EXHIBIT D-2
Clark, "Live Migration of Virtual Machines" (Clark)

Microsoft contends that the asserted claims of the '209 Patent are invalid as anticipated or obvious by Clark et al., "Live Migration of Virtual Machines" ("Clark") prior art reference under various subsections of 35 U.S.C. § 102 in view of other prior art references under 35 U.S.C. § 103 as set forth in Microsoft's invalidity contentions.

As Clark was published on May 3, 2005, Microsoft contends that it is prior art to the '209 Patent under at least pre-AIA 35 U.S.C. § 102(b).

Patent No. 8,381,209	Clark
Claim 1	
1[Pre] A computer implemented method of controlling network security of a virtual machine,	To the extent the preamble is limiting, Clark discloses a computer implemented method of controlling network security of a virtual machine. Specifically, Clark discloses controlling network security during live migration of virtual machines. For example, Clark states: "We designed and implemented our pre-copying migration engine to integrate with the Xen virtual machine monitor. Xen securely divides the resources of the host machine amongst a set of resource-isolated virtual machines each running a dedicated OS instance. In addition, there is one special management virtual machine used for the administration and control of the machine." Clark at 279. "Managed migration is performed by migration daemons running in the management VMs of the source and destination hosts. These are responsible for creating a new VM on the destination machine, and coordinating transfer of live system state over the network." Clark at 280. To the extent that it is argued that Clark does not disclose this limitation, it would have been at least obvious to combine it with any other reference disclosing this limitation as explained in Microsoft's Preliminary Invalidity Contention Cover Pleading.
1[a] the method comprising enforcing network security and routing at a hypervisor layer via dynamic updating of routing controls initiated by a migration of said virtual	Clark discloses enforcing network security and routing at a hypervisor layer via dynamic updating of routing controls initiated by a migration of said virtual machine from a first device to a second device. Specifically, Clark teaches migration of a virtual machine from a first device to a second device; the virtual machine migration causes the routing controls to update continuously with each migration that occurs. For example, Clark states: "To address these requirements we observed that in a cluster environment, the network interfaces of the source and destination machines typically exist on a single switched LAN. Our solution for

EXHIBIT D-2
Clark, "Live Migration of Virtual Machines" (Clark)

Patent No. 8,381,209	Clark
Claim 1	
machine from a first device to a second device.	managing migration with respect to network in this environment is to generate an unsolicited ARP reply from the migrated host, advertising that the IP has moved to a new location. This will reconfigure peers to send packets to the new physical address, and while a very small number of in-flight packets may be lost, the migrated domain will be able to continue using open connections with almost no observable interference." Clark at 276. "Some routers are configured not to accept broadcast ARP replies (in order to prevent IP spoofing), so an unsolicited ARP may not work in all scenarios. If the operating system is aware of the migration, it can opt to send directed replies only to interfaces listed in its own ARP cache, to remove the need for a broadcast. Alternatively, on a switched network, the migrating OS can keep its original Ethernet MAC address, relying on the network switch to detect its move to a new port." Clark at 276. "We designed and implemented our pre-copying migration engine to integrate with the Xen virtual machine monitor. Xen securely divides the resources of the host machine amongst a set of resource-isolated virtual machines each running a dedicated OS instance. In addition, there is one special management virtual machine used for the administration and control of the machine." Clark at 279. To the extent that it is argued that Clark does not disclose this limitation, it would have been at least obvious to combine it with any other reference disclosing this limitation as explained in Microsoft's Preliminary Invalidity Contention Cover Pleading.

Patent No. 8,381,209	Clark
Claim 2	
2[a] The method according to claim 1, further comprising: routing traffic for the virtual machine to the second device at the hypervisor layer; and	Clark discloses routing traffic for the virtual machine to the second device at the hypervisor layer. Specifically, Clark discloses a hypervisor that migrates a virtual machine to a new physical host; once the migration is complete, other interfaces are notified of the migration, and peers are reconfigured to send packets to the new physical address. For example, Clark states: "By carrying out the majority of migration while OSes continue to run, we achieve impressive performance with minimal service downtimes; we demonstrate the migration of entire OS instances on

Patent No. 8,381,209	Clark
Claim 2	
	a commodity cluster, recording service downtimes as low as 60ms. We show that that our performance is sufficient to make live migration a practical tool even for servers running interactive loads." Clark at 273. "Secondly, migrating at the level of an entire virtual machine means that in-memory state can be transferred in a consistent and (as will be shown) efficient fashion. This applies to kernel-internal state (e.g. the TCP control block for a currently active connection) as well as application-level state, even when this is shared between multiple cooperating processes." Clark at 273. "To address these requirements we observed that in a cluster environment, the network interfaces of the source and destination machines typically exist on a single switched LAN. Our solution for managing migration with respect to network in this environment is to generate an unsolicited ARP reply from the migrated host, advertising that the IP has moved to a new location. This will reconfigure peers to send packets to the new physical address, and while a very small number of in-flight packets may be lost, the migrated domain will be able to continue using open connections with almost no observable interference." Clark at 276. "We designed and implemented our pre-copying migration engine to integrate with the Xen virtual machine monitor. Xen securely divides the resources of the host machine amongst a set of resource-isolated virtual machines each running a dedicated OS instance. In addition, there is one special management virtual machine used for the administration and control of the machine." Clark at 279. To the extent that it is argued that Clark does not disclose this limitation, it would have been at least obvious to combine it with any other reference disclosing this limitation as explained in Microsoft's Preliminary Invalidity Contention Cover Pleading.
2[b] setting firewalls to permit a network traffic for the virtual machine to go to the second device at the hypervisor layer.	To the extent that it is argued that Clark does not disclose this limitation, it would have been at least obvious to combine it with any other reference disclosing this limitation as explained in Microsoft's Preliminary Invalidity Contention Cover Pleading.

EXHIBIT D-2
Clark, "Live Migration of Virtual Machines" (Clark)

Patent No. 8,381,209	Clark
Claim 3	
3[a] The method according to claim 1, further comprising: copying network security and routing for said virtual machine to said hypervisor layer;	Clark discloses copying network security and routing for said virtual machine to said hypervisor layer. Specifically, Clark discloses a virtual machine that migrates from one host to another, copying migration tables and/or routing tables. For example, Clark states: "The pre-copying scheme that we implemented for self migration is conceptually very similar to that for managed migration. At the start of each pre-copying round every page mapping in every virtual address space is write-protected. The OS maintains a dirty bitmap tracking dirtied physical pages, setting the appropriate bits as write faults occur. To discriminate migration faults from other possible causes (for example, copy-on-write faults, or access-permission faults) we reserve a spare bit in each PTE to indicate that it is write-protected only for dirty-logging purposes." Clark at 280. To log pages that are dirtied, Xen inserts shadow page tables underneath the running OS. The shadow tables are populated on demand by translating sections of the guest page tables. Translation is very simple for dirty logging: all page-table entries (PTEs) are initially read-only mappings in the shadow tables, regardless of what is permitted by the guest tables. If the guest tries to modify a page of memory, the resulting page fault is trapped by Xen. If write access is permitted by the relevant guest PTE then this permission is extended to the shadow PTE. At the same time, we set the appropriate bit in the VM's dirty bitmap. When the bitmap is copied to the control software at the start of each pre-copying round, Xen's bitmap is cleared and the shadow page tables are destroyed and recreated as the migratee OS continues to run. This causes all write permissions to be lost: all pages that are subsequently updated are then added to the now-clear dirty bitmap." Clark at 280. To the extent that it is argued that Clark does not disclose this limitation, this would have at least been inherent because Clark discloses copying of all page tables managed by the virtual machine OS. Furthermore, to the extent that it is argued that Clark does not disclose all or part of this limitation, it would have been at least obvious to combine it with any other reference disclosing this limitation as explained in Microsoft's Preliminary Invalidity Contention Cover Pleading.
3[b] migrating said virtual machine from a first	Clark discloses migrating said virtual machine from a first hardware device to a second hardware device. For example, Clark states:

EXHIBIT D-2
Clark, "Live Migration of Virtual Machines" (Clark)

Patent No. 8,381,209	Clark
Claim 3	
hardware device to a second hardware device.	"In this paper we explore a further benefit allowed by virtualization: that of live OS migration. Migrating an entire OS and all of its applications as one unit allows us to avoid many of the difficulties faced by process-level migration approaches. In particular the narrow interface between a virtualized OS and the virtual machine monitor (VMM) makes it easy avoid the problem of 'residual dependencies' in which the original host machine must remain available and network-accessible in order to service certain system calls or even memory accesses on behalf of migrated processes. With virtual machine migration, on the other hand, the original host may be decommissioned once migration has completed. This is particularly valuable when migration is occurring in order to allow maintenance of the original host." Clark at 273. "Managed migration is performed by migration daemons running in the management VMs of the source and destination hosts. These are responsible for creating a new VM on the destination machine, and coordinating transfer of live system state over the network." Clark at 280. Clark at Fig. 1:

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.