації вводу/виводу є доповненням до ряду технологій віртуалізації від Intel, що забезпечують апаратну підтримку рішень для віртуалізації.

Апаратна підтримка надає функцію зміни адреси, а також може безпосередньо призначати пристрої вводу-виводу, що працюють із системним програмним забезпеченням.

Архітектура Intel VT-d дозволяє системному програмному забезпеченню (VM або операційній системі в невіртуальному середовищі) створювати один або кілька захищених доменів, це окреме середовище, в якому виділяється частина фізичної пам'яті. Захищеним доменом DMA може бути пам'ять, виділена віртуальній машині, або пам'ять DMA, виділена гостьовим драйвером ОС, що працює на віртуальній машині. Програмне забезпечення системи призначає домен безпеки кожному пристрою вводу-виводу. Всі доступу до DMA з пристрою вводу/виводу перенесені на фізичну адресу вузла відповідно до виділеного домену, тим самим перешкоджаючи доступу до пам'яті за межами виділеного домену. Зміна адреси дозволяє пристроям (і драйверам) використовувати адреси віртуальної машини замість фізичної адреси пам'яті.

Віртуалізація – це свого роду рівень абстракції, який порушує стандартну парадигму архітектури комп'ютера, відокремлює операційну систему від фізичної апаратної платформи та програм, що працюють на ній. Віртуалізація дозволяє декільком віртуальним машинам, часто з неоднорідними операційними системами, працювати ізольовано, поруч, на одній фізичній машині. Кожна віртуальна машина має власний набір віртуальної апаратури (процесор, пам'ять, мережеві інтерфейси та дискове сховище), на який завантажується операційна система та програми. Операційна система бачить набір апаратних засобів і не знає про характер спільного використання з іншими гостьовими операційними системами, що працюють на тій же фізичній апаратній платформі. Технологія віртуалізації та її основні компоненти, такі як Монітор віртуальної машини, керують взаємодією з викликами операційної системи до віртуальної апаратури та фактичним виконанням, яке відбувається на базовому фізичному обладнанні.

Сьогодні віртуалізація зростає як провідна технологія ІТ. Ця технологія допомагає підприємствам, як великим, так і малим, вирішувати свої проблеми зі масштабуванням, безпекою та управлінням їх глобальною ІТ-інфраструктурою, ефективно використовуючи, а у деяких випадках навіть зменшувати, витрати.

Висновки та перспективи подальшого дослідження. Технологія віртуалізації Intel дозволяє розгорнути сторонні незалежні віртуальні пристрої для виконання важливих завдань управління та безпеки для виконання таких операцій, як глибоке сканування пакетів та виконання політики на настільних комп'ютерах. Віртуальні пристрої, що мають стійкість до відмов, можуть забезпечити стабільне середовище для виконання важливих завдань та включати все необхідне програмне

забезпечення для зручності та ефективності. Технологія забезпечує ізольоване, контрольоване та безпечне середовище для підтримки клієнтських платформ, забезпечуючи захист пам'яті та оптимізацію вводу/виводу у віртуальних машинах.

Список бібліографічного опису

1. Tomsho G. MCTS Guide to Configuring Microsoft Windows Server 2008 Active Directory / Gregory Tomsho., 2009. – 635 с. – (Networking).
2. Golden B. Virtualization FOR DUMmIES / Bernard Golden. – Indianapolis: Wiley Publishing, Inc, 2011. – 75 с
3. Kappel J. Microsoft Virtualization with Hyper-V / J. Kappel, A. Velte, T. Velte., 2009. – 415 с.
4. Acquisti A. Trust and Trustworthy Computing: Third International Conference / A. Acquisti, S. Smith, A. Sadeghi. – Berlin, Germany: TRUST. – (Proceedings)
5. Proceedings of International Conference on Soft Computing Techniques and Engineering Application – Cunming, China: Springer, 2013. – 578 с.
6. Технология виртуализации Intel [Електронний ресурс] – Режим доступу до ресурсу: https://www.intel.ru/content/www/ru/ru/virtualization/virtualization-technology/intel-virtualization-technology.html

References

1. Tomsho G. MCTS Guide to Configuring Microsoft Windows Server 2008 Active Directory / Gregory Tomsho., 2009. – 635 p. – (Networking).
2. Golden B. Virtualization FOR DUMmIES / Bernard Golden. – Indianapolis: Wiley Publishing, Inc, 2011. – 75 p.
3. Kappel J. Microsoft Virtualization with Hyper-V / J. Kappel, A. Velte, T. Velte., 2009. – 415 p.
4. Acquisti A. Trust and Trustworthy Computing: Third International Conference / A. Acquisti, S. Smith, A. Sadeghi. – Berlin, Germany: TRUST. – (Proceedings)
5. Proceedings of International Conference on Soft Computing Techniques and Engineering Application – Cunming, China: Springer, 2013. – 578 p.
6. Intel Virtualization Technology [Electronic resource] – Resource access mode: https://www.intel.ru/content/www/ru/ru/virtualization/virtualization-technology/intel-virtualization-technology.html