Содержание

1 Начальная настройка AMT

Начальная настройка AMT — активация управляющего модуля AMT (AMT Management Engine) и установке некоторых его параметров, таких как пароль доступа и режим работы. Настройка выполнятся при помощи MEBx (Management Engine BIOS Extensions) — специального расширения BIOS, ответственного за настройку AMT.

Обычно начальная настройка AMT для каждого компьютера выполняется только один раз. В последствии выполнять дополнительную настройку и изменение конфигурации можно удалённо, средствами AMT.

1.1 Режимы и фазы работы AMT

AMT может работать в двух режимах:

- **SMB** — для небольших сетей;
- **Enterprise** (по умолчанию) — для больших сетей.

В зависимости от того, на каком этапе настройки AMT вы находитесь, различают три фазы:

- **Factory** — конфигурирование AMT не выполнялось;
- **In-Setup** — конфигурирование AMT выполняется в настойщий момент;
- **Operational** — конфигурирование AMT завершено и AMT можно использовать удалённо.

1.2 Требования к паролю

- Пароль должен быть как минимум 8 символов в длину, допускается использование любых (за исключением четырёх нижеперечисленных) ASCII-символов из диапазона 32—126 включительно.
- Нельзя использовать символы “ ‘ , и :
- В пароле должна присутствовать хотя бы одна цифра (например, 0, 1, 2, 9).
- В пароле должен присутствовать хотя бы один не алфавитно-цифровой символ (например, !, @, $).
- В пароле должны присутствовать буквы верхнего и нижнего регистра (например, A, a, B, b).

1.3 Настройка ME в SMB режиме

1. Нажмите **Ctrl-P** в процессе загрузки.

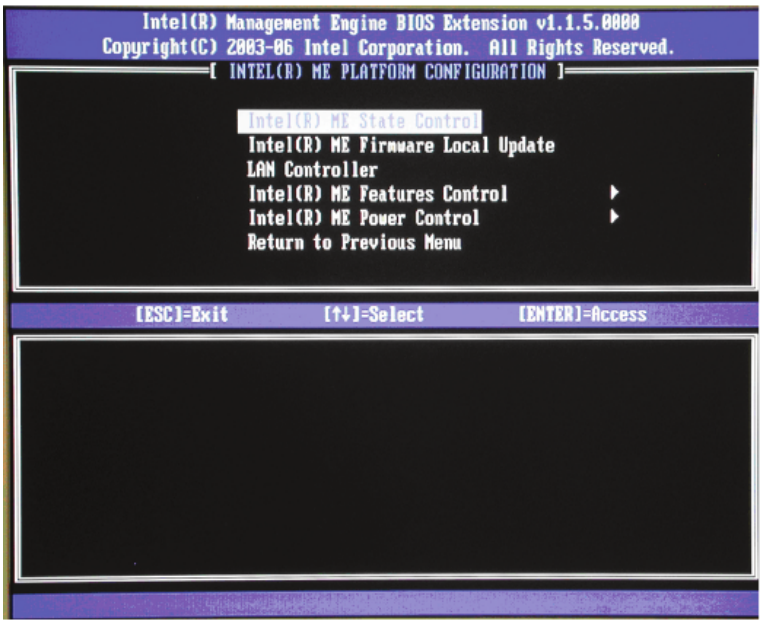
2. Введите пароль. Пароль по умолчанию: **admin**. Пароль чувствителен к регистру.

3. Измените пароль MEBx. Пароль должен удовлетворять правилам строгих паролей (см. выше).

Система переходит от фазы *Factory* к фазе *In-Setup*.

4. Выберите пункт меню **ME Platform Configuration**. Система предупреждает, что перезагрузится после того как установка будет завершена.

5. Выберите **Y**. В ходе настройки ME можно задавать параметры AMT/ASF, настройки питания, настройки обновления firmware и др.



6. Выберите **Intel ME State Control** и в нём выберите **Enabled**

- Настройка по умолчанию: **Enabled**
- Рекомендуемая настройка: **Enabled**

Эта опция может использоваться для того чтобы временно отключить ME. При этом функции AMT/ASF будут недоступны.

7. Выберите **Intel ME Firmware Local Update Qualifier** и в нём выберите **Always Open**

- Настройка по умолчанию: **Always Open**
- Рекомендуемая настройка: **Always Open**
- Есть варианты: **Never Open**, **Restricted**

Опция определяет, можно ли выполнять обновление firmware локально.

8. Пропустите пункт **LAN Controller**

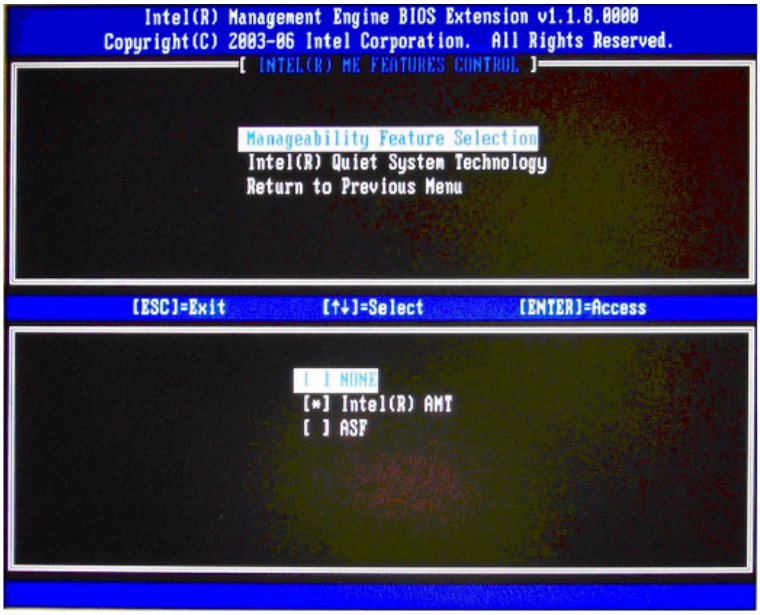
- Настройка по умолчанию: **Enabled**
- Рекомендуемая настройка: **Enabled**

Отключение сетевого контроллера возможно, только если выключен модуль ME (режим управления ME установлен в **None**). В этом случае удалённое управление становится невозможным.

9. Выберите **Intel ME Features Control**.

a. Выберите **Manageability Feature Selection**

- Настройка по умолчанию: **Intel AMT**
- Рекомендуемая настройка: **Intel AMT**



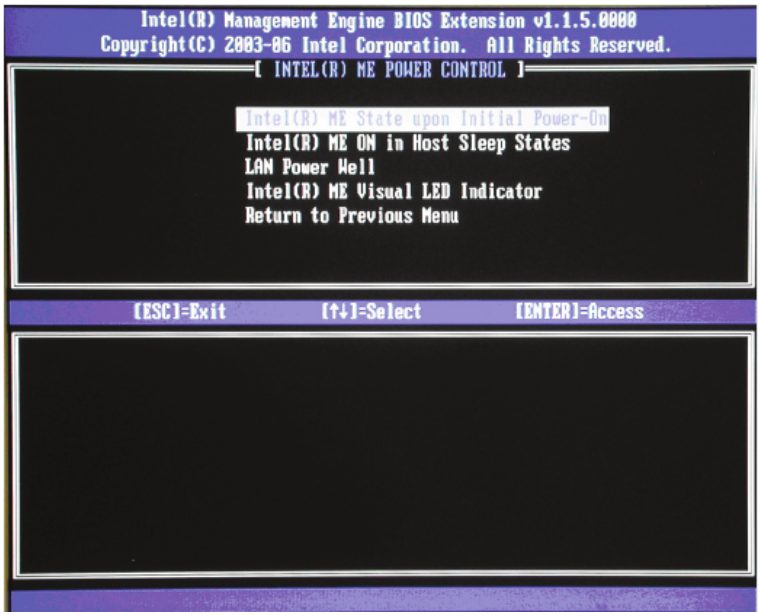
b. Пропустите **Intel Quiet Systems Technology**

- Настройка по умолчанию: **Disabled**
- Рекомендуемая настройка: **Disabled**

Эта настройка вообще используется для управления скоростью вращения вентилятора системного блока компьютера. В компьютерах HP она не используется, регулирование скорости вращения выполняется другими методами.

c. Пропустите **Return to the previous menu**

10. Выберите **Intel ME Power Control**.



a. Выберите **ME State upon Initial Power-On** и в нём выберите **On**

- Настройка по умолчанию: **Off**
- Рекомендуемая настройка: **On**
- **Off** — выключено при выключенном компьютере, но включается при включении
- **On** — включено даже при выключенном компьютере

ME State upon Initial Power-ON	ME ON in Host Sleep State	Host Behavior
On	Always	System will wake after G3 exit
On	Never, S3, S3+S4	System will not wake after G3 exit
Off	Always, Never, S3, S3+S4	System will not wake after G3 exit

b. Выберите **ME ON in Host Sleep States** и выберите **Always**

- Настройка по умолчанию: **Never**
- Рекомендуемая настройка: **Always**

ME ON in Host Sleep State	Host Power State	ME Power State
Always	S0	M0
Always	S3, S4, S5	M1
Never	S0	M0
Never	S3, S4, S5	Moff
Standby (S3)	S0	M0
Standby (S3)	S3	M1
Standby (S3)	S4, S5	Moff
Standby (S3) + Hibernate (S4)	S0	M0
Standby (S3) + Hibernate (S4)	S3, S4	M1
Standby (S3) + Hibernate (S4)	S5	Moff

(c) Пропустите **LAN Power Well**

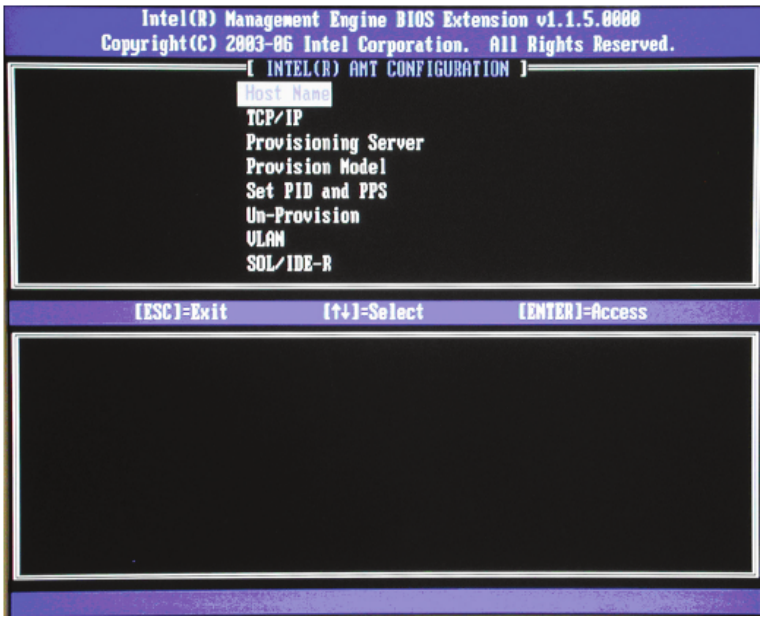
Функция **LAN Power Well** выполнена в компьютерах HP на аппаратном уровне и поэтому данная опция не используется.

(d) Пропустите **ME Visual LED Indicator**

Индикатор активности модуля ME. При выполнении операций с ME зажигается индикатор на материнской плате. В компьютерах HP не используется.

(e) Выберите **Return to previous menu**

11. Вернуться в предыдущее меню, сохранить настройки AMT. Компьютер уйдёт на перезагрузку.
12. Введите **Ctrl-P** во время загрузки POST.
13. Введите пароль для доступа к MEBx.
14. Выберите пункт **Intel AMT Configuration**.



15. Выберите пункт **Host Name** и введите имя хоста.
16. Выберите **TCP/IP**.
(a) В пункте **Disable Network Interface** выберите **N**
(b) В пункте **DHCP Disable** выберите **Y**
(c) В пункте **IP address** введите IP-адрес ME
(d) В пункте **Subnet Mask** введите сетевую маску ME
(e) В пункте **Default Gateway Address** введите шлюз по умолчанию для ME компьютера
(f) В пункте **Preferred DNS Address** предпочитаемый DNS-сервер
(g) В пункте **Alternate DNS Address** запасной DNS-сервер
(h) В пункте **Domain Name** введите доменное имя ME компьютера
17. Пропустите **Provisioning Server**.
18. Выберите **Provisioning Model**.
(a) В пункте **Intel AMT 1.0 Mode** введите **N**
(b) В пункте **Small Business** введите **Y**

- Настройка по умолчанию: **Enterprise**

- Рекомендуемая настройка: **SMB**

19. Пропустите **Un-Provision**.
20. Пропустите настройку **VLAN**

- Настройка по умолчанию: **Disabled**

- Рекомендуемая настройка: **User Dependent**

В качестве значения номера VLAN'а используйте число в диапазоне 1-4094.
21. Выберите **SOL/IDE-R**
(a) Выберите **Y**
(b) Выберите пункт **Username and Password** и выберите **Enabled**

- Настройка по умолчанию: **Enabled**

- Рекомендуемая настройка: **Enabled**

(c) Выберите пункт **Serial over LAN** и в нём выберите **Enabled**.

- Настройка по умолчанию: **Enabled**

- Рекомендуемая настройка: **Enabled**

22. Выберите пункт **Remote Firmware Update** и установите вариант **Enabled**.

- Настройка по умолчанию: **Enabled**

- Рекомендуемая настройка: **Enabled**

Эта настройка разрешает удалённо обновлять BIOS.

23. Выберите **Return to previous menu** для того чтобы выйти из текущего меню на уровень выше.

24. Выберите **Exit** и нажмите **Y** для того чтобы выйти из настройки MEBx с сохранением.

После того как система перезагрузится, она переходит от фазы *In-Setup* к фазе *Operational*. Теперь можно выполнять удалённое управление системой через Web-интерфейс или удалённую консоль ISV.

1.4 Настройка AMT в Enterprise режиме

Требует наличия специального сервера настройки (Setup and Configuration Server, S&CS), также известного как сервер обеспечения (Provisioning Server).

Процедура настройки модулей управления AMT компьютеров в enterprise-режиме называется *provisioning* (ближайший перевод: обеспечение или снабжение).

Отличается от режима настройки ME в режиме SMB тем, что необходимо задать ещё два параметра:

- **Provisioning ID (PID)**
- **Provisioning Passphrase (PPS)**

Параметр PID должен состоять из 8 символов, а PPS — из 32 символов. Каждые четыре символа отделяются друг от друга символом «-» и получается что нужно вводить 9 символов для параметра PID и 40 символов для для PPS.

Параметры генерируются автоматически с помощью сервера настройки.

Существует три режима настройки множества компьютеров:

- Legacy — устаревший;
- IT TLS-PSK — с использованием S&CS, выполнятся IT-отделом компании;
- OEM TLS-PSK — выполняется производителем.

1.5 Отлкючение AMT (Возврат в исходное состояние)

Сброс настроек AMT и возврат системы в исходное состояние известен называется *unprovisioning*.

Для того чтобы выполнить его нужно выбрать соответствующий пункт в меню MEBx.

1.6 Дополнительная информация

- Начальная настройка vPro[1] (англ.)
- vPro Setup and Configuration for the dc7700 Business PC with Intel vPro Technology[2] (англ.)

[1] http://xgu.ru/wiki/vpro/me
[2] http://xgu.ru/download/vpro-hp.pdf

2 Управление компьютером через web-интерфейс AMT

Web-интерфейс AMT — базовый интерфейс, при помощи которого возможно управление компьютером, поддерживающим технологию AMT. В роли web-сервера выступает управляющий механизм (Management Engine, ME) управляемого компьютера; в роли web-клиента — браузер, с которым работает администратор.

2.1 Использование web-интерфейса

Управление системой через AMT возможно при помощи web-сервера, встроенного в ME компьютера с поддержкой vPro. Для того чтобы воспользоваться им, нужно

- активировать AMT;
- установить IP-адрес на сетевой интерфейс ME;
- установить пароль на доступ к ME.

После этого можно обращаться на Web-интерфейс по порту 16992 (HTTP) или 16993 (HTTPS).

Введите пароль, заданный при настройке ME.

И имя пользователя, и пароль совпадаеют с теми, которые вы используете при доступе к консоли управления ME непосредственно.

После того как пароль введён, и аутентификация пройдена, вы получаете доступ к web-интерфейсу AMT.

С левой стороны экрана находится панель, на которой перечислены

- **System Status** (состояние системы);
- **Hardware Information** (информация о железе);
- **Event Log** (журнал событий);
- **Remote Control** (удалённое управление);
- **Power Policies** (политики питания);
- **Network Settings** (сетевые настройки);
- **User Accounts** (пользовательские учётные записи)

Удалённое управление системой.

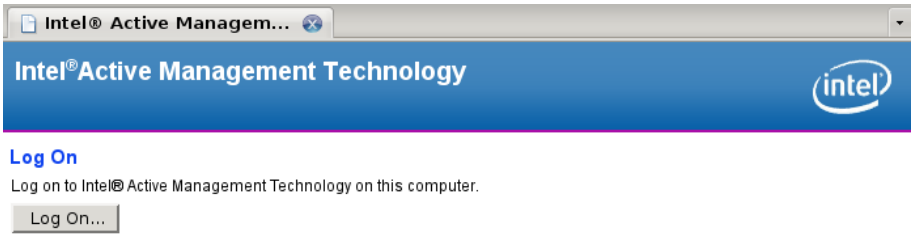
Систему можно выключить или включить. При использовании web-интерфейса загружать можно только с локальных носителей информации (жёсткого диска или CD-привода), загрузка при помощи протокола IDE-R невозможна.

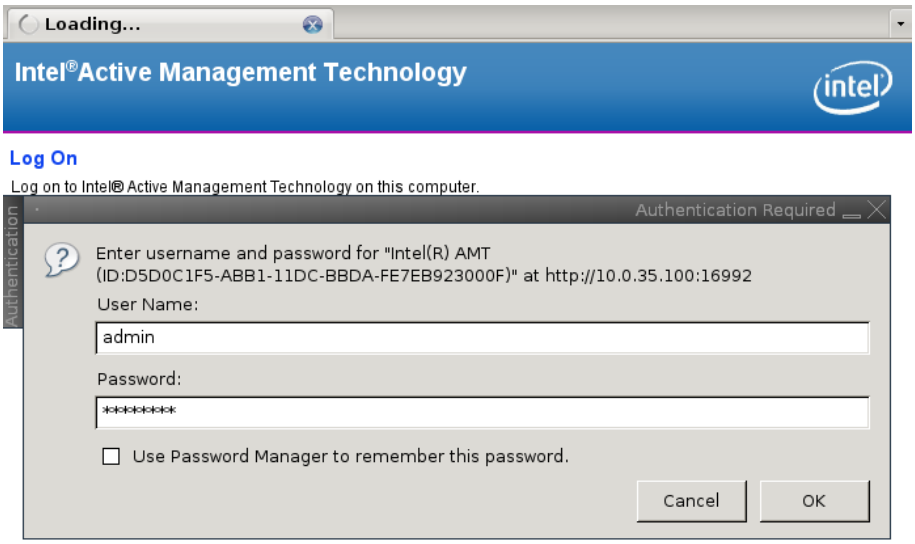
2.2 Дополнительная информация

- Управление компьютером через Web-интерфейс AMT[3]

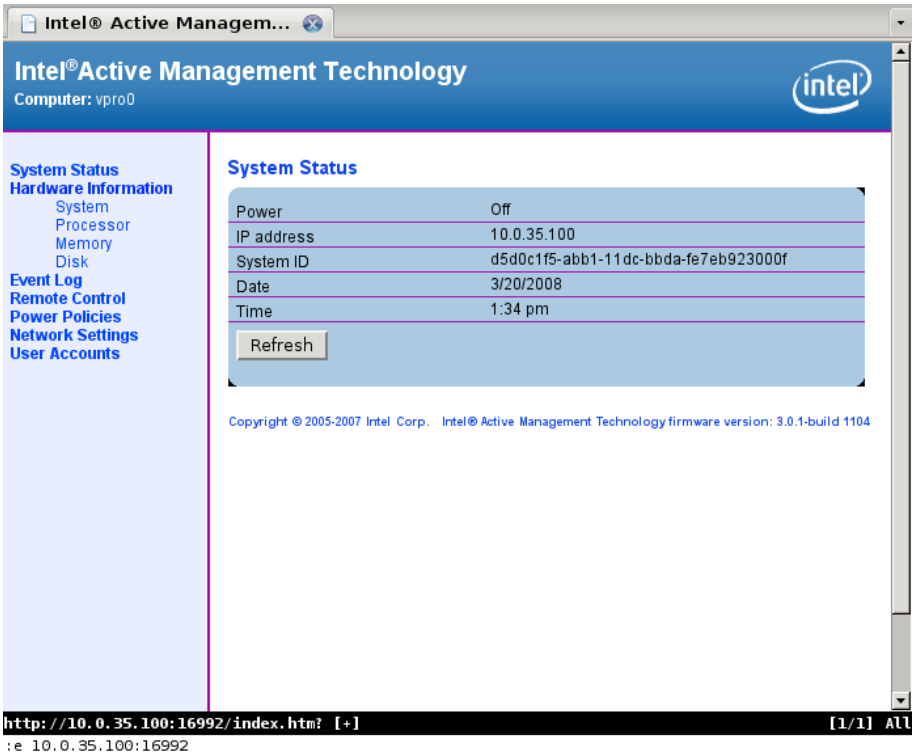
[3] http://xgu.ru/wiki/vpro/amt-web

2.3 Скриншоты web-интерфейса AMT

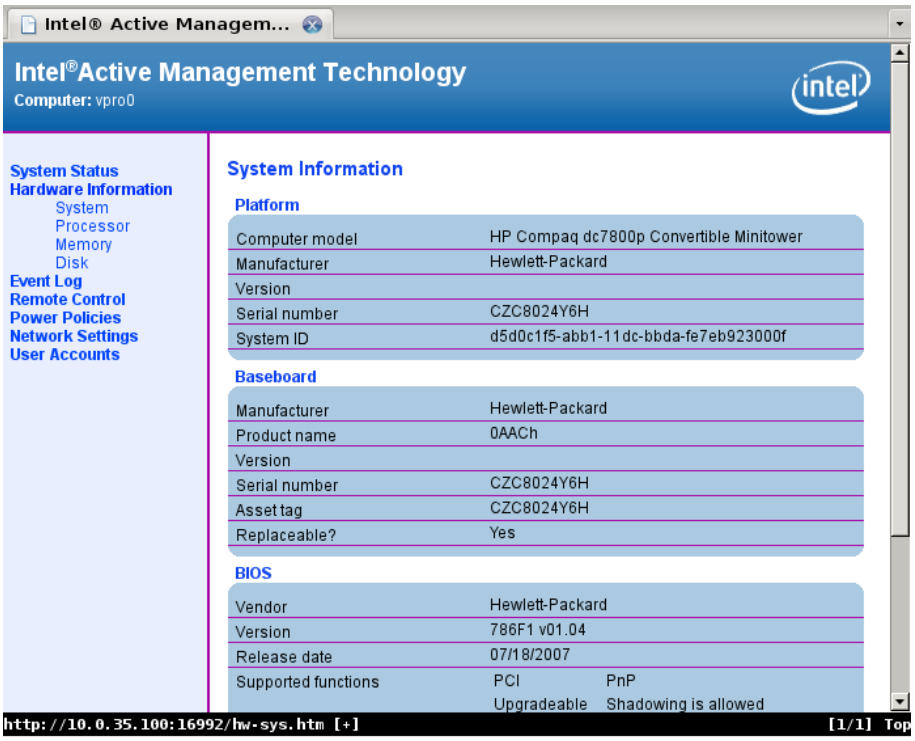


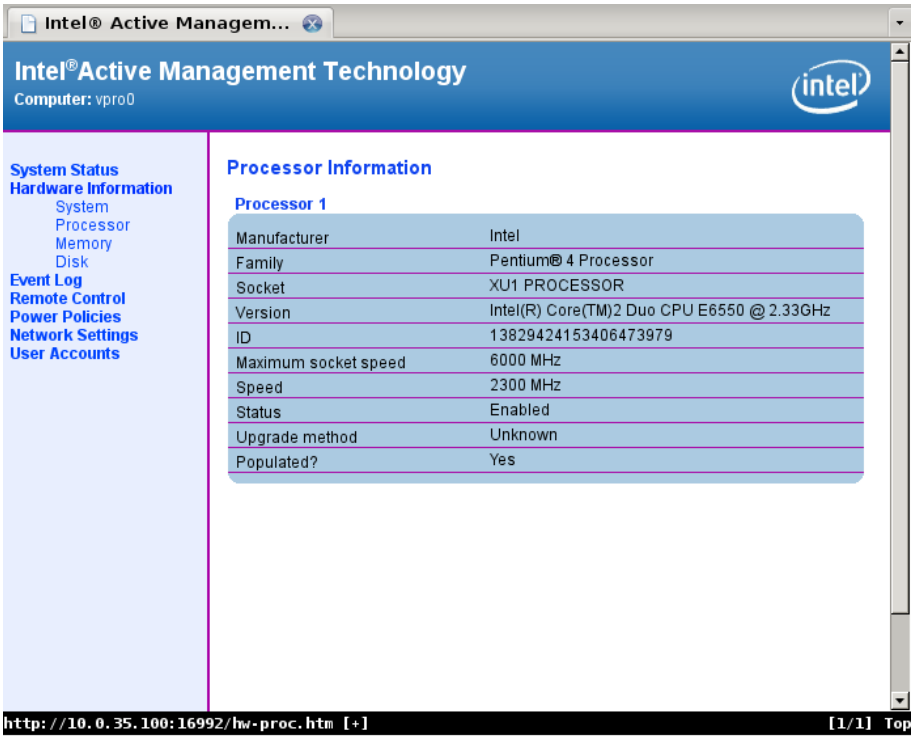


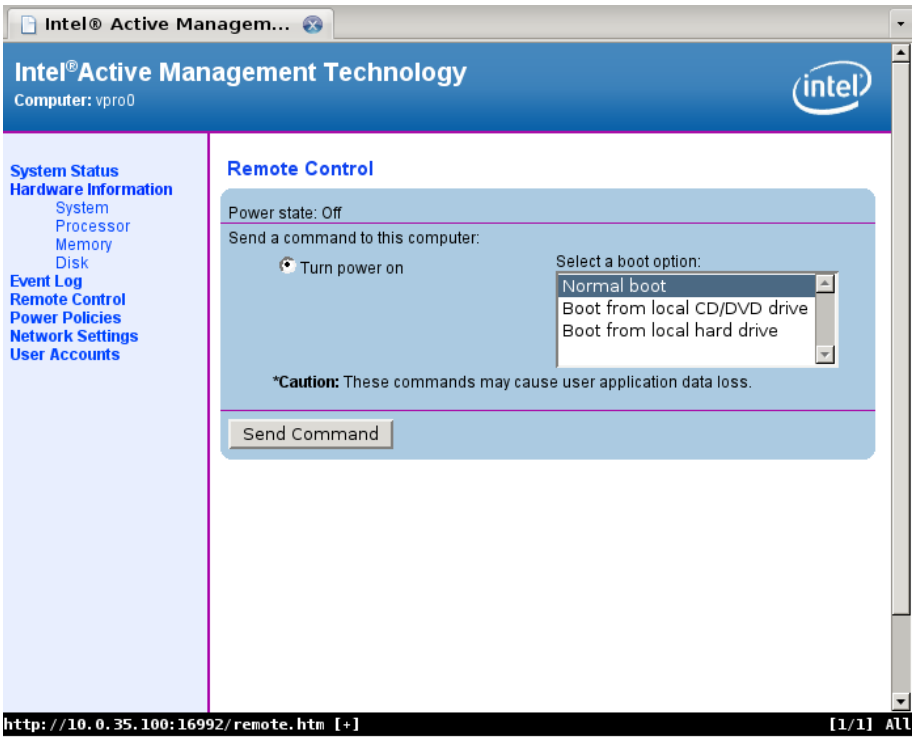

```
Waiting for 10.0.35.100...                                    [1/1] All
:e 10.0.35.100:16992
```

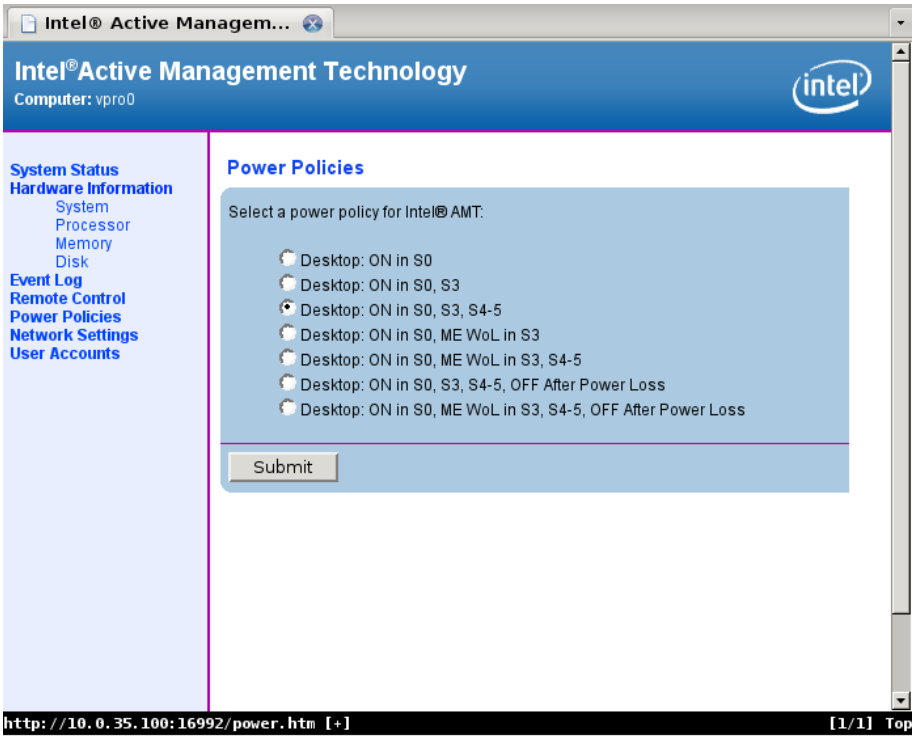


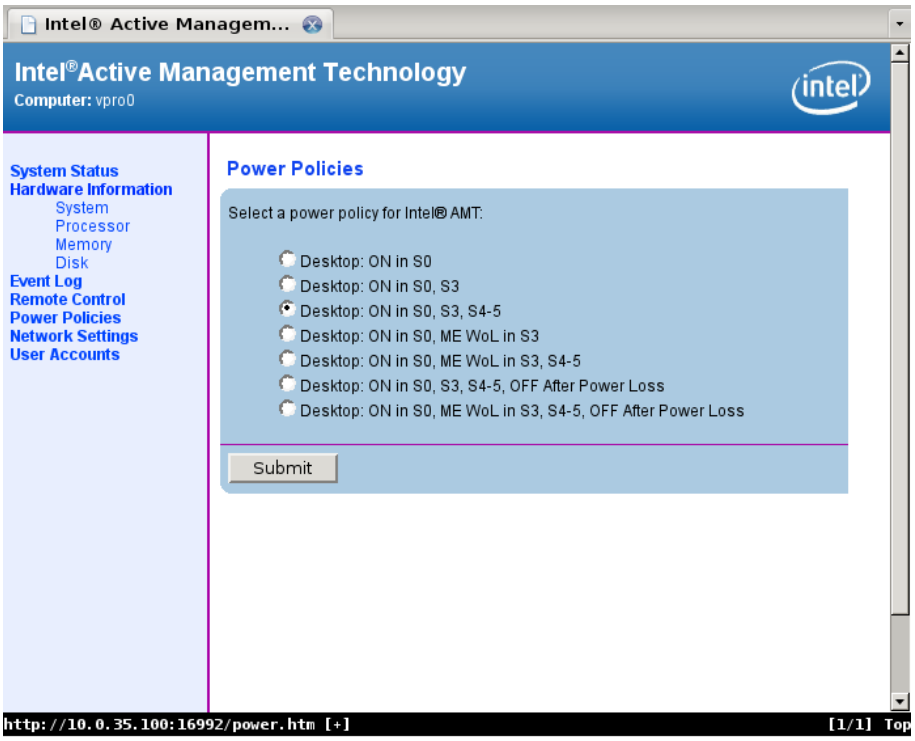

```
http://10.0.35.100:16992/index.htm? [+]                       [1/1] All
:e 10.0.35.100:16992
```

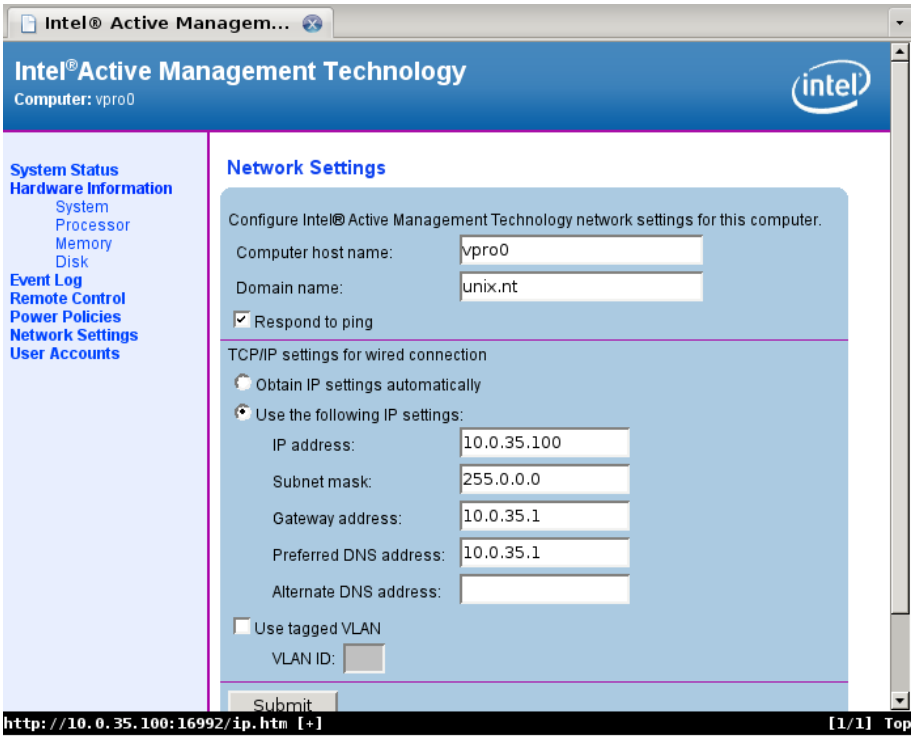

Intel® Active Managem...
Intel®Active Management Technology
Computer: vpro0
System Status
Hardware Information
System
Processor
Memory
Disk
Event Log
Remote Control
Power Policies
Network Settings
User Accounts
System Information
Platform
Computer model HP Compaq dc7800p Convertible Minitower
Manufacturer Hewlett-Packard
Version
Serial number CZC8024Y6H
System ID d5d0c1f5-abb1-11dc-bbda-fe7eb923000f
Baseboard
Manufacturer Hewlett-Packard
Product name 0AACh
Version
Serial number CZC8024Y6H
Asset tag CZC8024Y6H
Replaceable? Yes
BIOS
Vendor Hewlett-Packard
Version 786F1 v01.04
Release date 07/18/2007
Supported functions PCI PnP
Upgradeable Shadowing is allowed
http://10.0.35.100:16992/hw-sys.htm [+]
[1/1] Top

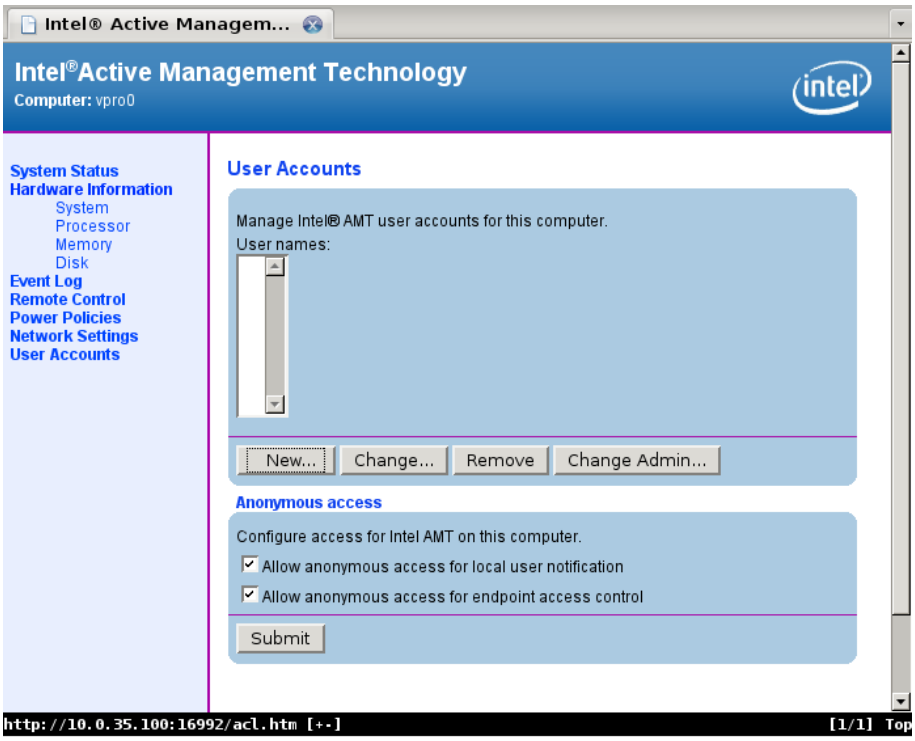

Intel® Active Managem...
Intel®Active Management Technology
Computer: vpro0
System Status
Hardware Information
System
Processor
Memory
Disk
Event Log
Remote Control
Power Policies
Network Settings
User Accounts
Processor Information
Processor 1
Manufacturer Intel
Family Pentium® 4 Processor
Socket XU1 PROCESSOR
Version Intel(R) Core(TM)2 Duo CPU E6550 @ 2.33GHz
ID 13829424153406473979
Maximum socket speed 6000 MHz
Speed 2300 MHz
Status Enabled
Upgrade method Unknown
Populated? Yes
http://10.0.35.100:16992/hw-proc.htm [+]
[1/1] Top

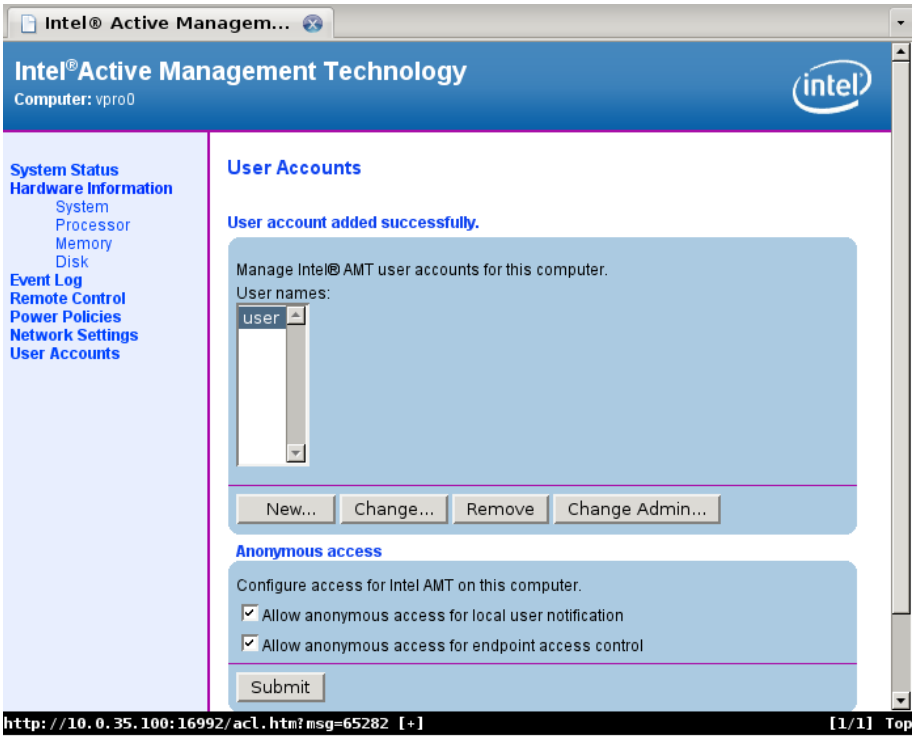

Intel® Active Managem...
Intel®Active Management Technology
Computer: vpro0
System Status
Hardware Information
System
Processor
Memory
Disk
Event Log
Remote Control
Power Policies
Network Settings
User Accounts
Remote Control
Power state: Off
Send a command to this computer:
Turn power on
Select a boot option:
Normal boot
Boot from local CD/DVD drive
Boot from local hard drive
*Caution: These commands may cause user application data loss.
Send Command
http://10.0.35.100:16992/remote.htm [+]
[1/1] All

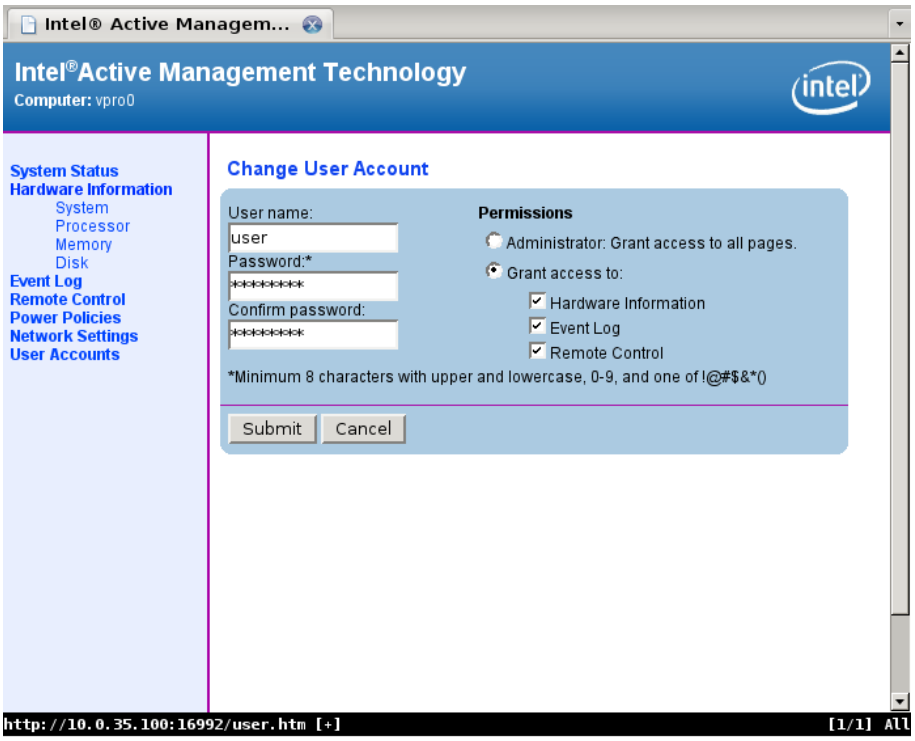

Intel® Active Managem...
Intel®Active Management Technology
Computer: vpro0
System Status
Hardware Information
System
Processor
Memory
Disk
Event Log
Remote Control
Power Policies
Network Settings
User Accounts
Power Policies
Select a power policy for Intel® AMT:
Desktop: ON in S0
Desktop: ON in S0, S3
Desktop: ON in S0, S3, S4-5
Desktop: ON in S0, ME WoL in S3
Desktop: ON in S0, ME WoL in S3, S4-5
Desktop: ON in S0, S3, S4-5, OFF After Power Loss
Desktop: ON in S0, ME WoL in S3, S4-5, OFF After Power Loss
Submit
http://10.0.35.100:16992/power.htm [+]
[1/1] Top


Intel® Active Managem...
Intel®Active Management Technology
Computer: vpro0
intel
System Status
Hardware Information
System
Processor
Memory
Disk
Event Log
Remote Control
Power Policies
Network Settings
User Accounts
Power Policies
Select a power policy for Intel® AMT:
Desktop: ON in S0
Desktop: ON in S0, S3
Desktop: ON in S0, S3, S4-5
Desktop: ON in S0, ME WoL in S3
Desktop: ON in S0, ME WoL in S3, S4-5
Desktop: ON in S0, S3, S4-5, OFF After Power Loss
Desktop: ON in S0, ME WoL in S3, S4-5, OFF After Power Loss
Submit
http://10.0.35.100:16992/power.htm [+]
[1/1] Top


Intel® Active Managem...
Intel®Active Management Technology
Computer: vpro0
intel
System Status
Hardware Information
System
Processor
Memory
Disk
Event Log
Remote Control
Power Policies
Network Settings
User Accounts
Network Settings
Configure Intel® Active Management Technology network settings for this computer.
Computer host name:
vpro0
Domain name:
unix.nt
Respond to ping
TCP/IP settings for wired connection
Obtain IP settings automatically
Use the following IP settings:
IP address:
10.0.35.100
Subnet mask:
255.0.0.0
Gateway address:
10.0.35.1
Preferred DNS address:
10.0.35.1
Alternate DNS address:
Use tagged VLAN
VLAN ID:
Submit
http://10.0.35.100:16992/ip.htm [+]
[1/1] Top


Intel® Active Managem...
Intel®Active Management Technology
Computer: vpro0
System Status
Hardware Information
System
Processor
Memory
Disk
Event Log
Remote Control
Power Policies
Network Settings
User Accounts
User Accounts
Manage Intel® AMT user accounts for this computer.
User names:
New...
Change...
Remove
Change Admin...
Anonymous access
Configure access for Intel AMT on this computer.
Allow anonymous access for local user notification
Allow anonymous access for endpoint access control
Submit
http://10.0.35.100:16992/acl.htm [+-]
[1/1] Top


Intel® Active Managem...
Intel®Active Management Technology
Computer: vpro0
System Status
Hardware Information
System
Processor
Memory
Disk
Event Log
Remote Control
Power Policies
Network Settings
User Accounts
User Accounts
User account added successfully.
Manage Intel® AMT user accounts for this computer.
User names:
user
New...
Change...
Remove
Change Admin...
Anonymous access
Configure access for Intel AMT on this computer.
Allow anonymous access for local user notification
Allow anonymous access for endpoint access control
Submit
http://10.0.35.100:16992/acl.htm?msg=65282 [+]
[1/1] Top


Intel® Active Managem...
Intel®Active Management Technology
Computer: vpro0
intel
System Status
Hardware Information
System
Processor
Memory
Disk
Event Log
Remote Control
Power Policies
Network Settings
User Accounts
Change User Account
User name:
user
Password:*
Confirm password:
Permissions
Administrator: Grant access to all pages.
Grant access to:
Hardware Information
Event Log
Remote Control
Minimum 8 characters with upper and lowercase, 0-9, and one of !@#$&()
Submit
Cancel
http://10.0.35.100:16992/user.htm [+]
[1/1] All

3 Использование AMT Commander

AMT Commander — одна из основных программ, входящих в комплект *AMT Developer Toolkit*, набора программного обеспечения Intel, предназначенного для демонстрации возможностей vPro и для разработки нового программного обеспечения, использующего vPro.

3.1 Инсталляция AMT Developer Toolkit

Необходимо установить в системе Microsoft .NET Framework (>=2.0). После этого необходимо скачать и установить Intel AMT Developer Toolkit.

В его состав входит несколько программ, главная из которых — **AMT Commander**, программа предназначенная для управления удалённой системой при помощи технологии AMT.

Список программ, входящих в состав AMT Developer Toolkit:

- **Intel AMT Commander** — основной инструмент для управления компьютером при помощи технологии Intel AMT;
- **Intel AMT Defender** — инструмент для создания и применения правил фильтрации сетевого трафика при помощи технологии Intel AMT;
- **Intel AMT Director** — инструмент для управления компьютерами по AMT в Enterprise режиме;
- **Intel AMT Guardpost** — легковесный Outpost, serial-агент;
- **Intel AMT Monitor** — программа, изображающая графически, в каком состояние находилось питание наблюдаемых компьютеров;
- **Intel AMT Outpost Service Control Panel** — панель для управления программой AMT Outpost, serial-агентом, который используется при доступе к компьютеру с помощью Serial-over-LAN.

Перед началом установки убедитесь, что в системе установлен *Microsoft Windows .NET Framework 2.0*. Установите .MSI-пакет AMT Developer Toolkit, полученный и сайта Intel или из другого надёжного источника.

При инсталляции используйте все значения предлагаемые инсталлятором. Будут установлены все компоненты Intel AMT Developer Toolkit.

После того как инсталляция закончена, можно запускать Intel AMT Commander.

Скриношоты процесса установки представлены ниже.

3.2 Использование AMT Commander

Добавьте компьютер (или множество компьютеров), которыми вы собираетесь управлять. При добавлении вы должны будете указать пароль, установленный в ходе настройки AMT через MBEx.

После того того как компьютер добавлен, для управления им нужно выполнить подключение к нему.

Для этого нажмите кнопку **Connect**. После того как соединение будет установлено, текст на кнопке **Connect** заменится на **Disconnect**. Вы можете нажать на эту кнопку, когда закончите работать с копьютером.

3.2.1 Управление питанием компьютера

Посмотрите информацию о компьютере, а также попробуйте с помощью AMT Commander выключить и включить его.

3.2.2 Перенаправление Serial-консоли

Для перенаправления Serial-консоли выберите в меню **Remote Command** и в нём перезагрузить с помощью команды **Reboot with Remoting**.

На экране должен появится вывод удалённого компьютера на консоль.

Если вы хотите использовать PuTTY для работы с консолью, нужно разместить файл `putty.exe` в каталоге с AMT Commander'ом.

3.2.3 Удалённая загрузка системы с помощью IDE-R

Если вы хотите загрузить удалённую систему с локального компакт-диска, воспользуйтесь технологией перенаправления IDE-R, предназначенной для перенаправления IDE поверх TCP/IP.

Нужно чтобы диск, с которого вы собираетесь загрузить удалённую систему, находился в приводе.

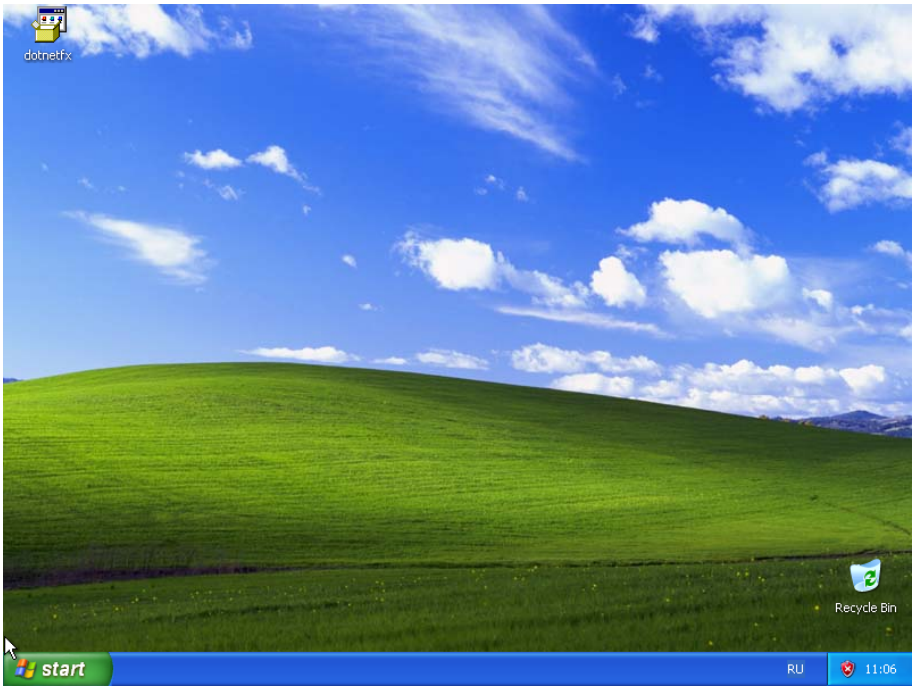
3.3 Дополнительная информация

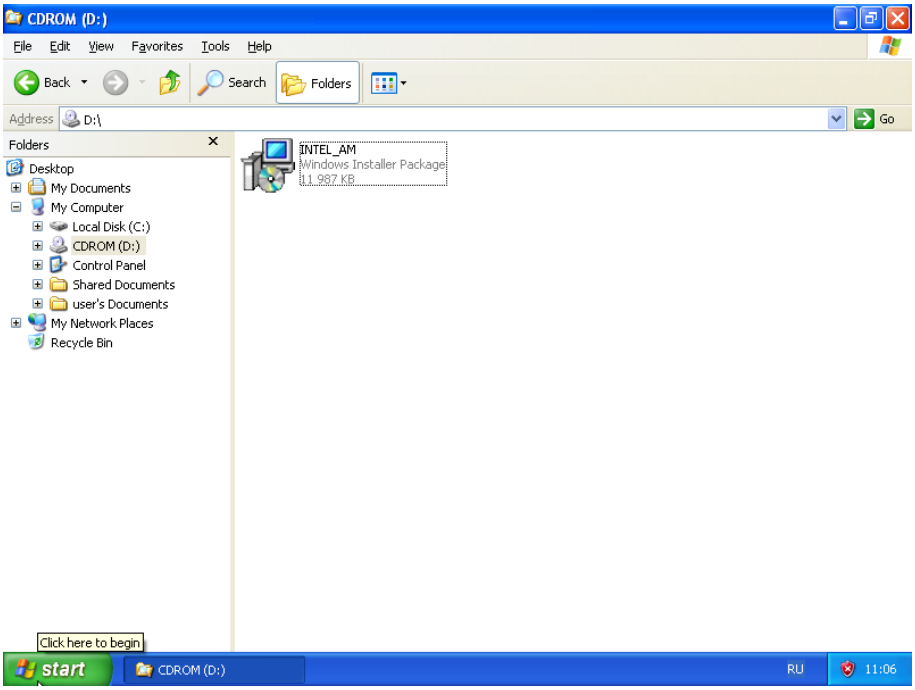
- Использование AMT Commander[4]
- Intel® AMT Developer Tool Kit (DTK)[5] (англ.) — домашняя страница
- Ylian Saint-hilaire (Intel)[6] (англ.) — блог ведущего разработчика Intel Developer Toolkit и Intel AMT Commander

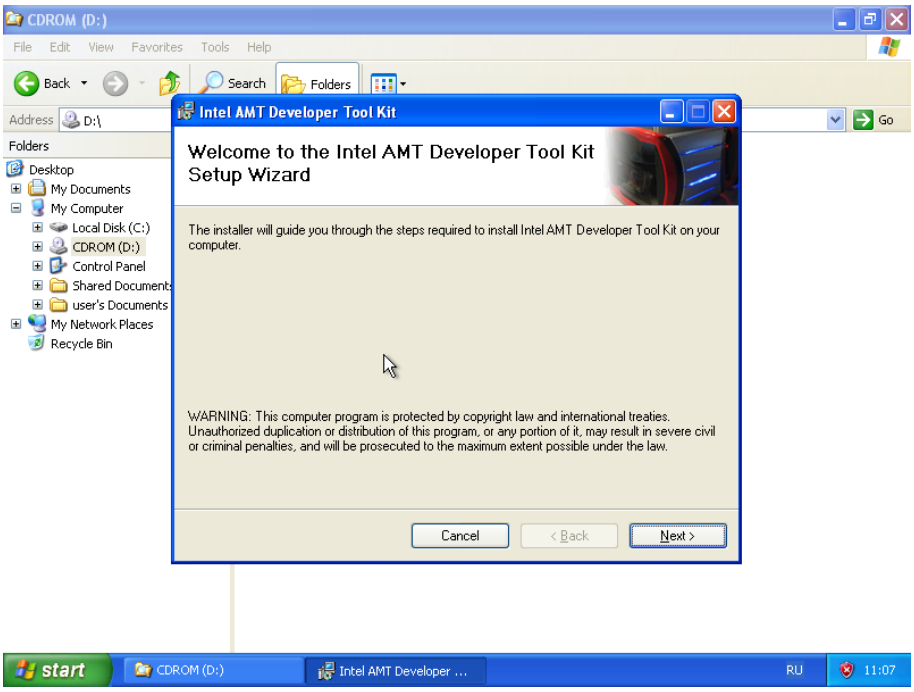
[4] http://xgu.ru/wiki/vpro/amt-dtk
[5] http://www.intel.com/software/amt-dtk/
[6] http://softwareblogs.intel.com/author/ylian-saint-hilaire/

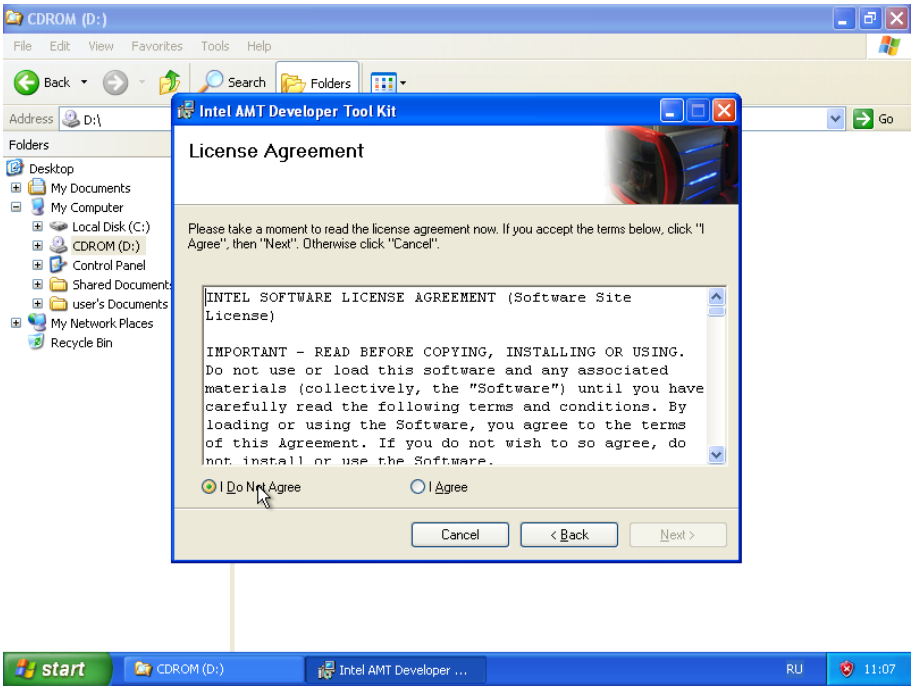
3.4 Скриншоты процесса инсталляции и использования AMT Developer Toolkit

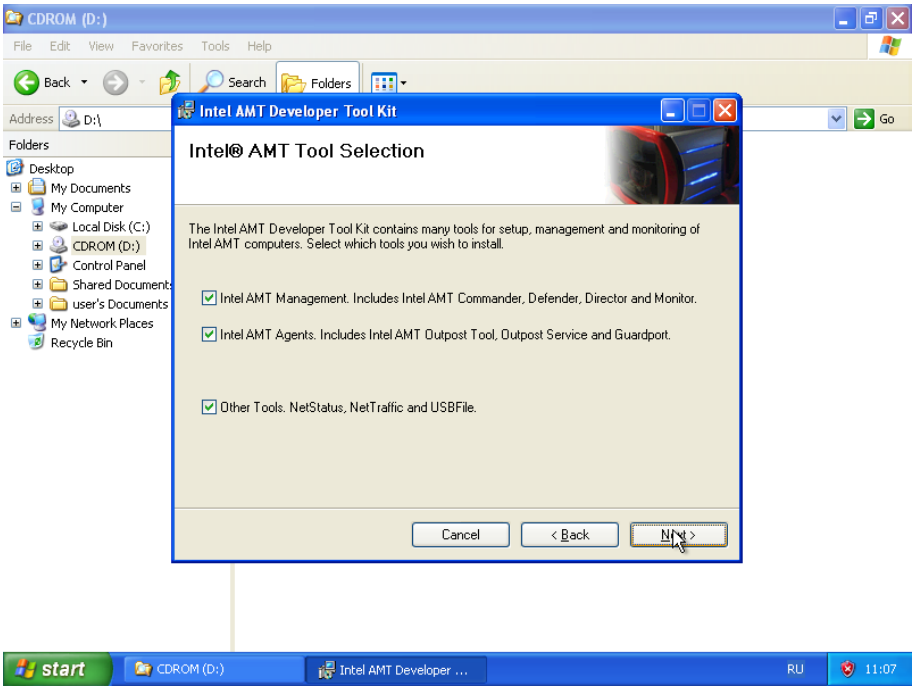
3.4.1 Установка AMT Developer Toolkit

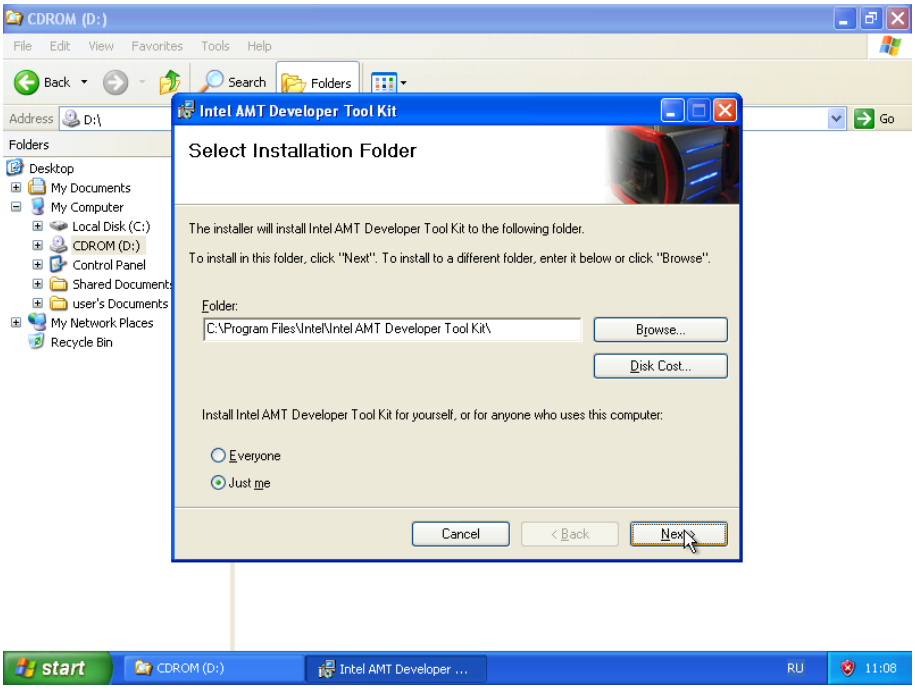


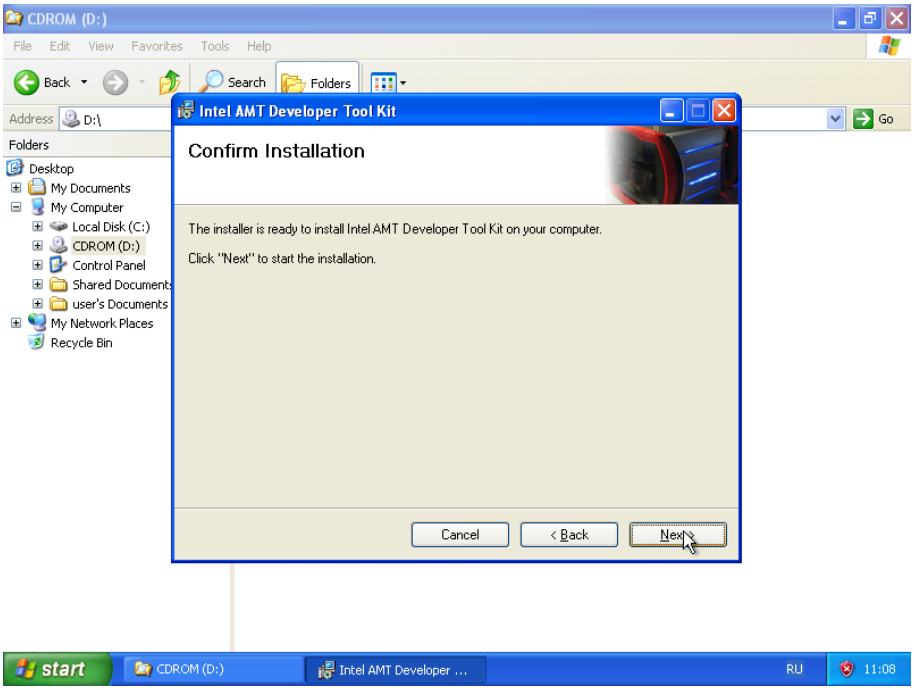


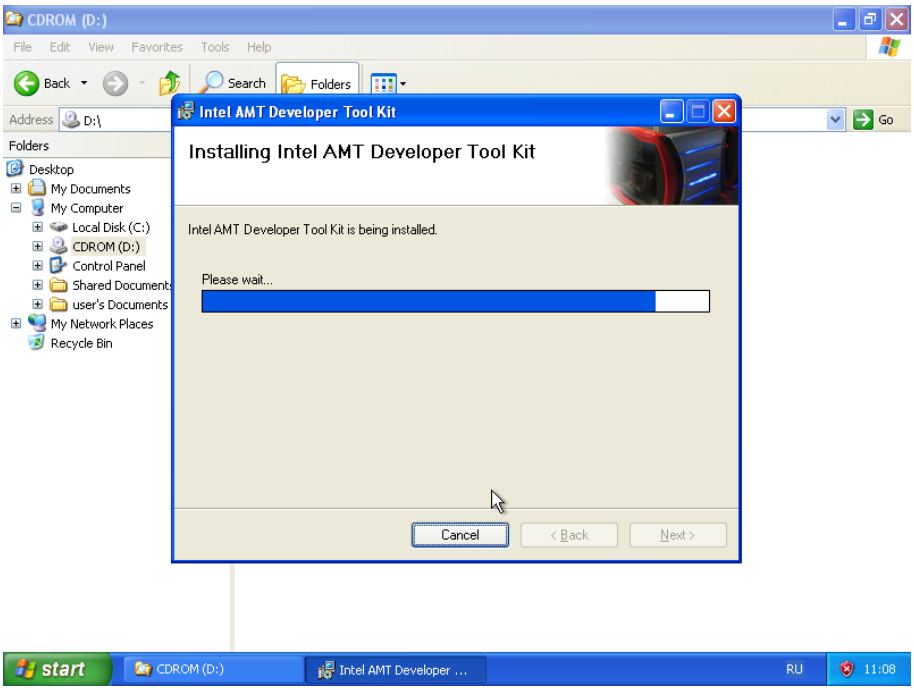

CDROM (D:)
File Edit View Favorites Tools Help
Back Search Folders
Address D:\
Go
Folders
Desktop
My Documents
My Computer
Local Disk (C:)
CDROM (D:)
Control Panel
Shared Documents
user's Documents
My Network Places
Recycle Bin
Intel AMT Developer Tool Kit
Welcome to the Intel AMT Developer Tool Kit Setup Wizard
The installer will guide you through the steps required to install Intel AMT Developer Tool Kit on your computer.
WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.
Cancel
< Back
Next >
start
CDROM (D:)
Intel AMT Developer ...
RU
11:07

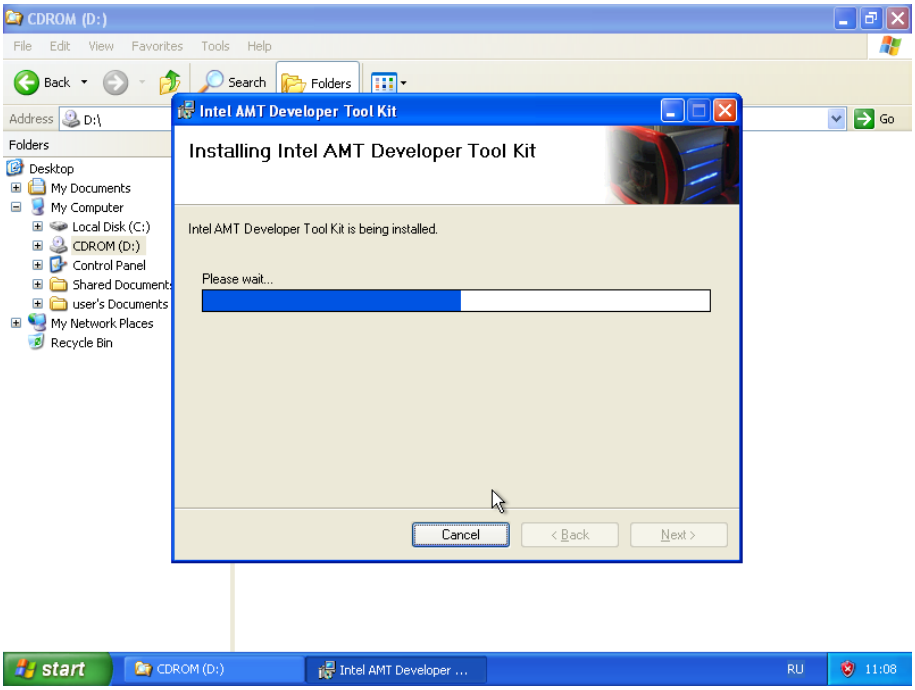

CDROM (D:)
File Edit View Favorites Tools Help
Back Search Folders
Address D:\
Go
Folders
Desktop
My Documents
My Computer
Local Disk (C:)
CDROM (D:)
Control Panel
Shared Documents
user's Documents
My Network Places
Recycle Bin
Intel AMT Developer Tool Kit
License Agreement
Please take a moment to read the license agreement now. If you accept the terms below, click "I Agree", then "Next". Otherwise click "Cancel".
INTEL SOFTWARE LICENSE AGREEMENT (Software Site License)
IMPORTANT - READ BEFORE COPYING, INSTALLING OR USING.
Do not use or load this software and any associated materials (collectively, the "Software") until you have carefully read the following terms and conditions. By loading or using the Software, you agree to the terms of this Agreement. If you do not wish to so agree, do
I Do Not Agree
I Agree
Cancel
< Back
Next >
start
CDROM (D:)
Intel AMT Developer ...
RU
11:07

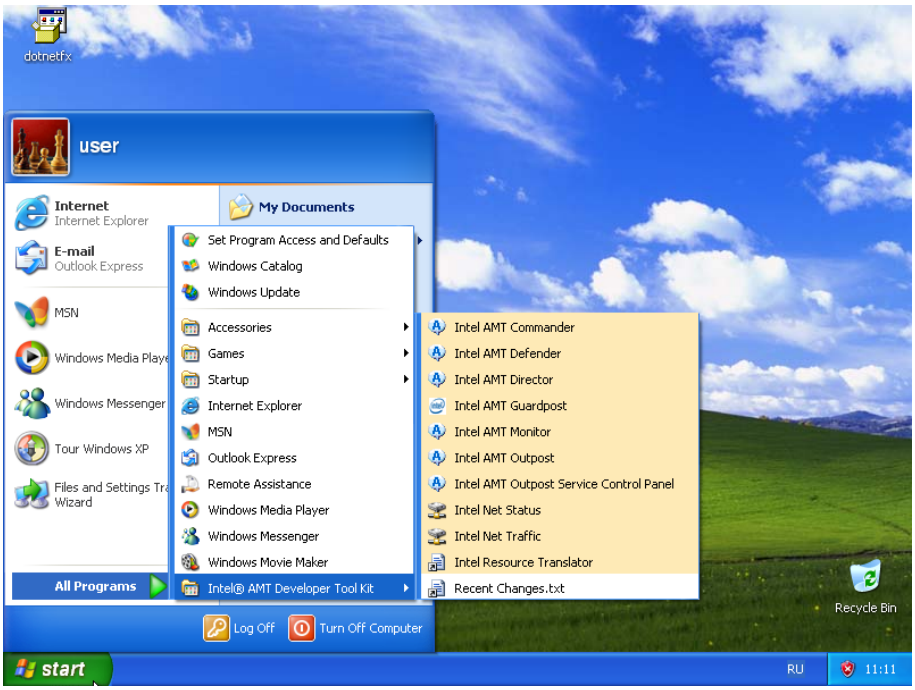

CDROM (D:)
File Edit View Favorites Tools Help
Back Search Folders
Address D:\
Go
Folders
Desktop
My Documents
My Computer
Local Disk (C:)
CDROM (D:)
Control Panel
Shared Documents
user's Documents
My Network Places
Recycle Bin
Intel AMT Developer Tool Kit
Intel® AMT Tool Selection
The Intel AMT Developer Tool Kit contains many tools for setup, management and monitoring of Intel AMT computers. Select which tools you wish to install.
Intel AMT Management. Includes Intel AMT Commander, Defender, Director and Monitor.
Intel AMT Agents. Includes Intel AMT Outpost Tool, Outpost Service and Guardport.
Other Tools. NetStatus, NetTraffic and USBFile.
Cancel
< Back
Next >
start
CDROM (D:)
Intel AMT Developer ...
RU
11:07


CDROM (D:)
File Edit View Favorites Tools Help
Back Search Folders
Address D:\
Go
Folders
Desktop
My Documents
My Computer
Local Disk (C:)
CDROM (D:)
Control Panel
Shared Documents
user's Documents
My Network Places
Recycle Bin
Intel AMT Developer Tool Kit
Select Installation Folder
The installer will install Intel AMT Developer Tool Kit to the following folder.
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".
Folder:
C:\Program Files\Intel\Intel AMT Developer Tool Kit\
Browse...
Disk Cost...
Install Intel AMT Developer Tool Kit for yourself, or for anyone who uses this computer:
Everyone
Just me
Cancel
< Back
Next >
start
CDROM (D:)
Intel AMT Developer ...
RU
11:08

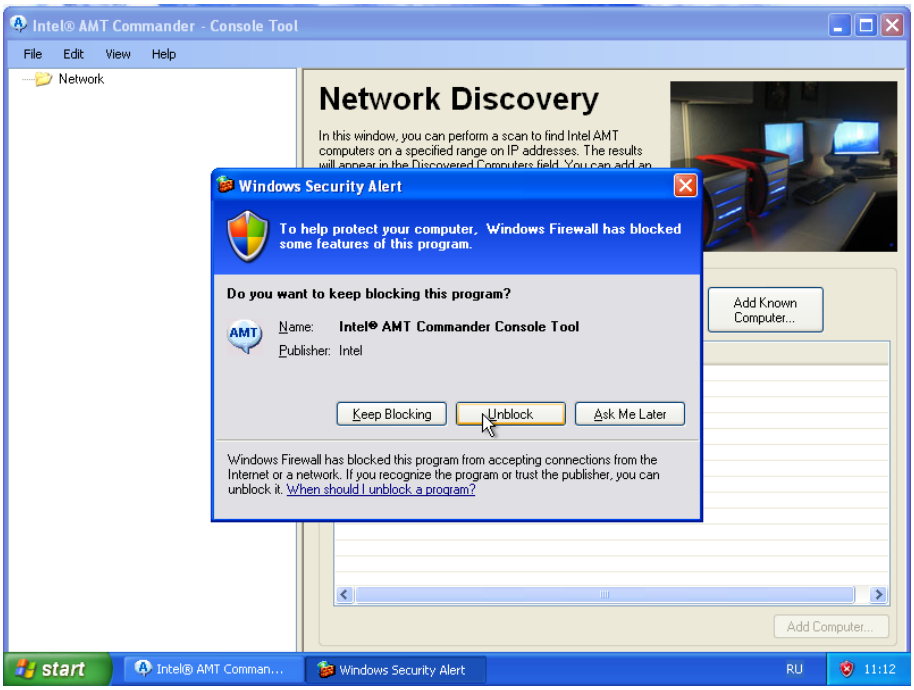

CDROM (D:)
File Edit View Favorites Tools Help
Back Search Folders
Address D:\
Go
Folders
Desktop
My Documents
My Computer
Local Disk (C:)
CDROM (D:)
Control Panel
Shared Documents
user's Documents
My Network Places
Recycle Bin
Intel AMT Developer Tool Kit
Confirm Installation
The installer is ready to install Intel AMT Developer Tool Kit on your computer.
Click "Next" to start the installation.
Cancel
< Back
Next
start
CDROM (D:)
Intel AMT Developer ...
RU
11:08

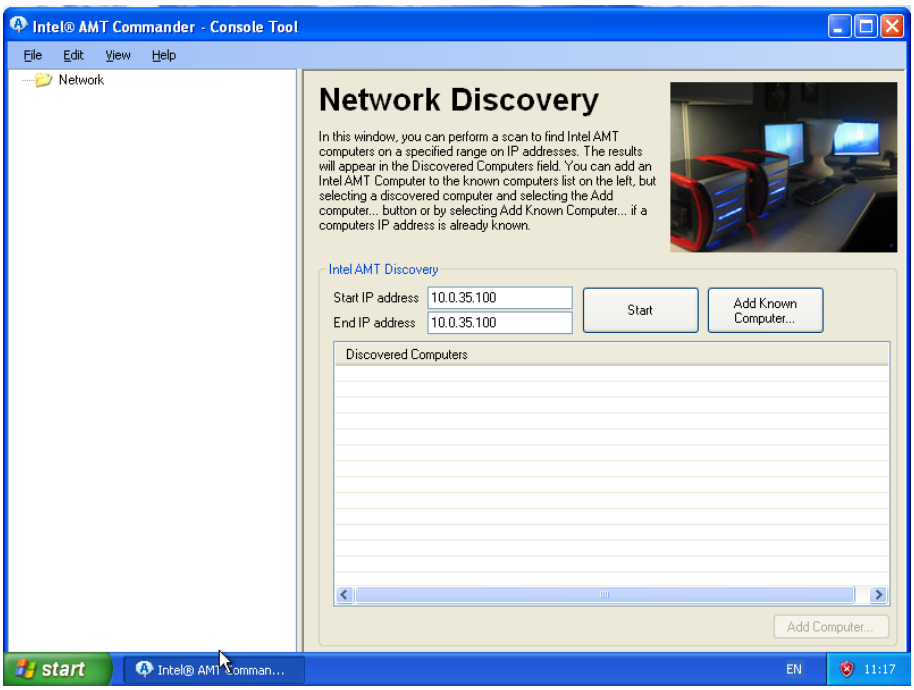

CDROM (D:)
File Edit View Favorites Tools Help
Back Search Folders
Address D:\
Go
Folders
Desktop
My Documents
My Computer
Local Disk (C:)
CDROM (D:)
Control Panel
Shared Documents
user's Documents
My Network Places
Recycle Bin
Intel AMT Developer Tool Kit
Installing Intel AMT Developer Tool Kit
Intel AMT Developer Tool Kit is being installed.
Please wait...
Cancel
< Back
Next >
start
CDROM (D:)
Intel AMT Developer ...
RU
11:08

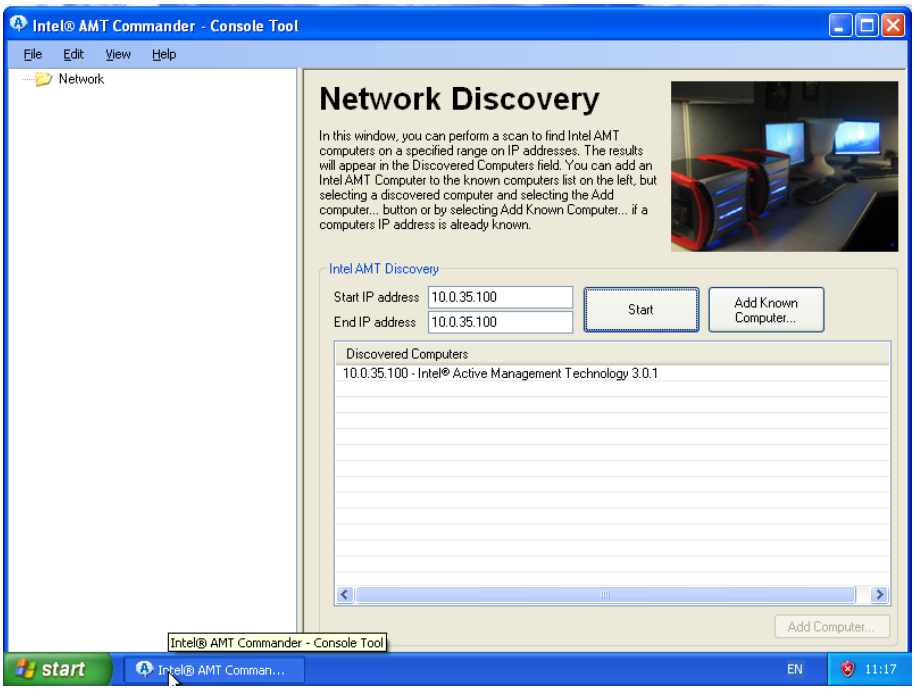

CDROM (D:)
File Edit View Favorites Tools Help
Back Search Folders
Address D:\
Go
Folders
Desktop
My Documents
My Computer
Local Disk (C:)
CDROM (D:)
Control Panel
Shared Documents
user's Documents
My Network Places
Recycle Bin
Intel AMT Developer Tool Kit
Installing Intel AMT Developer Tool Kit
Intel AMT Developer Tool Kit is being installed.
Please wait...
Cancel
< Back
Next >
start
CDROM (D:)
Intel AMT Developer ...
RU
11:08

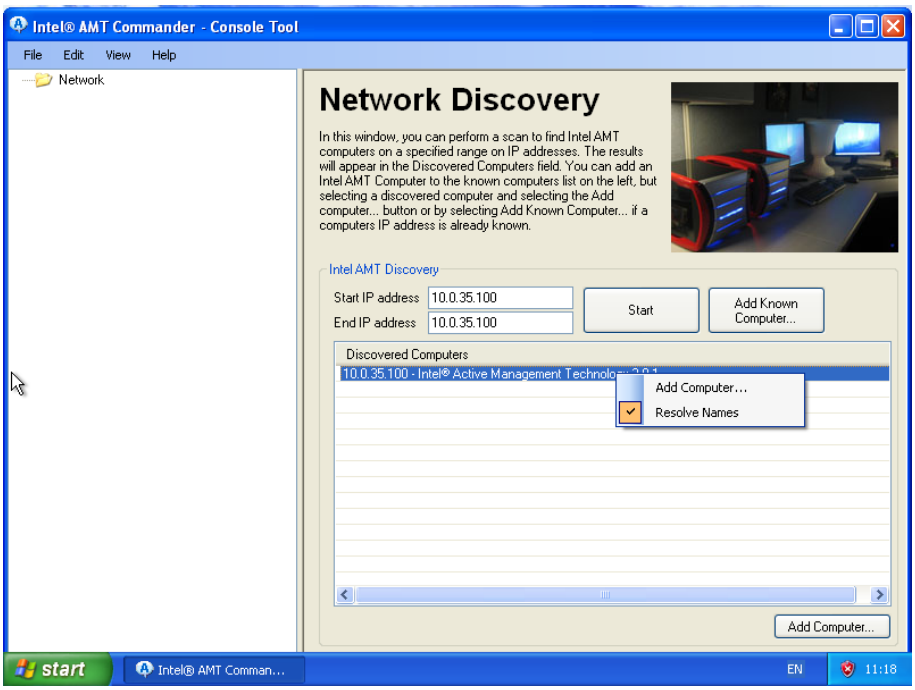

dotnetfx
user
Internet
Internet Explorer
E-mail
Outlook Express
MSN
Windows Media Player
Windows Messenger
Tour Windows XP
Files and Settings Transfer Wizard
My Documents
Set Program Access and Defaults
Windows Catalog
Windows Update
Accessories
Games
Startup
Internet Explorer
MSN
Outlook Express
Remote Assistance
Windows Media Player
Windows Messenger
Windows Movie Maker
All Programs
Intel® AMT Developer Tool Kit
Intel AMT Commander
Intel AMT Defender
Intel AMT Director
Intel AMT Guardpost
Intel AMT Monitor
Intel AMT Outpost
Intel AMT Outpost Service Control Panel
Intel Net Status
Intel Net Traffic
Intel Resource Translator
Recent Changes.txt
Log Off
Turn Off Computer
Recycle Bin
start
RU
11:11

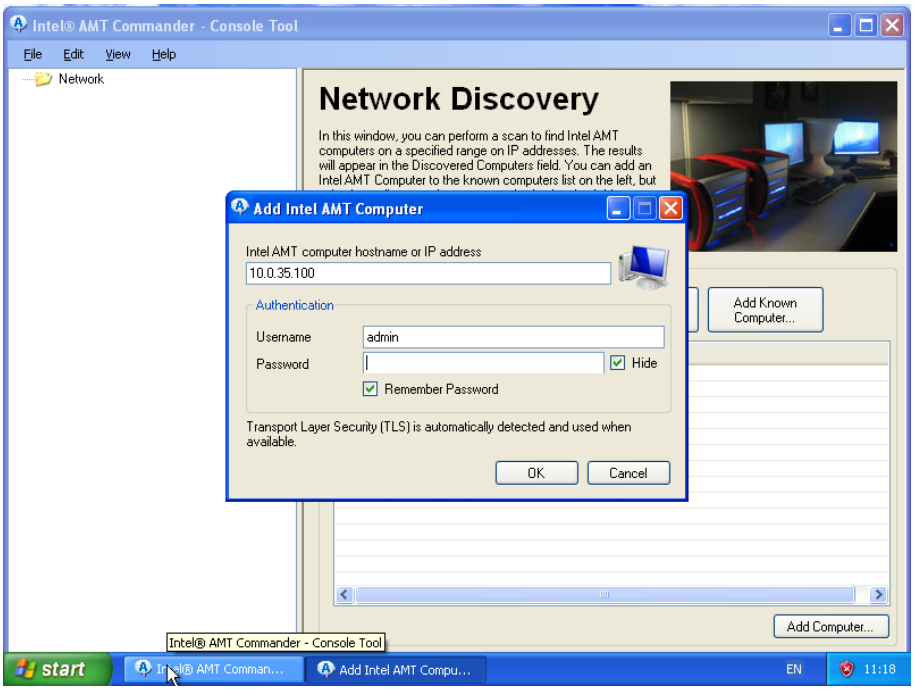
3.4.2 Использование Intel AMT Commander

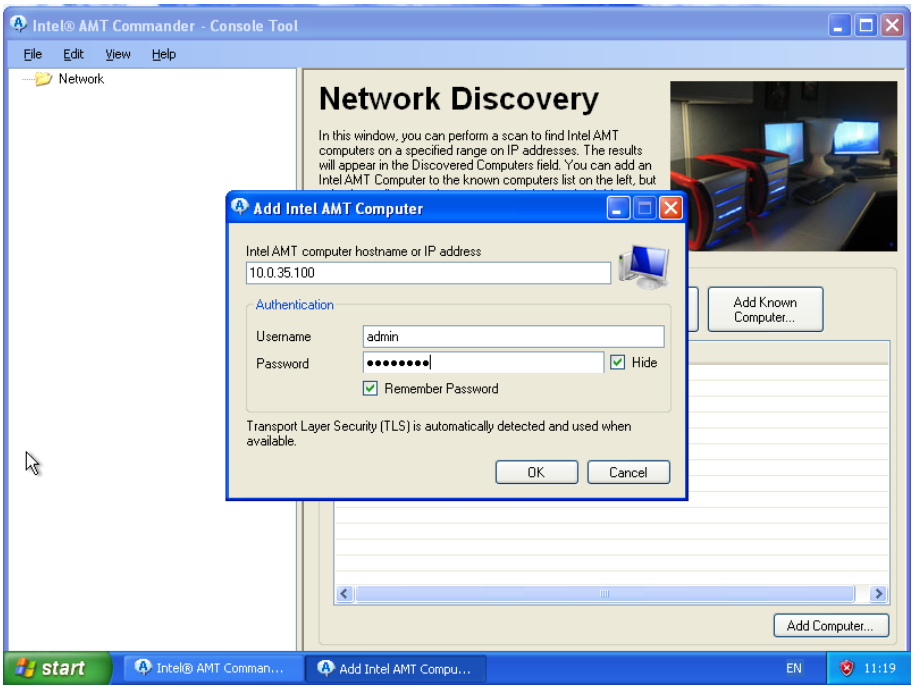


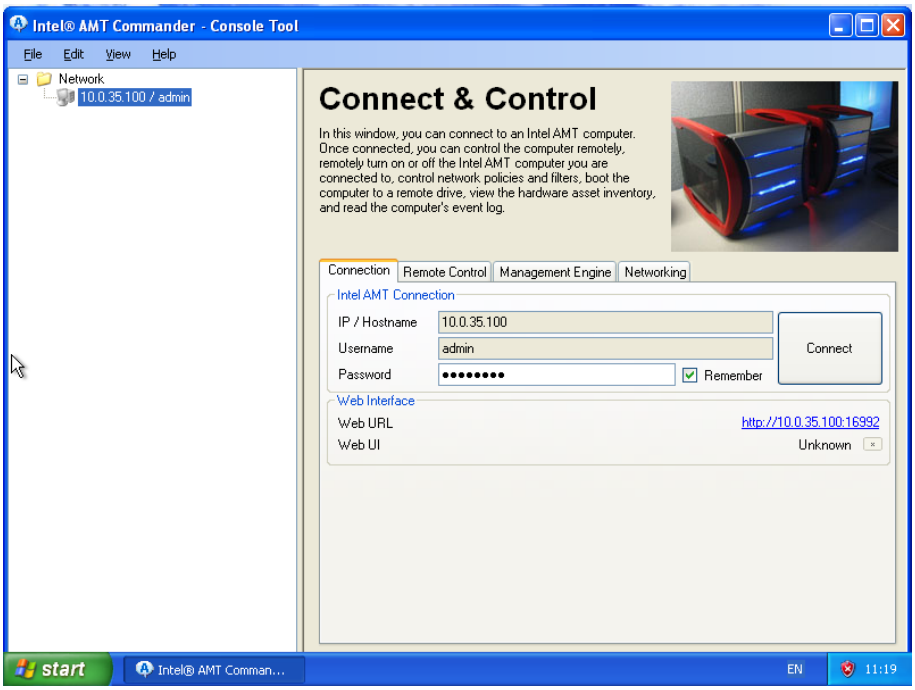


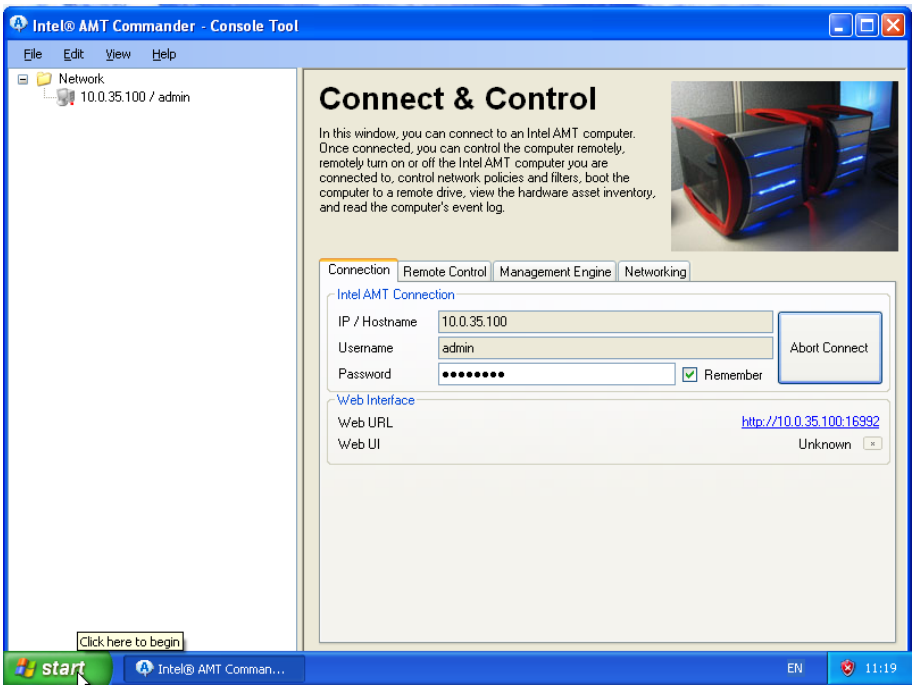

Intel® AMT Commander - Console Tool
File Edit View Help
Network
Network Discovery
In this window, you can perform a scan to find Intel AMT computers on a specified range on IP addresses. The results will appear in the Discovered Computers field. You can add an Intel AMT Computer to the known computers list on the left, but selecting a discovered computer and selecting the Add computer... button or by selecting Add Known Computer... if a computers IP address is already known.
Intel AMT Discovery
Start IP address 10.0.35.100
End IP address 10.0.35.100
Start
Add Known Computer...
Discovered Computers
10.0.35.100 - Intel® Active Management Technology 3.0.1
Add Computer...
Intel® AMT Commander - Console Tool
start
Intel® AMT Comman...
EN
11:17

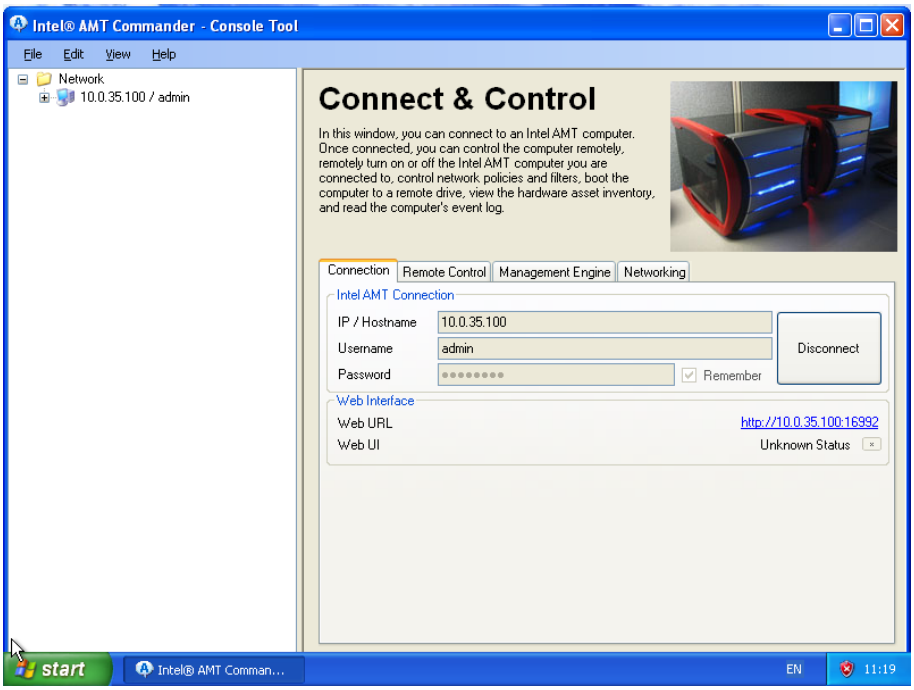

Intel® AMT Commander - Console Tool
File Edit View Help
Network
Network Discovery
In this window, you can perform a scan to find Intel AMT computers on a specified range on IP addresses. The results will appear in the Discovered Computers field. You can add an Intel AMT Computer to the known computers list on the left, but selecting a discovered computer and selecting the Add computer... button or by selecting Add Known Computer... if a computers IP address is already known.
Intel AMT Discovery
Start IP address 10.0.35.100
End IP address 10.0.35.100
Start
Add Known Computer...
Discovered Computers
10.0.35.100 - Intel® Active Management Technology
Add Computer...
Resolve Names
Add Computer...
start
Intel® AMT Comman...
EN
11:18

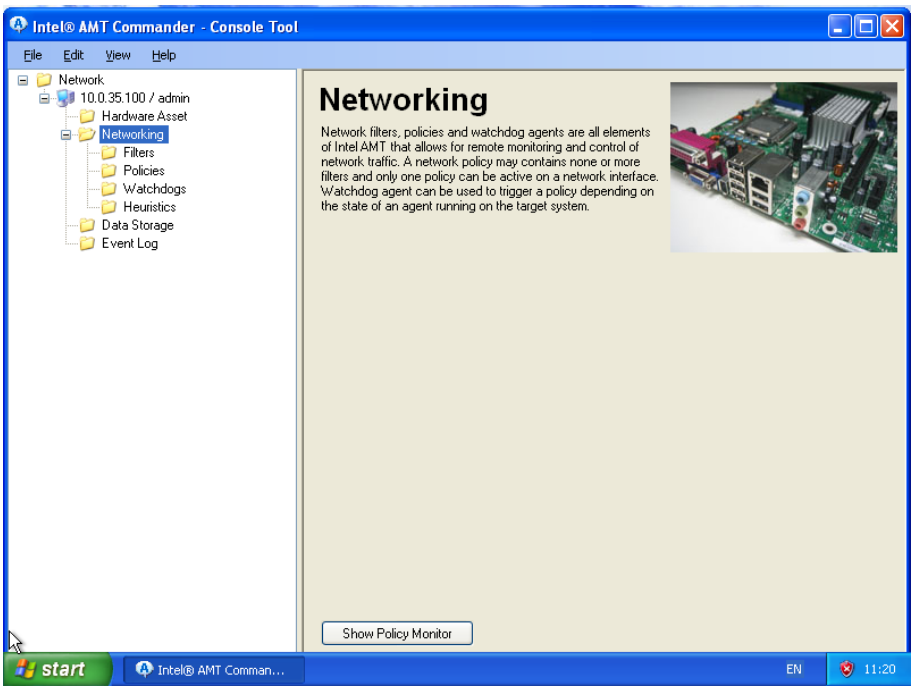

Intel® AMT Commander - Console Tool
File Edit View Help
Network
Network Discovery
In this window, you can perform a scan to find Intel AMT computers on a specified range on IP addresses. The results will appear in the Discovered Computers field. You can add an Intel AMT Computer to the known computers list on the left, but
Add Known Computer...
Add Intel AMT Computer
Intel AMT computer hostname or IP address
10.0.35.100
Authentication
Username
admin
Password
Hide
Remember Password
Transport Layer Security (TLS) is automatically detected and used when available.
OK
Cancel
Add Computer...
Intel® AMT Commander - Console Tool
start
Intel® AMT Comman...
Add Intel AMT Compu...
EN
11:18

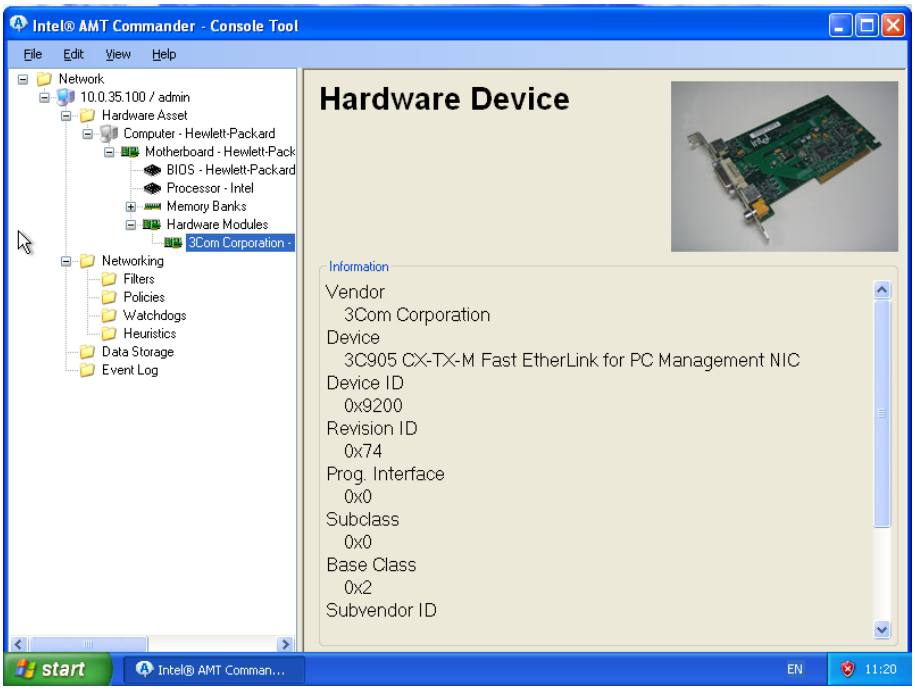

Intel® AMT Commander - Console Tool
File Edit View Help
Network
Network Discovery
In this window, you can perform a scan to find Intel AMT computers on a specified range on IP addresses. The results will appear in the Discovered Computers field. You can add an Intel AMT Computer to the known computers list on the left, but
Add Known Computer...
Add Intel AMT Computer
Intel AMT computer hostname or IP address
10.0.35.100
Authentication
Username
admin
Password
Hide
Remember Password
Transport Layer Security (TLS) is automatically detected and used when available.
OK
Cancel
Add Computer...
start
Intel® AMT Comman...
Add Intel AMT Compu...
EN
11:19

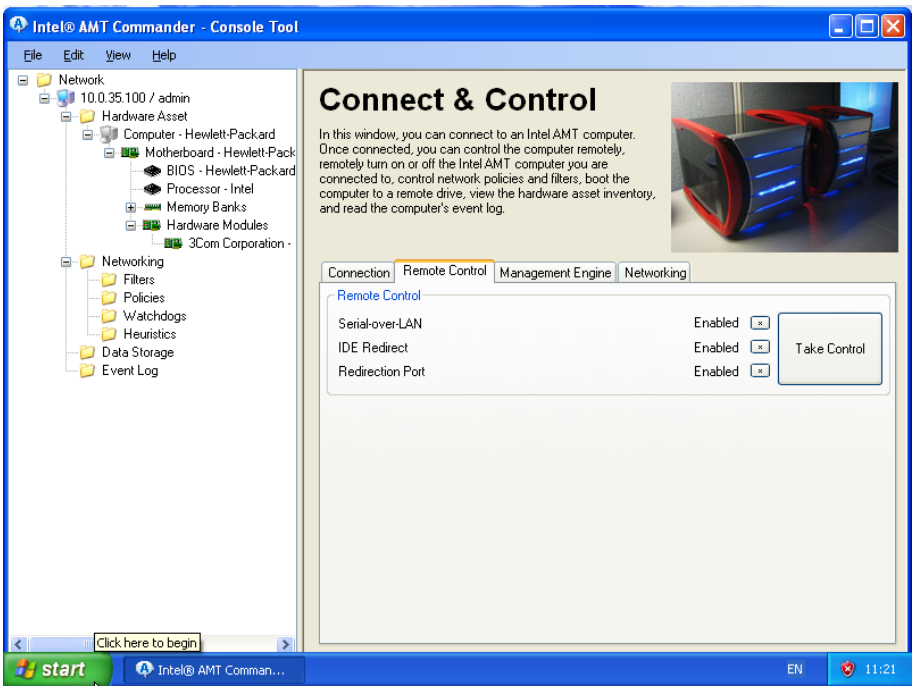

Intel® AMT Commander - Console Tool
File Edit View Help
Network
10.0.35.100 / admin
Connect & Control
In this window, you can connect to an Intel AMT computer. Once connected, you can control the computer remotely, remotely turn on or off the Intel AMT computer you are connected to, control network policies and filters, boot the computer to a remote drive, view the hardware asset inventory, and read the computer's event log.
Connection
Remote Control
Management Engine
Networking
Intel AMT Connection
IP / Hostname
10.0.35.100
Username
admin
Password
Remember
Connect
Web Interface
Web URL
http://10.0.35.100:16992
Web UI
Unknown
start
Intel® AMT Comman...
EN
11:19

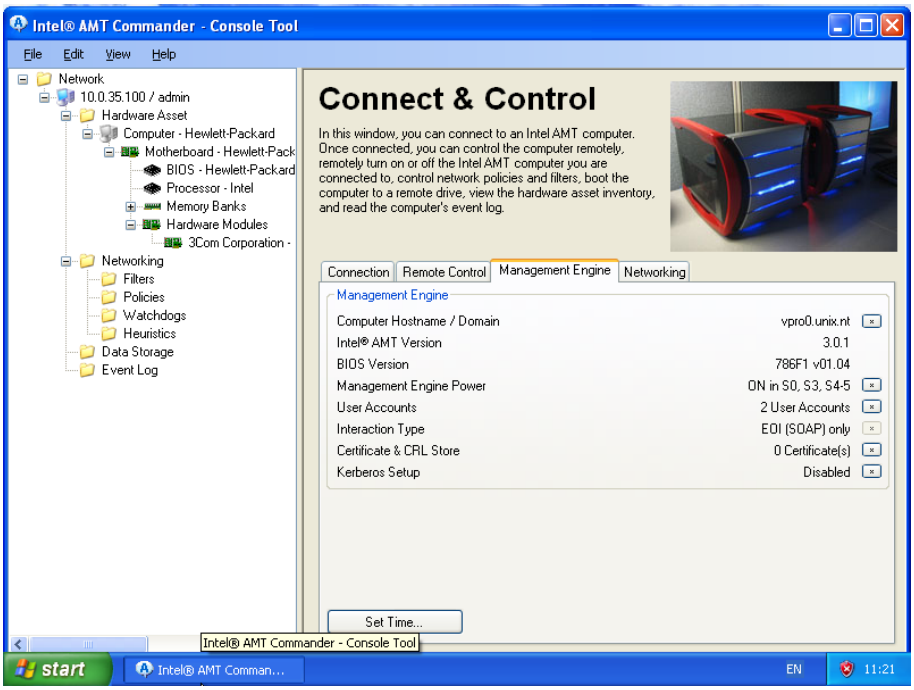

Intel® AMT Commander - Console Tool
File Edit View Help
Network
10.0.35.100 / admin
Connect & Control
In this window, you can connect to an Intel AMT computer. Once connected, you can control the computer remotely, remotely turn on or off the Intel AMT computer you are connected to, control network policies and filters, boot the computer to a remote drive, view the hardware asset inventory, and read the computer's event log.
Connection
Remote Control
Management Engine
Networking
Intel AMT Connection
IP / Hostname
10.0.35.100
Username
admin
Password
Remember
Abort Connect
Web Interface
Web URL
http://10.0.35.100:16992
Web UI
Unknown
Click here to begin
start
Intel® AMT Comman...
EN
11:19

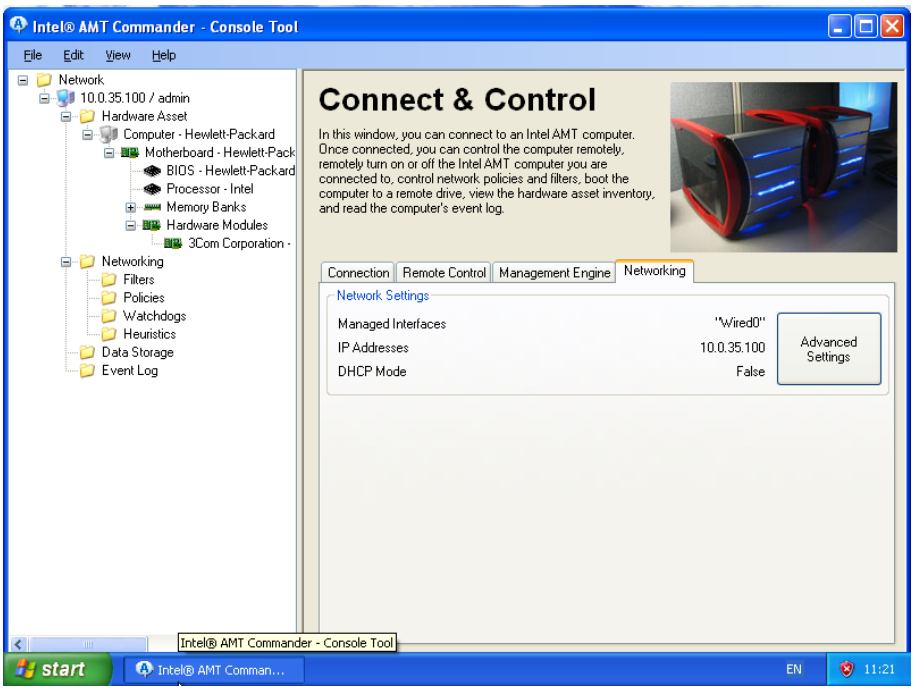

Intel® AMT Commander - Console Tool
File Edit View Help
Network
10.0.35.100 / admin
Connect & Control
In this window, you can connect to an Intel AMT computer. Once connected, you can control the computer remotely, remotely turn on or off the Intel AMT computer you are connected to, control network policies and filters, boot the computer to a remote drive, view the hardware asset inventory, and read the computer's event log.
Connection
Remote Control
Management Engine
Networking
Intel AMT Connection
IP / Hostname
10.0.35.100
Username
admin
Password
Remember
Disconnect
Web Interface
Web URL
http://10.0.35.100:16992
Web UI
Unknown Status
start
Intel® AMT Comman...
EN
11:19


Intel® AMT Commander - Console Tool
File Edit View Help
Network
10.0.35.100 / admin
Hardware Asset
Networking
Filters
Policies
Watchdogs
Heuristics
Data Storage
Event Log
Networking
Network filters, policies and watchdog agents are all elements of Intel AMT that allows for remote monitoring and control of network traffic. A network policy may contains none or more filters and only one policy can be active on a network interface. Watchdog agent can be used to trigger a policy depending on the state of an agent running on the target system.
Show Policy Monitor
start
Intel® AMT Comman...
EN
11:20

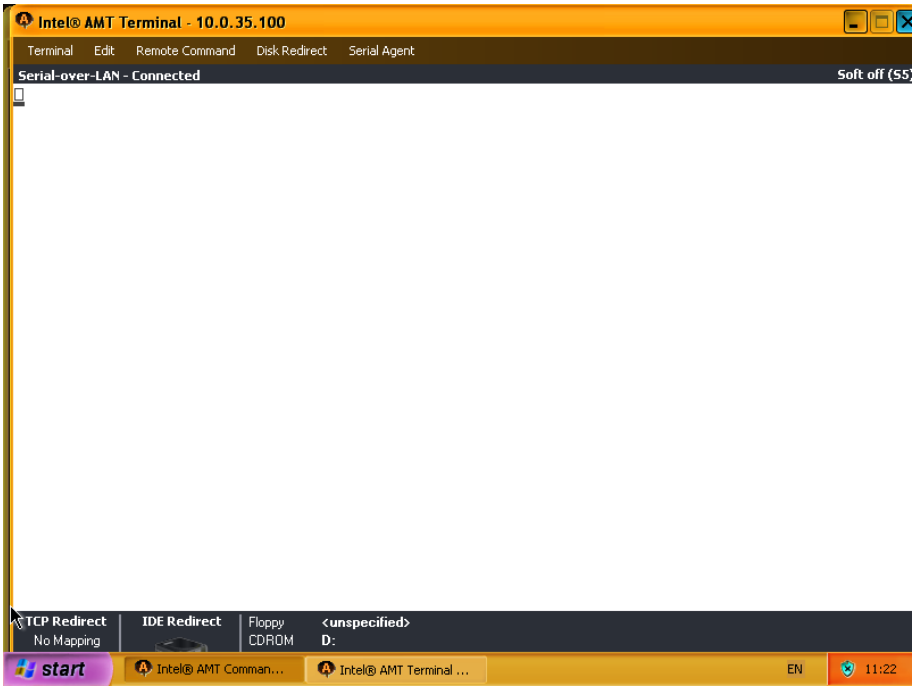

Intel® AMT Commander - Console Tool
File Edit View Help
Network
10.0.35.100 / admin
Hardware Asset
Computer - Hewlett-Packard
Motherboard - Hewlett-Pack
BIOS - Hewlett-Packard
Processor - Intel
Memory Banks
Hardware Modules
3Com Corporation -
Networking
Filters
Policies
Watchdogs
Heuristics
Data Storage
Event Log
Hardware Device
Information
Vendor
3Com Corporation
Device
3C905 CX-TX-M Fast EtherLink for PC Management NIC
Device ID
0x9200
Revision ID
0x74
Prog. Interface
0x0
Subclass
0x0
Base Class
0x2
Subvendor ID
start
Intel® AMT Comman...
EN
11:20

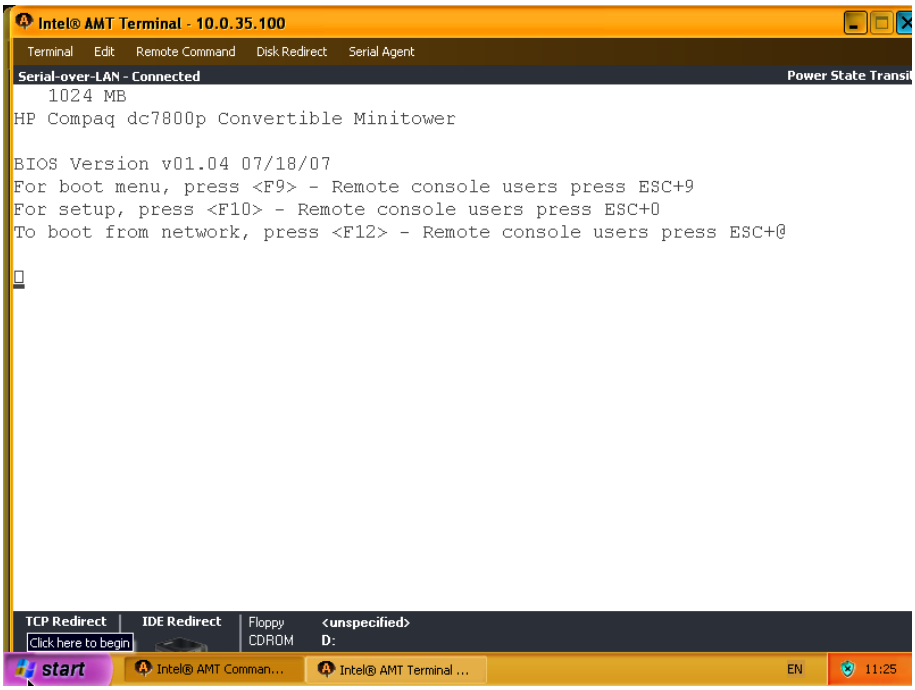

Intel® AMT Commander - Console Tool
File Edit View Help
Network
10.0.35.100 / admin
Hardware Asset
Computer - Hewlett-Packard
Motherboard - Hewlett-Pack
BIOS - Hewlett-Packard
Processor - Intel
Memory Banks
Hardware Modules
3Com Corporation -
Networking
Filters
Policies
Watchdogs
Heuristics
Data Storage
Event Log
Connect & Control
In this window, you can connect to an Intel AMT computer. Once connected, you can control the computer remotely, remotely turn on or off the Intel AMT computer you are connected to, control network policies and filters, boot the computer to a remote drive, view the hardware asset inventory, and read the computer's event log.
Connection
Remote Control
Management Engine
Networking
Remote Control
Serial-over-LAN
Enabled
IDE Redirect
Enabled
Redirection Port
Enabled
Take Control
Click here to begin
start
Intel® AMT Comman...
EN
11:21

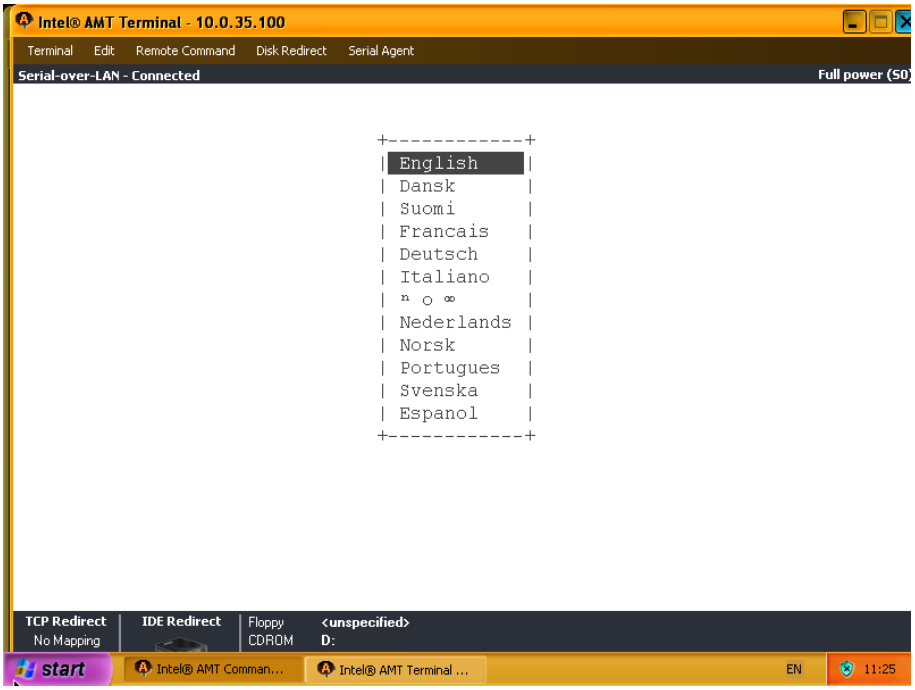

Intel® AMT Commander - Console Tool
File Edit View Help
Network
10.0.35.100 / admin
Hardware Asset
Computer - Hewlett-Packard
Motherboard - Hewlett-Pack
BIOS - Hewlett-Packard
Processor - Intel
Memory Banks
Hardware Modules
3Com Corporation -
Networking
Filters
Policies
Watchdogs
Heuristics
Data Storage
Event Log
Connect & Control
In this window, you can connect to an Intel AMT computer. Once connected, you can control the computer remotely, remotely turn on or off the Intel AMT computer you are connected to, control network policies and filters, boot the computer to a remote drive, view the hardware asset inventory, and read the computer's event log.
Connection
Remote Control
Management Engine
Networking
Management Engine
Computer Hostname / Domain
vpro0.unix.nt
Intel® AMT Version
3.0.1
BIOS Version
786F1 v01.04
Management Engine Power
ON in S0, S3, S4-5
User Accounts
2 User Accounts
Interaction Type
EOI (SOAP) only
Certificate & CRL Store
0 Certificate(s)
Kerberos Setup
Disabled
Set Time...
Intel® AMT Commander - Console Tool
start
Intel® AMT Comman...
EN
11:21

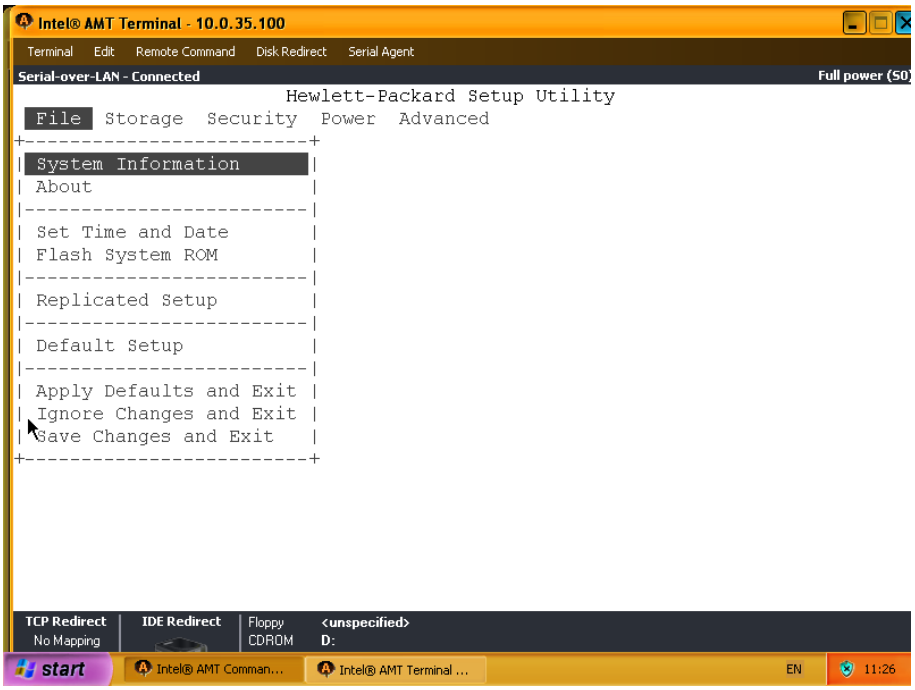

Intel® AMT Commander - Console Tool
File Edit View Help
Network
10.0.35.100 / admin
Hardware Asset
Computer - Hewlett-Packard
Motherboard - Hewlett-Pack
BIOS - Hewlett-Packard
Processor - Intel
Memory Banks
Hardware Modules
3Com Corporation -
Networking
Filters
Policies
Watchdogs
Heuristics
Data Storage
Event Log
Connect & Control
In this window, you can connect to an Intel AMT computer. Once connected, you can control the computer remotely, remotely turn on or off the Intel AMT computer you are connected to, control network policies and filters, boot the computer to a remote drive, view the hardware asset inventory, and read the computer's event log.
Connection
Remote Control
Management Engine
Networking
Network Settings
Managed Interfaces
"Wired0"
IP Addresses
10.0.35.100
DHCP Mode
False
Advanced Settings
Intel® AMT Commander - Console Tool
start
Intel® AMT Comman...
EN
11:21

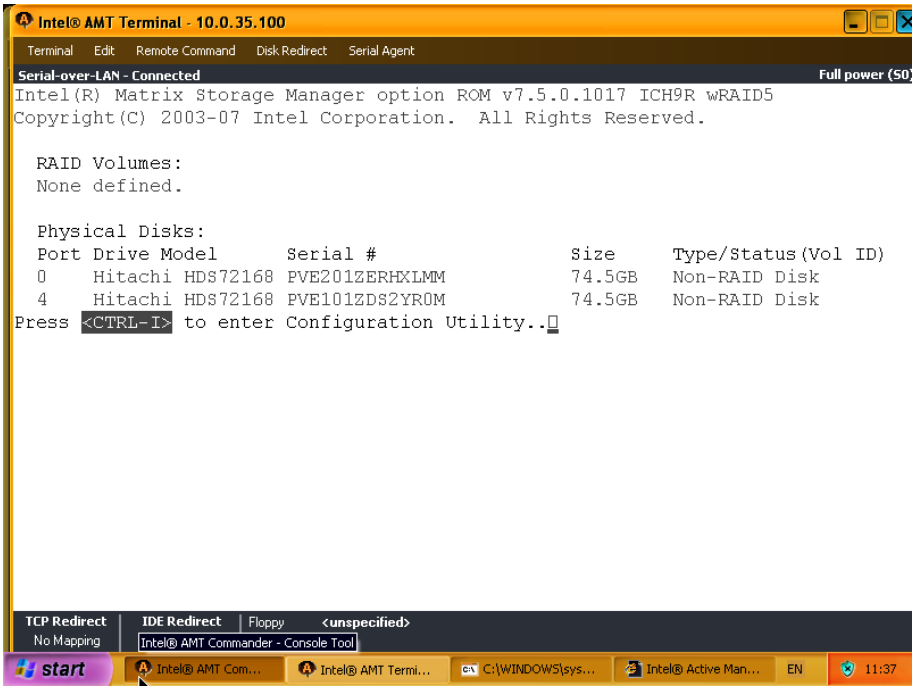
3.4.3 Перенаправление последовательного порта

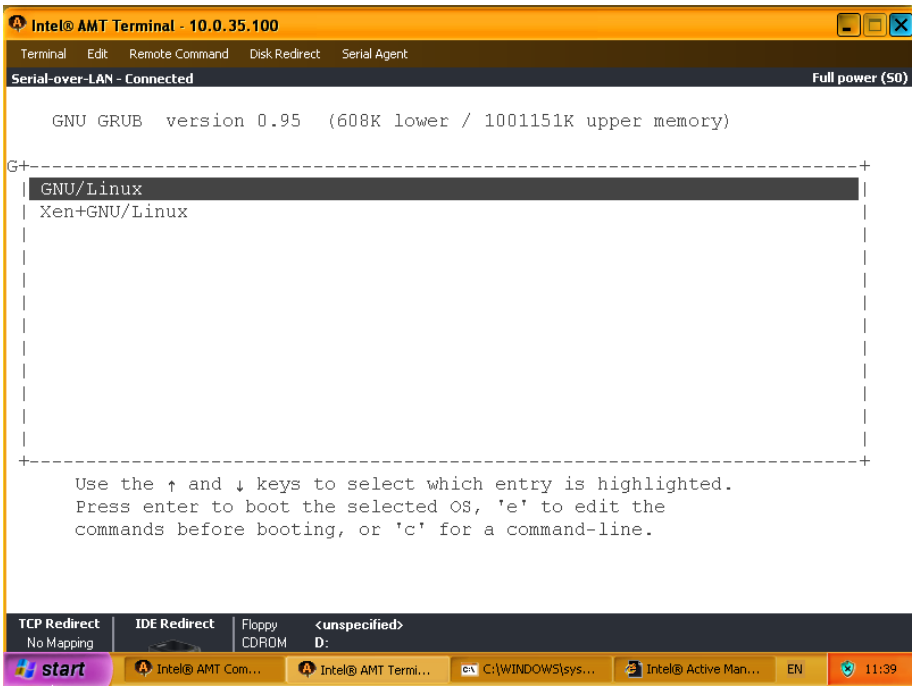


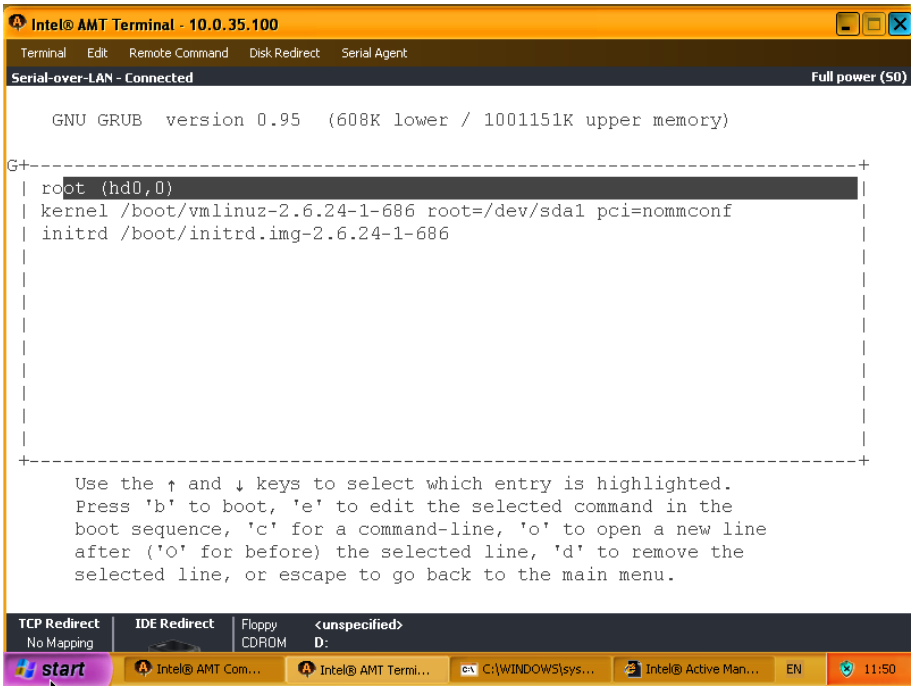


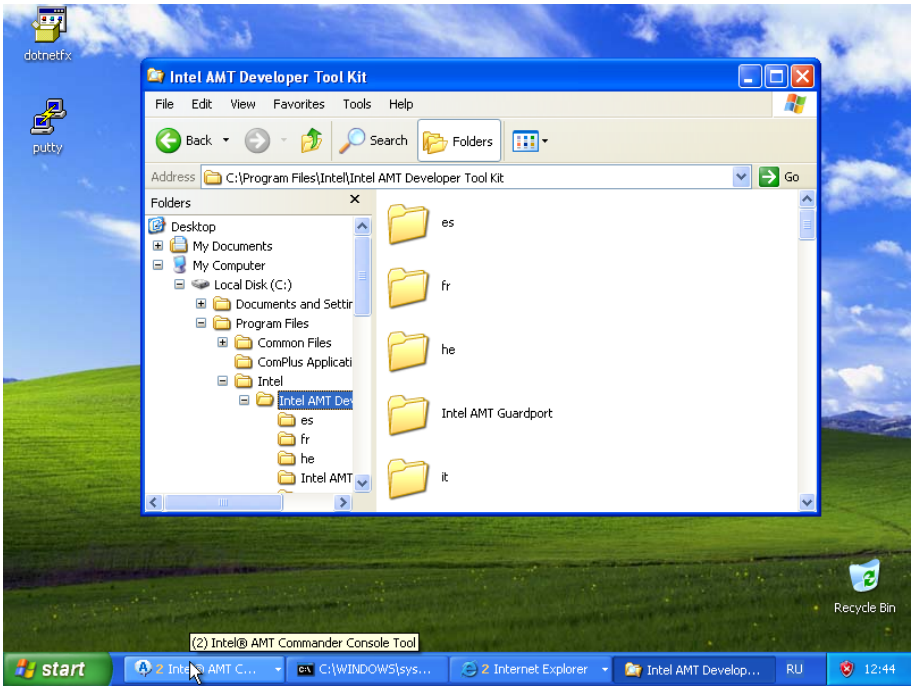

Intel® AMT Terminal - 10.0.35.100
Terminal Edit Remote Command Disk Redirect Serial Agent
Serial-over-LAN - Connected
Full power (S0)
English
Dansk
Suomi
Francais
Deutsch
Italiano
Nederlands
Norsk
Portugues
Svenska
Espanol
TCP Redirect
No Mapping
IDE Redirect
Floppy
CDROM
<unspecified>
D:
start
Intel® AMT Comman...
Intel® AMT Terminal ...
EN
11:25


Intel® AMT Terminal - 10.0.35.100
Terminal Edit Remote Command Disk Redirect Serial Agent
Serial-over-LAN - Connected
Full power (S0)
Hewlett-Packard Setup Utility
File Storage Security Power Advanced
System Information
About
Set Time and Date
Flash System ROM
Replicated Setup
Default Setup
Apply Defaults and Exit
Ignore Changes and Exit
Save Changes and Exit
TCP Redirect
No Mapping
IDE Redirect
Floppy
CDROM
<unspecified>
D:
start
Intel® AMT Comman...
Intel® AMT Terminal ...
EN
11:26

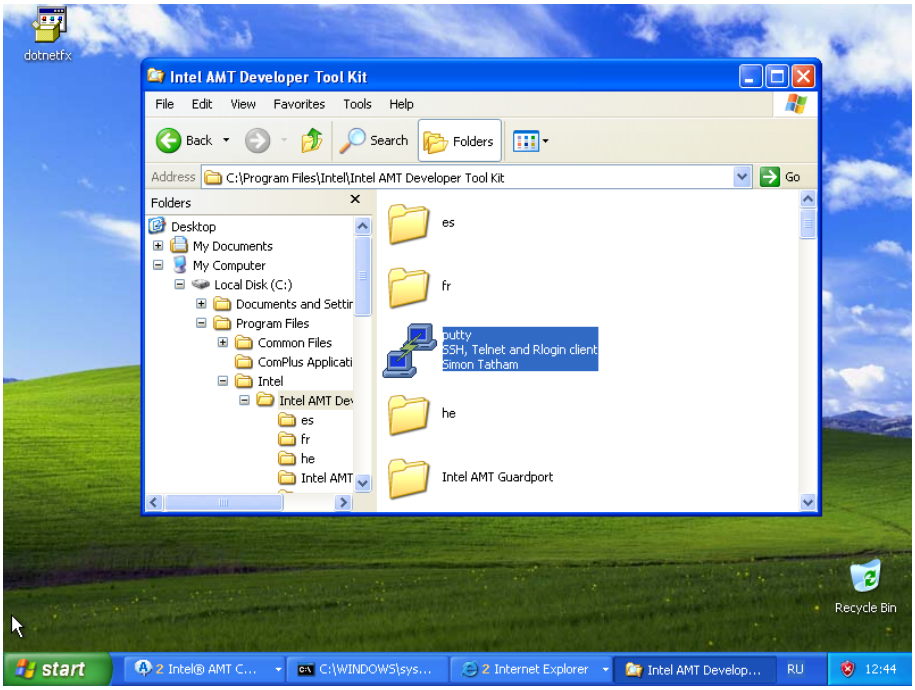

Intel® AMT Terminal - 10.0.35.100
Terminal Edit Remote Command Disk Redirect Serial Agent
Serial-over-LAN - Connected
Full power (S0)
Intel(R) Matrix Storage Manager option ROM v7.5.0.1017 ICH9R wRAID5
Copyright(C) 2003-07 Intel Corporation. All Rights Reserved.
RAID Volumes:
None defined.
Physical Disks:
Port Drive Model Serial # Size Type/Status(Vol ID)
0 Hitachi HDS72168 PVE201ZERHXLMM 74.5GB Non-RAID Disk
4 Hitachi HDS72168 PVE101ZDS2YR0M 74.5GB Non-RAID Disk
Press <CTRL-I> to enter Configuration Utility..
TCP Redirect
No Mapping
IDE Redirect
Floppy
<unspecified>
Intel® AMT Commander - Console Tool
start
Intel® AMT Com...
Intel® AMT Termi...
C:\WINDOWS\sys...
Intel® Active Man...
EN
11:37

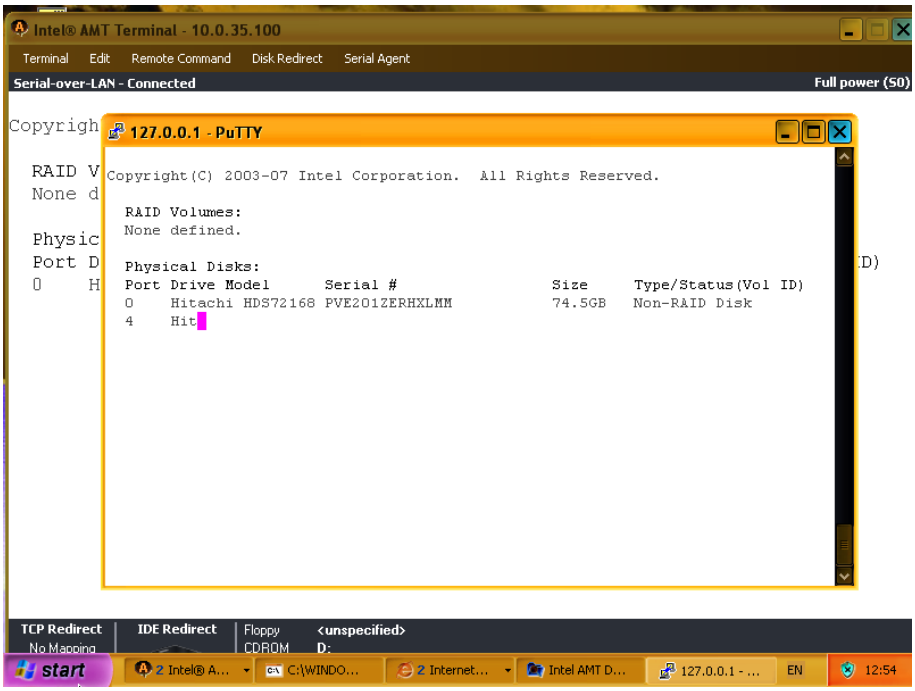

Intel® AMT Terminal - 10.0.35.100
Terminal Edit Remote Command Disk Redirect Serial Agent
Serial-over-LAN - Connected
Full power (S0)
GNU GRUB version 0.95 (608K lower / 1001151K upper memory)
GNU/Linux
Xen+GNU/Linux
Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the
commands before booting, or 'c' for a command-line.
TCP Redirect
No Mapping
IDE Redirect
Floppy
CDROM
<unspecified>
D:
start
Intel® AMT Com...
Intel® AMT Termi...
C:\WINDOWS\sys...
Intel® Active Man...
EN
11:39



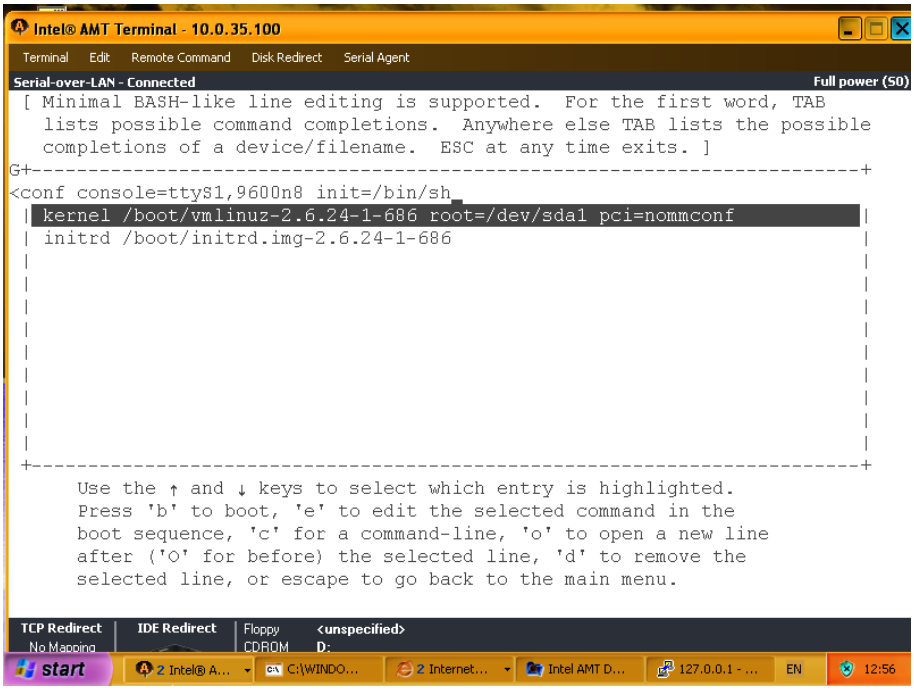


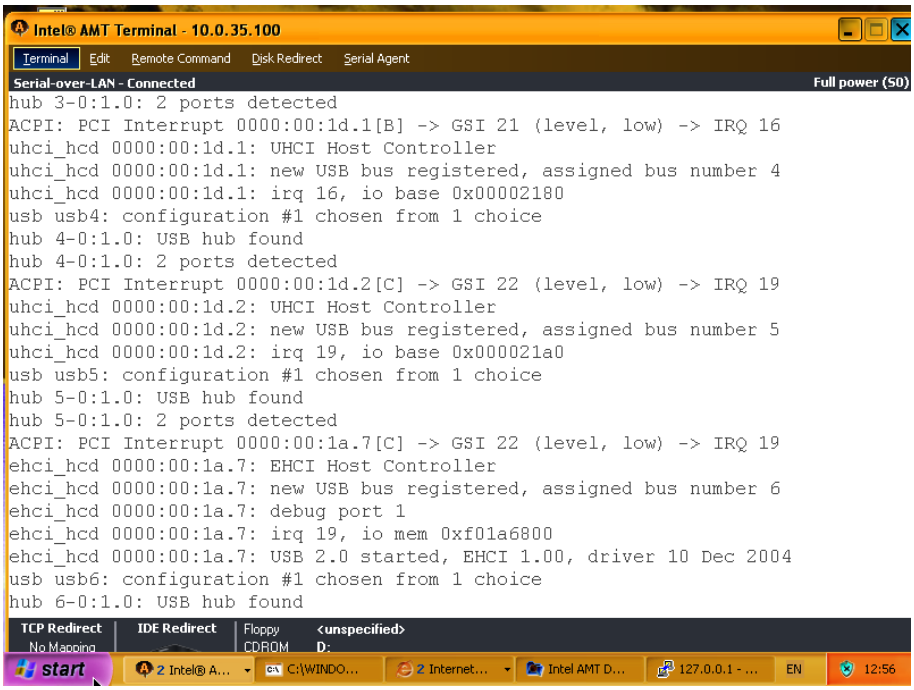
Использование PuTTY для подключения

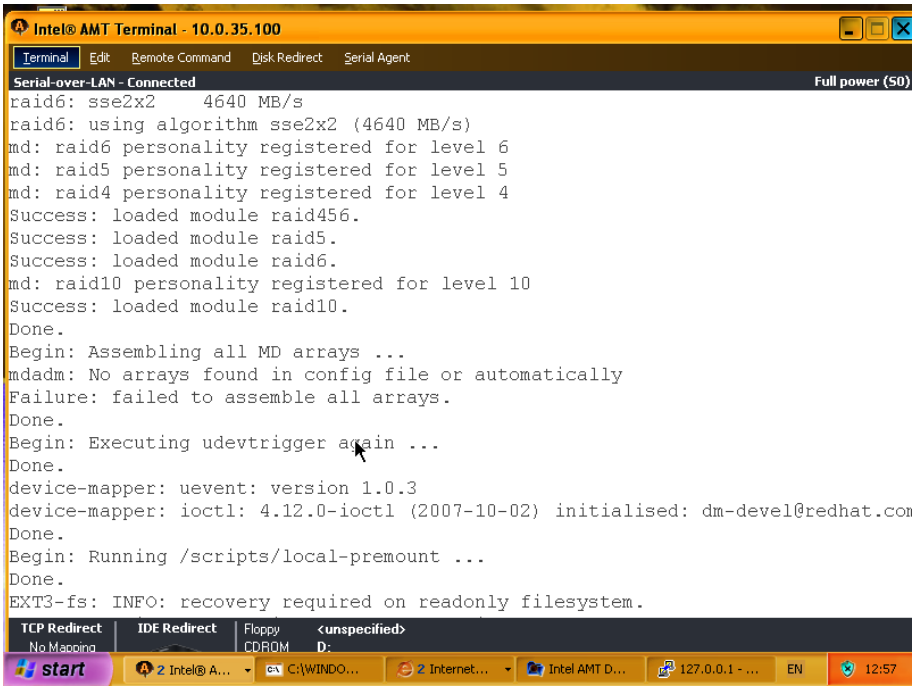


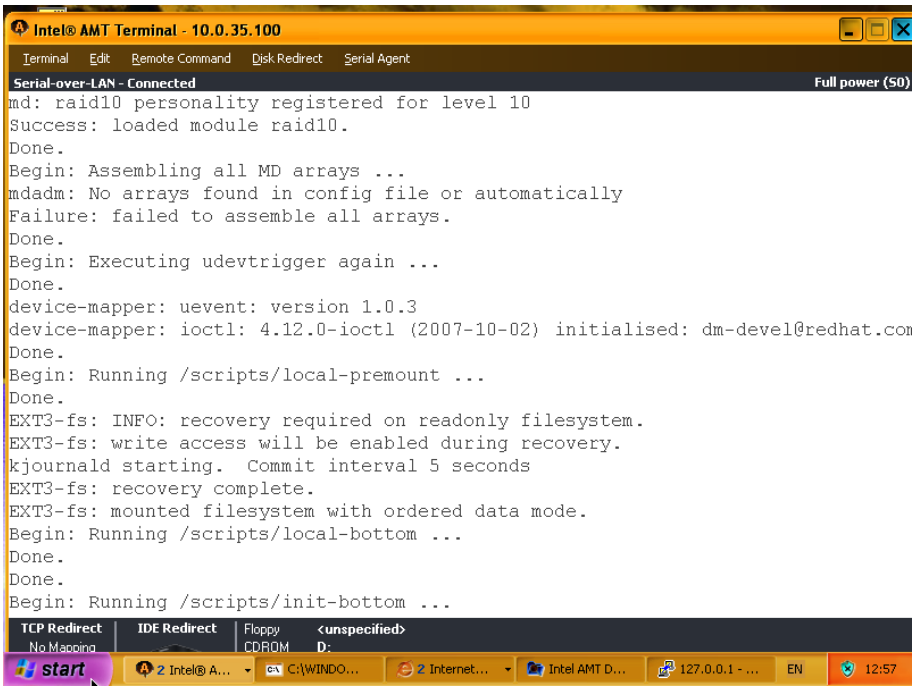


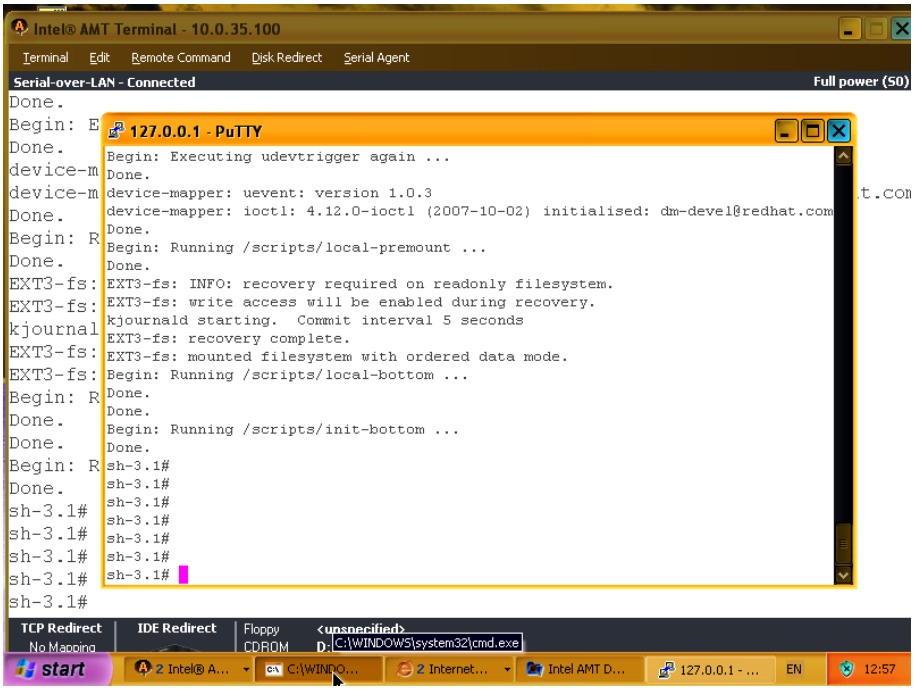
Загрузка операционной системы с перенаправленым консоли на последовательный порт

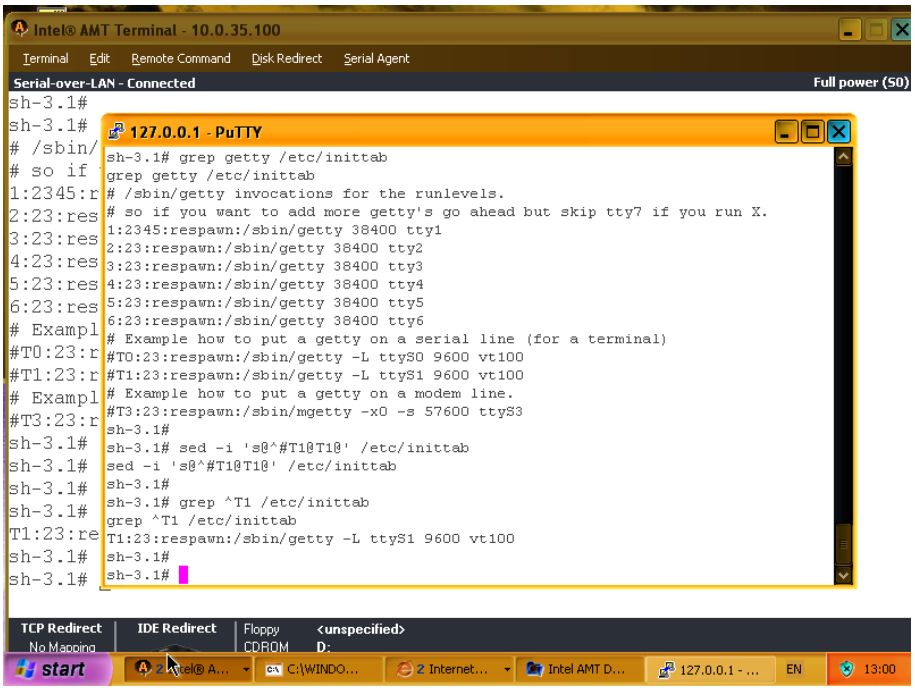

Intel® AMT Terminal - 10.0.35.100
Terminal Edit Remote Command Disk Redirect Serial Agent
Serial-over-LAN - Connected
Full power (S0)
[Minimal BASH-like line editing is supported. For the first word, TAB
lists possible command completions. Anywhere else TAB lists the possible
completions of a device/filename. ESC at any time exits.]
G+
<conf console=ttyS1,9600n8 init=/bin/sh
kernel /boot/vmlinuz-2.6.24-1-686 root=/dev/sda1 pci=nommconf
initrd /boot/initrd.img-2.6.24-1-686
Use the ↑ and ↓ keys to select which entry is highlighted.
Press 'b' to boot, 'e' to edit the selected command in the
boot sequence, 'c' for a command-line, 'o' to open a new line
after ('O' for before) the selected line, 'd' to remove the
selected line, or escape to go back to the main menu.
TCP Redirect
No Mapping
IDE Redirect
Floppy
CDROM
<unspecified>
D:
start
2 Intel® A...
C:\WINDO...
2 Internet...
Intel AMT D...
127.0.0.1 - ...
EN
12:56


Intel® AMT Terminal - 10.0.35.100
Terminal Edit Remote Command Disk Redirect Serial Agent
Serial-over-LAN - Connected
Full power (S0)
hub 3-0:1.0: 2 ports detected
ACPI: PCI Interrupt 0000:00:1d.1[B] -> GSI 21 (level, low) -> IRQ 16
uhci_hcd 0000:00:1d.1: UHCI Host Controller
uhci_hcd 0000:00:1d.1: new USB bus registered, assigned bus number 4
uhci_hcd 0000:00:1d.1: irq 16, io base 0x00002180
usb usb4: configuration #1 chosen from 1 choice
hub 4-0:1.0: USB hub found
hub 4-0:1.0: 2 ports detected
ACPI: PCI Interrupt 0000:00:1d.2[C] -> GSI 22 (level, low) -> IRQ 19
uhci_hcd 0000:00:1d.2: UHCI Host Controller
uhci_hcd 0000:00:1d.2: new USB bus registered, assigned bus number 5
uhci_hcd 0000:00:1d.2: irq 19, io base 0x000021a0
usb usb5: configuration #1 chosen from 1 choice
hub 5-0:1.0: USB hub found
hub 5-0:1.0: 2 ports detected
ACPI: PCI Interrupt 0000:00:1a.7[C] -> GSI 22 (level, low) -> IRQ 19
ehci_hcd 0000:00:1a.7: EHCI Host Controller
ehci_hcd 0000:00:1a.7: new USB bus registered, assigned bus number 6
ehci_hcd 0000:00:1a.7: debug port 1
ehci_hcd 0000:00:1a.7: irq 19, io mem 0xf01a6800
ehci_hcd 0000:00:1a.7: USB 2.0 started, EHCI 1.00, driver 10 Dec 2004
usb usb6: configuration #1 chosen from 1 choice
hub 6-0:1.0: USB hub found
TCP Redirect
No Mapping
IDE Redirect
Floppy
CDROM
<unspecified>
D:
start
2 Intel® A...
C:\WINDO...
2 Internet...
Intel AMT D...
127.0.0.1 - ...
EN
12:56


Intel® AMT Terminal - 10.0.35.100
Terminal
Edit
Remote Command
Disk Redirect
Serial Agent
Serial-over-LAN - Connected
Full power (S0)
raid6: sse2x2 4640 MB/s
raid6: using algorithm sse2x2 (4640 MB/s)
md: raid6 personality registered for level 6
md: raid5 personality registered for level 5
md: raid4 personality registered for level 4
Success: loaded module raid456.
Success: loaded module raid5.
Success: loaded module raid6.
md: raid10 personality registered for level 10
Success: loaded module raid10.
Done.
Begin: Assembling all MD arrays ...
mdadm: No arrays found in config file or automatically
Failure: failed to assemble all arrays.
Done.
Begin: Executing udevtrigger again ...
Done.
device-mapper: uevent: version 1.0.3
device-mapper: ioctl: 4.12.0-ioctl (2007-10-02) initialised: dm-devel@redhat.com
Done.
Begin: Running /scripts/local-premount ...
Done.
EXT3-fs: INFO: recovery required on readonly filesystem.
TCP Redirect
No Mapping
IDE Redirect
Floppy
CDROM
<unspecified>
D:
start
2 Intel® A...
C:\WINDO...
2 Internet...
Intel AMT D...
127.0.0.1 - ...
EN
12:57


Intel® AMT Terminal - 10.0.35.100
Terminal
Edit
Remote Command
Disk Redirect
Serial Agent
Serial-over-LAN - Connected
Full power (S0)
md: raid10 personality registered for level 10
Success: loaded module raid10.
Done.
Begin: Assembling all MD arrays ...
mdadm: No arrays found in config file or automatically
Failure: failed to assemble all arrays.
Done.
Begin: Executing udevtrigger again ...
Done.
device-mapper: uevent: version 1.0.3
device-mapper: ioctl: 4.12.0-ioctl (2007-10-02) initialised: dm-devel@redhat.com
Done.
Begin: Running /scripts/local-premount ...
Done.
EXT3-fs: INFO: recovery required on readonly filesystem.
EXT3-fs: write access will be enabled during recovery.
kjournald starting. Commit interval 5 seconds
EXT3-fs: recovery complete.
EXT3-fs: mounted filesystem with ordered data mode.
Begin: Running /scripts/local-bottom ...
Done.
Done.
Begin: Running /scripts/init-bottom ...
TCP Redirect
No Mapping
IDE Redirect
Floppy
CDROM
<unspecified>
D:
start
2 Intel® A...
C:\WINDO...
2 Internet...
Intel AMT D...
127.0.0.1 - ...
EN
12:57


Intel® AMT Terminal - 10.0.35.100
Terminal Edit Remote Command Disk Redirect Serial Agent
Serial-over-LAN - Connected
Full power (50)
127.0.0.1 - PuTTY
Begin: Executing udevtrigger again ...
Done.
device-mapper: uevent: version 1.0.3
device-mapper: ioctl: 4.12.0-ioctl (2007-10-02) initialised: dm-devel@redhat.com
Done.
Begin: Running /scripts/local-premount ...
Done.
EXT3-fs: INFO: recovery required on readonly filesystem.
EXT3-fs: write access will be enabled during recovery.
kjournald starting. Commit interval 5 seconds
EXT3-fs: recovery complete.
EXT3-fs: mounted filesystem with ordered data mode.
Begin: Running /scripts/local-bottom ...
Done.
Done.
Begin: Running /scripts/init-bottom ...
Done.
sh-3.1#
TCP Redirect
IDE Redirect
Floppy
CDROM
<unspecified>
C:\WINDOWS\system32\cmd.exe
start
12:57


Intel® AMT Terminal - 10.0.35.100
Terminal Edit Remote Command Disk Redirect Serial Agent
Serial-over-LAN - Connected
Full power (50)
127.0.0.1 - PuTTY
sh-3.1# grep getty /etc/inittab
grep getty /etc/inittab
/sbin/getty invocations for the runlevels.
so if you want to add more getty's go ahead but skip tty7 if you run X.
1:2345:respawn:/sbin/getty 38400 tty1
2:23:respawn:/sbin/getty 38400 tty2
3:23:respawn:/sbin/getty 38400 tty3
4:23:respawn:/sbin/getty 38400 tty4
5:23:respawn:/sbin/getty 38400 tty5
6:23:respawn:/sbin/getty 38400 tty6
Example how to put a getty on a serial line (for a terminal)
#T0:23:respawn:/sbin/getty -L ttyS0 9600 vt100
#T1:23:respawn:/sbin/getty -L ttyS1 9600 vt100
Example how to put a getty on a modem line.
#T3:23:respawn:/sbin/mgetty -x0 -s 57600 ttyS3
sh-3.1#
sh-3.1# sed -i 's@^#T1@T1@' /etc/inittab
sed -i 's@^#T1@T1@' /etc/inittab
sh-3.1#
sh-3.1# grep ^T1 /etc/inittab
grep ^T1 /etc/inittab
T1:23:respawn:/sbin/getty -L ttyS1 9600 vt100
sh-3.1#
TCP Redirect
IDE Redirect
Floppy
CDROM
<unspecified>
start
13:00

4 Intel VT-x: Windows XP в Xen

Здесь рассматривается процедура подготовки и запуска домена с Windows в системе виртуализации Xen на платформе с аппаратной поддержкой виртуализации (HVM).

4.1 Предварительные требования

В первую очередь, для установки Windows XP, как и любой другой системы с закрытым кодом, необходима поддержка центральным процессором технологии виртуализации Intel®Virtualization Technology (VT) или Pacifica (AMD). Поддержка аппаратной виртуализации должна быть и у Xen. При сборке из исходных текстов понадобится установить в систему:

- **dev86** — Ассемблер и компоновщик для реального режима 80x86. Этот пакет необходим для сборки кода BIOS, запускаемого в (виртуальном) реальном режиме. Если пакет dev86 недоступен для x86_64, то можно использовать i386 версию.
- **LibVNCServer** — Немодифицируемый VGA дисплей, клавиатуру и мышь можно виртуализировать с помощью библиотеки vncserver.
- **SDL-devel**, **SDL** — Если пакеты SDL и SDL-devel не были установлены по умолчанию, то взять их можно из системы портов или скомпилировав из исходных текстов.

При выполнении вышеуказанной процедуры на Debian GNU/Linux необходимо учесть, что пакет **dev86** в Debian разбит на два пакета – **bin86** и **bcc** – и перед компиляцией Xen из архива исходных текстов должны быть установлены оба эти пакета.

4.2 Конфигурационный файл домена

В терминологии Xen гостевые домены, исполняющиеся в режиме аппаратной виртуализации называются HVM-доменами. Для облегчения процесса конфигурирования существует пример конфигурационного файла такого домена (при установке из исходников он называется `/etc/xen/xmexample.hvm`; при установке из пакетов путь может быть другим). В нём помимо опций использующихся в паравиртуальных доменах есть и сугубо специфические:

- **kernel** – VMX firmware loader, /usr/lib/xen/boot/vmxloader
- **builder** – Функции сборки домена. VMX-домены используют vmx builder
- **acpi** – Задействует ACPI VMX-домена, по умолчанию равно "0" (отключено)
- **apic** – Задействует APIC VMX-домена, по умолчанию равно "0" (отключено)
- **pae** – Задействует PAE VMX-домена, по умолчанию равно "0" (отключено)

- **vif** – Опционально определяет MAC адрес и/или режим моста для сетевого интерфейса. Если значение MAC не указано, то назначается случайный адрес. Есть возможность задать параметр type=ioemu для использования ioemu в VMX NIC. Если это значение не определено, то vbd используется как в паравиртуальных("нормальных", с модифицированным ядром) доменах.

- **disk** – Определяет дисковые устройства, к которым гостевой домен должен иметь доступ. Если для домена используется физический носитель в качестве диска, то он должен быть описан строкой типа:

```
phy:UNAME,ioemu:DEV,MODE,
```

где `UNAME` – имя устройства, `DEV` – имя диска, как его видит домен и `MODE` принимает значения `r` для read-only и `w` для read-write. Если это значение не определено, то ioemu используется как паравиртуальных доменах.

Если используется образ диска, то строка принимает вид:

```
file:FILEPATH,ioemu:DEV,MODE
```

Если используется больше одного диска, то они разделяются запятой. Например:

```
disk = ['file:/var/images/image1.img,ioemu:hda,w', \
        'file:/var/images/image2.img,ioemu:hdb,w']
```

- **cdrom** – Образ CD-ROM. По умолчанию, для Domain0 это значение равно /dev/cdrom. Внутри VMX-домена CD-ROM будет виден как /dev/hdc.

- **boot** – Загрузка с floppy (a), hard disk (c) или CD-ROM (d).

- **device_model** – Инструмент эмуляции устройств для VMX-домена. Могут быть изменены параметры, приведенные ниже.

- **sdl** – Задействует библиотеку SDL для отображения графики, по умолчанию равно "0" (отключено)

- **vnc** – Задействует библиотеку VNC для отображения графики, по умолчанию равно "0" (отключено)

- **vncviewer** – Если vnc=1 и vncviewer=0, пользователь может использовать vncviewer для подключения к VMX-домену. Например:

```
$ vncviewer domain0_IP_address:VMX_domain_id
```

- **ne2000** – Задействует режим совместимости ne2000, по умолчанию равно "0" (отключено, используется pcnet)

- **serial** – Перенаправление последовательных портов гостевого домена на реальное устройство.

- **usb** – Включение поддержки USB без указания специфического устройства. По умолчанию эта функция отключена, в случае же определения параметра usbdevice, ее необходимо задействовать.

- **usbdevice** – Включение поддержки конкретных устройств. Например, поддержка мыши PS/2 через USB:

```
usbdevice='mouse'
```

- **localtime** – Установка локального времени. По умолчанию равно "0", т.е UTC

- **enable-audio** – Поддержка звука. Находится в разработке.

- **full-screen** – Поддержка полноэкранного режима. Находится в разработке.

- **nographic** – Другой способ перенаправить вывод на последовательный порт. В этом случае опции 'sdl' или 'vnc' не работают. Использование данного режима не рекомендуется.

4.3 Проверка на поддержку VMX

После загрузки самого Dom0 убедимся в наличии поддержки VMX (процессоры Intel):

```
# xm dmesg | grep VMX
(XEN) VMXON is done
(XEN) VMXON is done
...
(XEN) VMXON is done
(XEN) VMXON is done
(XEN) VMXON is done
#
```

Если используется процессор AMD:

```
# xm dmesg | grep -i svm
(XEN) AMD SVM Extension is enabled for cpu 0.
(XEN) AMD SVM Extension is enabled for cpu 1.
```

В общем случае:

```
# xm info | grep caps
hw_caps                : 178bfbff:ebd3fbff:00000000:00000010:00.....
xen_caps               : xen-3.0-x86_32p hvm-3.0-x86_32 hvm-3.0-x86_32p
```

hvm-3.0-x86_32 говорит о том, что XEN успешно обнаружил процессор, который поддерживает технологии Intel VT или AMD-V.

Если у вас другое сообщение, то проверьте настройки BIOS и задействуйте поддержку аппаратной виртуализации, если она выключена.

4.4 Создание дискового раздела для гостевой системы

Создаем образ диска Xen:

```
# mkdir -p /root/xenimages
    # cd /root/xenimages
    # dd if=/dev/zero of=WS128.img bs=1M count=4096
```

Также необходимо создать iso-образ системы WinXP – ServicePack2. В данном случае, разместим его в каталоге `/root/xenimages`.

На основе эталонного файла конфигурации создадим свой собственный:

```
# cat /etc/xen/winXP128
kernel = "/usr/lib/xen/boot/hvmloader"
builder='hvm'
memory = 512
name = "WinXP128"
vcpus=1
pae=0
acpi=0
apic=0
cpus = ""
vif = [ 'type=ioemu, bridge=xenbr0' ]
disk = [
'file:/root/xenimages/winXP128.img,ioemu:hda,w',
'file:/root/xenimages/en_winxp_pro_with_sp2.iso,ioemu:hdc:cdrom,r'
]
on_poweroff = 'destroy'
on_reboot   = 'destroy'
on_crash    = 'destroy'
device_model = '/usr/lib/xen/bin/qemu-dm'
boot='d'
sdl=0
vnc=1
vncviewer=0
stdvga=0
serial='pty'
ne2000=0
```

Обратите внимание на то, что указан параметр `boot=d`, что необходимо для установки. Впоследствии его необходимо заменить на `boot='c'`. Доступ к гостевому домену будет осуществляться через VNC, использование SDL не предполагается.

4.5 Запуск домена и инсталляция гостевой системы

Начинаем установку и подсоединяемся к домену с помощью VNC – сразу после создания домена подключаемся к нему с помощью vncviewer.

```
# xm create -c /etc/xen/winXP128
Using config file "/etc/xen/winXP128".
Started domain WinXP128
```

Подключение к VNC:

```
%$ vncviewer localhost:0
```

С установкой могут быть проблемы. Можно попробовать решить проблему так: на экране установки, предлагающем нажать F6 для установки SCSI или RAID контроллера, надо нажать F5 и выбрать пункт `Standard PC` из предложенного меню.

```
ACPI Multiprocessor PC
ACPI Uniprocessor PC
Advanced Configuration and Power Interface (ACPI) PC
Compaq SystemPro Multiprocessor or 100% Compatible PC
MPS Uniprocessor PC
MPS Multiprocessor PC
Standard PC
Standard PC with C-Step i486
Other
```

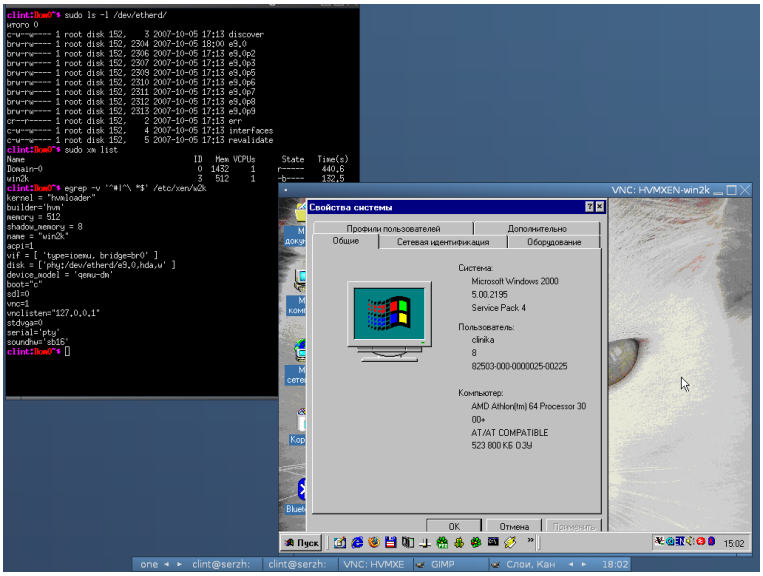
После того, как программа установки Windows отформатирует диск и скопирует на него необходимые файлы, выполняется перезагрузка. Согласно нашему файлу конфигурации, виртуальная машина будет закрыта и нам предоставится удачная возможность отредактировать параметр `boot='c'`, после чего запускаем виртуальную машину и соединяемся с консолью:

```
%# xm create /etc/xen/winXP128
Using config file "/etc/xen/winXP128".
Started domain WinXP128
```

VNC:

```
%$ vncviewer localhost:0
```

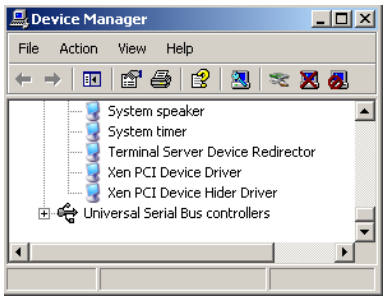
4.6 Запуск уже установленной Windows в домене Xen



Операционная система Windows одного хоста, запущенная в домене Xen на другом хосте

Если на компьютере установлено две операционные системы, и одна из них это Xenolinux (Xen + Linux), то вторую можно запустить как пользовательский домен Xen. Если операционная система установлена не локально, а на другом компьютере, её тоже можно запустить в домене Xen, только для этого необходимо как-то дать возможность доступа системе виртуализации к образу установленной системы, так чтобы, грубо говоря, виртуальный домен увидел диск. Это можно сделать, например, с помощью AoE или iSCSI.

4.7 Паравиртуальные драйверы



Окно Device Manager в Windows с установленными свободными паравиртуальными драйверами

Аппаратная виртуализация берёт на себя основные трудности по переключению контекстов гостевых операционных систем и хост-системы, но она ничего (пока что) не делает для ускорения ввода/вывода. Как только задача требует ввода/вывода любая система виртуализации (но не паравиртуализации!) существенно замедляет свою работу.

Одна из главных причин разработки и использования паравиртуальных драйверов — возможность существенного повышения производительности работы гостевых систем, работающих в режиме полной виртуализации.

Во второй половине 2007 года появились первая реализация свободных паравиртуальных драйверов под Windows, сделанная Джеймсом Харпером (James Harper).

В конце 2007 года вышла версия 0.5.0 драйверов, которые можно рассматривать как экспериментальные. Их можно ставить в виртуальную машину и играться с ними, но их пока что ни в коем случае не стоит использовать на производственных системах.

В настоящий момент свободные паравиртуальные драйверы Xen для Windows находятся в крайне сыром состоянии и могут использоваться исключительно в экспериментальных целях.

4.8 Проброс PCI-устройств внутрь домена Windows

Начиная с Xen 3.2.0 при наличии в системе аппаратной поддержки виртуализации ввода/вывода Intel VT-d (не путать с виртуализацией процессора VT-x!) существует возможность выполнять монопольное выделение PCI-устройства домену Xen. Раньше это было возможно для паравиртуальных

доменов, но было невозможно для HVM-доменов, а именно в таком исполняется Windows.

При выполнении проброса PCI-устройства Windows работает с ним напрямую, на полной скорости, и используя собственные драйвера. Это позволяет обойти проблемы с производительностью, которые есть при эмуляции устройств, а также задействовать все возможности устройства, о которых знает драйвер.

При выделении устройства гостевому оно становится недоступным для домена 0 и используется гостевым доменом монопольно.

Графический адаптер является очень специфическим устройством, монопольное выделение которого пока не поддерживается. Это означает, что запускать Counter Strike внутри гостевого домена Xen и при этом напрямую использовать графическую карту пока не получится.

4.9 Дополнительная информация

- Windows XP в Xen[7]

[7] http://xgu.ru/wiki/xen/winxp

5 Intel VT-x: Windows Vista в Xen

Здесь рассматривается процесс инсталляции и запуска виртуальной машины под управлением в MS Windows Vista внутри полностью виртуализированного домена Xen на машине с поддержкой процессором архитектурных расширений виртуализации (HVM). Отдельное внимание уделяется решению проблем с сетью внутри виртуальной машины.

5.1 Подготовка хост-системы

Выполните подготовку хост-системы (домена 0 Xen) как описано на странице Инсталляция Xen или другим способом.

В ходе инсталляции Windows доступ к виртуальной машине будет осуществляться через VNC-сервер, встроенный в Xen. По умолчанию сервер привязан к интерфейсу loopback и доступен только по адресу 127.0.0.1.

Если необходимо работать с VNC-консолью с другой машины, можно пойти двумя путями:

1. (более безопасный) Перенести порт VNC на неё с помощью SSH (см. подробнее на странице SSH);
2. (более простой) Разрешить доступ к VNC-консоли с других машин.

Для этого нужно отредактировать файл /etc/xen/xend-config.sxp, в котором найти и изменить параметры:

```
(vnc-listen '0.0.0.0')
```

и

```
(vnc-password 'PASSWORD')
```

Если последний параметр не установить, доступ по VNC будет разрешён без пароля.

5.1.1 Проверка на поддержку VMX-расширений

Хост-система должна поддерживать VMX-расширения процессора (см. Аппаратные требования Xen).

Убедиться в наличии поддержки VMX можно так.

Для процессоров Intel:

```
# xm dmesg | grep VMX
(XEN) VMXON is done
(XEN) VMXON is done
...
(XEN) VMXON is done
(XEN) VMXON is done
(XEN) VMXON is done
#
```

Если используется процессор AMD:

```
# xm dmesg | grep -i svm
(XEN) AMD SVM Extension is enabled for cpu 0.
(XEN) AMD SVM Extension is enabled for cpu 1.
```

В общем случае:

```
# xm info | grep caps
hw_caps                : 178bfbff:ebd3fbff:00000000:00000010:00002.....
xen_caps               : xen-3.0-x86_32p hvm-3.0-x86_32 hvm-3.0-x86_32p
```

hvm-3.0-x86_32 говорит о том, что XEN успешно обнаружил процессор, который поддерживает технологии Intel VT или AMD-V.

Если у вас другое сообщение, но вы уверены, что у процессора есть архитектурные расширения виртуализации, то проверьте настройки BIOS и, если вы этого еще не сделали, задействуйте поддержку VT.

Возможно, BIOS вашей материнской платы искуственно отключает виртуализацию. В этом случае нужно обновить или исправить BIOS (см. например GA-M59SLI-S4)

5.2 Подготовка образа инсталляционного диска

Можно использовать непосредственно диск с инсталлятором Windows, а можно предварительно создать с него образ.

Образ создаётся традиционным путём:

```
%# cd /Volumes/ISO
%# cat /dev/hdd > windows-vista.iso
%# ls -l windows-vista.iso
-rw-r--r-- 1 igor igor 4681433088 2007-09-23 12:07 windows-vista.iso
```

5.3 Подготовка конфигурационного файла домена Xen

Необходимо создать конфигурационный файл виртуальной машины, в которой будет работать Vista.

Можно использовать распространяемый с дистрибутивом Xen пример и доработать его, а можно воспользоваться этим примером:

```
$ grep -v ^# /etc/xen/windows-vista-hvm | grep -vx ''
kernel = "hvmloader"
builder='hvm'
memory = 1024
shadow_memory = 8
name = "windows-vista-hvm"
vif = [ 'type=ioemu, bridge=service0, mac=00:16:3e:03:00:c3' ]
disk = [ 'file:/xen/images/windows-vista-hvm.img,hda,w', \
         'file:/Volumes/ISO/windows-vista.iso,hdc:cdrom,r' ]
device_model = 'qemu-dm'
boot="d"
sdl=0
vnc=1
vncpasswd=''
stdvga=0
```

```
serial='pty'
usb=1
```

Параметры, использованные в этом конфигурационном файле (с полным списком можно ознакомиться в «Руководстве пользователя Xen»):

- **kernel** – VMX firmware loader, /usr/lib/xen/boot/vmxloader
- **builder** – Функции сборки домена. VMX-домены используют vmx builder
- **vif** – Опционально определяет MAC адрес и/или режим моста для сетевого интерфейса. Если значение MAC не указано, то назначается случайный адрес. Есть возможность задать параметр type=ioemu для использования ioemu в VMX NIC. Если это значение не определено, то vbd используется как в паравиртуальных("нормальных", с модифицированным ядром) доменах.
- **disk** – Определяет дисковые устройства, к которым гостевой домен должен иметь доступ. Если для домена используется физический носитель в качестве диска, то он должен быть описан строкой типа:

```
phy:UNAME,ioemu:DEV,MODE,
```

где **UNAME** – имя устройства, **DEV** – имя диска, как его видит домен и **MODE** принимает значения **r** для read-only и **w** для read-write. Если это значение не определено, то ioemu используется как паравиртуальных доменах.

Если используется образ диска, то строка принимает вид:

```
file:FILEPATH,ioemu:DEV,MODE
```

Если используется больше одного диска, то они разделяются запятой. Например:

```
disk = ['file:/var/images/image1.img,ioemu:hda,w', \
        'file:/var/images/image2.img,ioemu:hdb,w']
```

- **boot** – Загрузка с floppy (a), hard disk (c) или CD-ROM (d).
- **device_model** – Инструмент эмуляции устройств для VMX-домена. Могут быть изменены параметры, приведенные ниже.
- **sdl** – Задействует библиотеку SDL для отображения графики, по умолчанию равно "0" (отключено)
- **vnc** – Задействует библиотеку VNC для отображения графики, по умолчанию равно "0" (отключено)
- **serial** – Перенаправление последовательных портов гостевого домена на реальное устройство.
- **usb** – Включение поддержки USB без указания специфического устройства. По умолчанию эта функция отключена, в случае же определения параметра usbdevice, ее необходимо задействовать.

- **usbdevice** – Включение поддержки конкретных устройств. Например, поддержка мыши PS/2 через USB:

```
usbdevice='mouse'
```

- **localtime** – Установка локального времени. По умолчанию равно "0", т.е UTC
- **enable-audio** – Поддержка звука. Находится в разработке.
- **full-screen** – Поддержка полноэкранного режима. Находится в разработке.
- **nographic** – Другой способ перенаправить вывод на последовательный порт. В этом случае опции 'sdl' или 'vnc' не работают. Использование данного режима не рекомендуется.

5.4 Подготовка диска для виртуальной машины

Виртуальная машина под управлением Windows Vista требует обязательного использования жёсткого диска.

В качестве виртуального жёсткого диска можно использовать:

- файл в хост-системе;
- блочное устройство в хост-системе, которым может быть:
  - физический жёсткий диск или его раздел;
  - том LVM;
  - сетевое или другое хранилище, доступное в виде блочного устройства.

В случае если будет использоваться файл, его нужно создать и указать в конфигурационном файле виртуальной машины в качестве диска.

```
%$ grep disk /etc/xen/windows-vista-hvm | grep -v ^#
disk = [ 'file:/xen/images/windows-vista-hvm.img,hda,w', \
         'file:/Volumes/ISO/windows-vista.iso,hdc:cdrom,r' ]
```

Создание файла проще всего выполнить с помощью команды **dd**. Здесь создаётся разреженный файл размером 10G (минимальный размер диска при инсталляции Vista в конфигурации по умолчанию):

```
%$ sudo dd if=/dev/zero \
           of=/xen/images/windows-vista-hvm.img \
           bs=1k seek=10240k count=1
1+0 записей считано
1+0 записей написано
 скопировано 1024 байта (1,0 kB), 4,6e-05 секунд, 22,3 MB/s

%$ ls -l /xen/images/windows-vista-hvm.img
-rw-r--r-- 1 root root 10737419264
        2007-09-23 12:17 /xen/images/windows-vista-hvm.img
```

5.5 Первый запуск

После того как

1. Xen в домене 0 установлен и настроен;
2. Создан образ инсталляционного диска Windows Vista (или доступен сам диск);
3. Создан файл для диска виртуальной машины (или доступно нечто вместо него);
4. Создан конфигурационный файл новой виртуальной машины

виртуальную машину можно запускать.

Запуск выполняется с помощью команды:

```
%$ sudo xm create windows-vista-hvm
Using config file "./windows-vista-hvm".
Started domain windows-vista-hvm
```

Если старт прошёл успешно, новый домен появится в списке доменов, работающих в хост-системе:

```
%$ sudo xm list
Name                                        ID   Mem VCPUs      State   Time(s)
Domain-0                                     0  1000     1     r-----    706.4
windows-vista-hvm                            7  1032     1     ------      0.5
```

После того как виртуальная машина запущена, можно подключиться к её экрану с помощью VNC.

Используем vncviewer (в Debian GNU/Linux он находится в пакете xvncviewer):

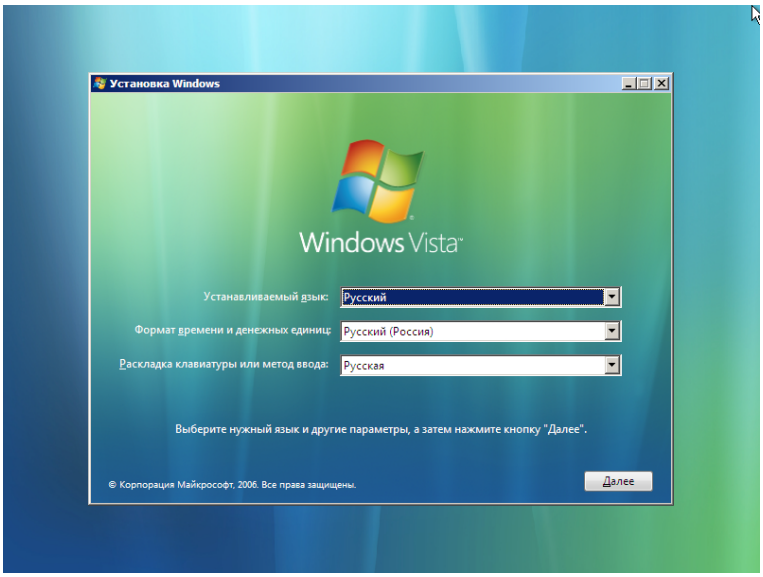
```
$ vncviewer 127.0.0.1:0
VNC viewer version 3.3.7 - built Dec 30 2006 12:48:54
Copyright (C) 2002-2003 RealVNC Ltd.
Copyright (C) 1994-2000 AT&T Laboratories Cambridge.
See http://www.realvnc.com for information on VNC.
VNC server supports protocol version 3.3 (viewer 3.3)
No authentication needed
Desktop name "HVMXEN-windows-vista-hvm"
Connected to VNC server, using protocol version 3.3
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap and visual, TrueColor, depth 24.
Got 256 exact BGR233 colours out of 256
Using BGR233 pixel format:
  8 bits per pixel.
  True colour: max red 7 green 7 blue 3, shift red 0 green 3 blue 6
Using shared memory PutImage
Throughput 20000 kbit/s - changing to Hextile
```

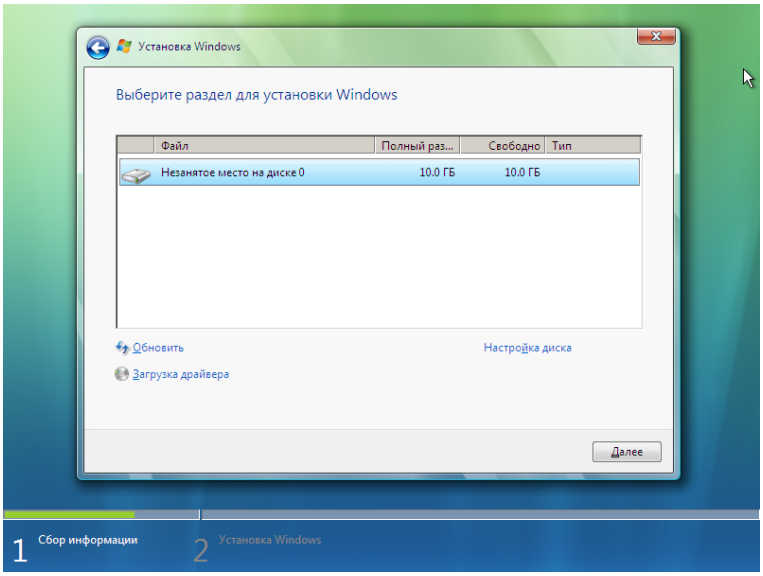
```
Throughput 20000 kbit/s - changing from 8bit
Using viewer's native pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

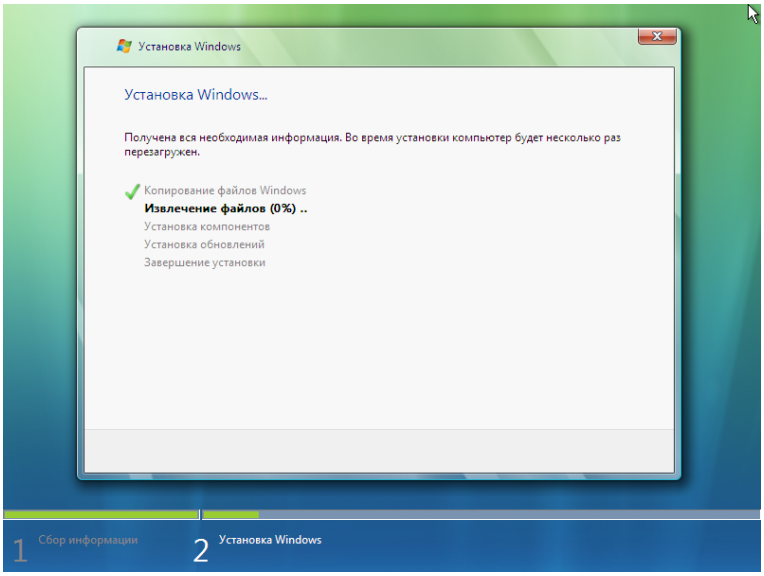
Программа покажет экран инсталлятора операционной системы.

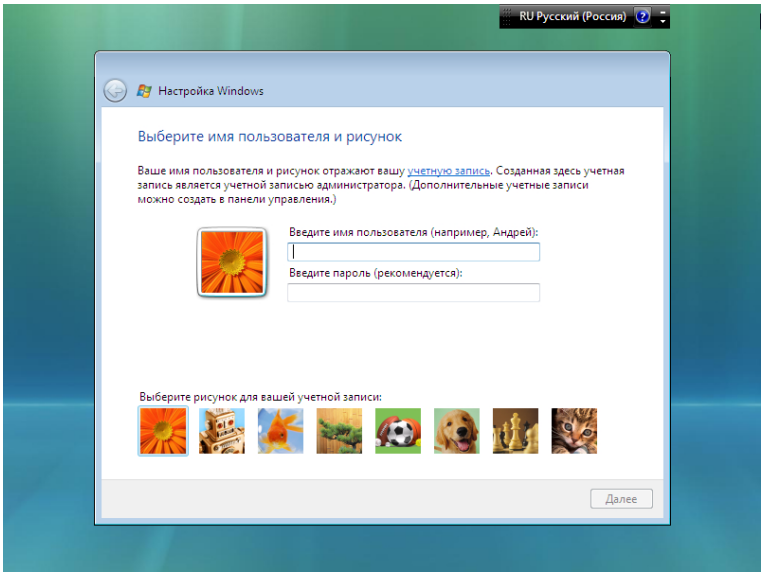
5.6 Инсталляция Vista

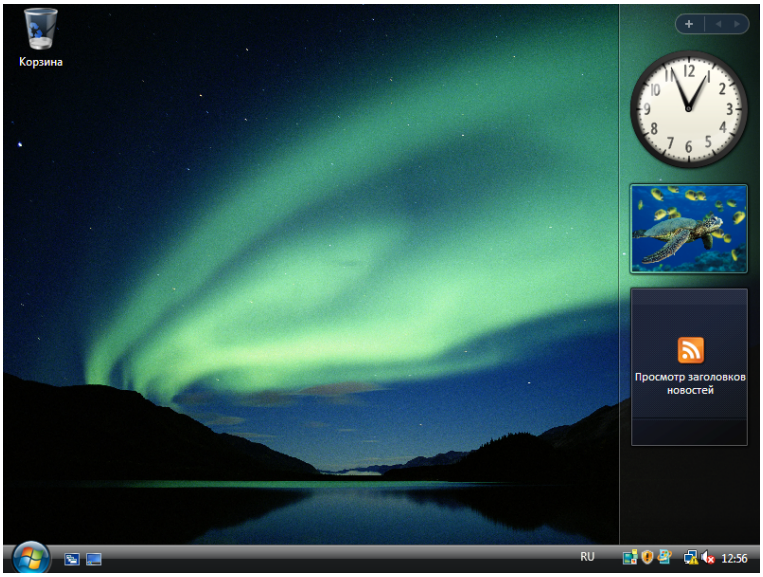
Инсталляция выполняется традиционно. В ходе инсталляции система будет несколько раз перезагружаться, при этом подключение по VNC будет теряться. Для его восстановления нужно вызывать **vncviewer** повторно.






Установка Windows
Установка Windows...
Получена вся необходимая информация. Во время установки компьютер будет несколько раз перезагружен.
Копирование файлов Windows
Извлечение файлов (0%) ..
Установка компонентов
Установка обновлений
Завершение установки
1 Сбор информации
2 Установка Windows


RU Русский (Россия)
Настройка Windows
Выберите имя пользователя и рисунок
Ваше имя пользователя и рисунок отражают вашу учетную запись. Созданная здесь учетная запись является учетной записью администратора. (Дополнительные учетные записи можно создать в панели управления.)
Введите имя пользователя (например, Андрей):
Введите пароль (рекомендуется):
Выберите рисунок для вашей учетной записи:
Далее



Система успешно установлена.

5.7 Изменение порядка загрузки

После того как система была проинсталлирована, имеет смысл перейти на загрузку виртуальной машины с диска (не с CD). Для этого нужно поменять значение параметра `boot` в конфигурационном файле домена с `d` на `c`.

```
%$ grep ^boot /etc/xen/windows-vista-hvm
boot="c"
```

5.8 Инсталляция сети

Неизвестно по какой причине, но Windows Vista не работает корректно с сетевым адаптером RTL8139, который эмулируется в HVM-доменах Xen по умолчанию: сетевое устройство обнаруживается и драйвер устанавливается, но сеть не работает.

Самое простое решение проблемы — перейти на эмуляцию сетевого устройства NE2000. С ним у Windows Vista никаких проблем не замечено.

Правда, драйвер для этой карты по умолчанию отсутствует в поставке Vista, и его необхдимо установить дополнительно.

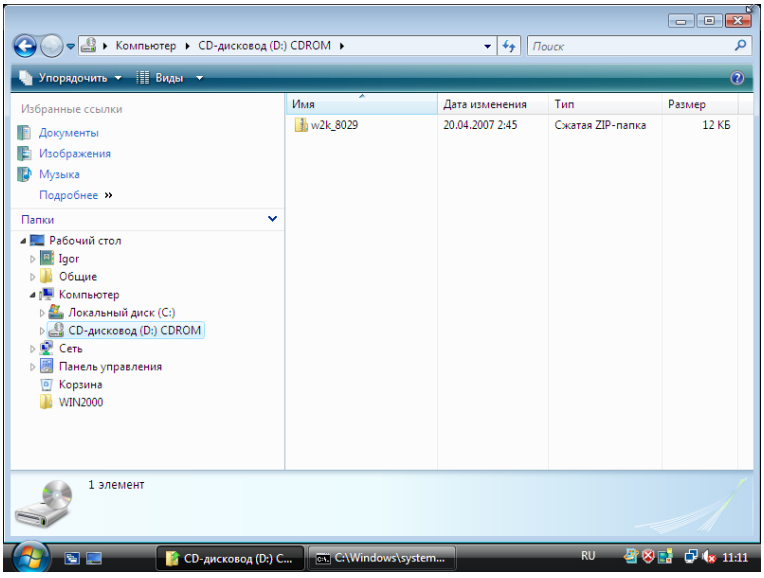
Для того чтобы передать драйвер Windows Vista, в которой пока что сеть не работает, нужно подготовить ISO-образ с драйвером и загрузить его в виртуальную машину.

- ZIP-архив с драйвером NE2000[8]
- ISO-образ с драйвером NE2000[9]

ISO-образ нужно подлючить к работающей машине (Ctrl-Alt-2) или указать в параметре **disk** машины.

```
$ grep ^disk /etc/xen/windows-vista-hvm
disk = [ 'file:/xen/images/windows-vista-hvm.img,hda,w', \
         'file:/Volumes/ISO/ne2k-drivercd.iso,hdc:cdrom,r' ]
```

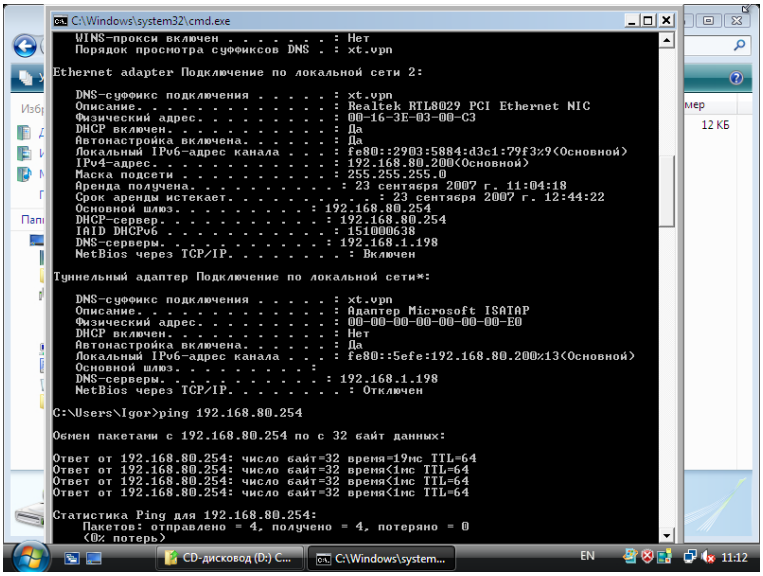
Диск содержит ZIP-архив. Его необходимо распаковать, и инициировать инсталляцию драйвера стандартным способом.



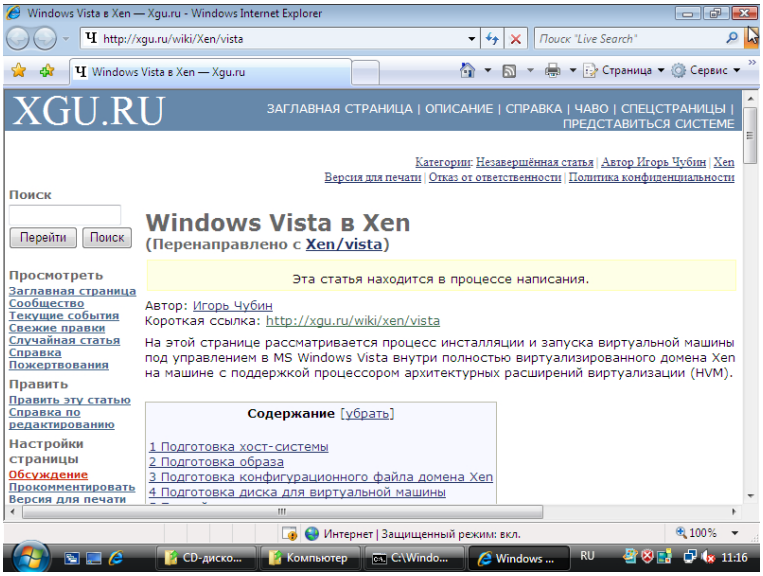
После того как драйвер установлен, сеть начинает работать.

Это можно проверить с помощью команд **ipconfig** и **ping**:

[8] http://xgu.ru/download/w2k_8029.zip
[9] http://xgu.ru/download/ne2k-drivercd.iso



Или с помощью других приложений, которые используют сеть:



5.9 Запуск и работа

Windows Vista проинсталлирована и готова к работе.

5.10 Дополнительная информация

- Windows Vista в Xen[10]

[10] http://xgu.ru/wiki/xen/vista

6 Intel VT-d: Монопольное выделение устройств в Xen

VT-d — технология виртуализации ввода/вывода, предложенная Intel. Эта технология позволяет обеспечить монопольное выделение устройства HVM-домену, в то время как без её помощи (или аналогичной технологии IOMMU от AMD) это возможно только для паравиртуальных доменов.

На этой странице подробнее рассматриваются вопросы применения технологии VT-d в Xen, какие преимущества она даёт, а также как правильно её использовать.

6.1 Организация ввода/вывода в домене Xen

Существует три основных способа обеспечения ввода/вывода (и, фактически, доступа к оборудованию) для гостевой операционной системы, работающей внутри домена Xen:

1. Эмуляция устройств со стороны домена 0 и использование традиционных драйверов в гостевой системе;
2. Монопольное выделение устройств гостевой системе;
3. Использование паравиртуальных драйверов.

В настоящий момент наиболее распространённым является первый способ, т.е. *эмуляция устройств*. Xen использует для эмуляции, так называемый QEMU Device Model (qemu-dm). Это специальный процесс, работающий в пространстве пользователя (userlevel) в домене 0 и предоставляющий виртуальные устройства гостевому домену.

Полной противоположностью этому подходу является второй подход — *монопольное выделение устройства гостевой системе*. В этом случае никаких затрат на эмуляцию не требуется. Гостевой домен работает с устройством напрямую, без всякого посредничества домена 0. Он видит устройство "*как есть*", и использует стандартные драйверы от этого устройства. Работа с устройством осуществляется на полной скорости.

Во третьем способе используются особые драйверы, которые выполняет ввод/вывод не через эмулируемые устройства, а при помощи специального *паравиртуального интерфейса*, предоставляемого системой виртуализации и хост-системой.

Далее будет подробнее рассмотрен второй способ, то есть монопольное выделение устройств гостевым доменам.

6.2 Монопольное выделение устройств гостевому домену

В настоящий момент такой способ работает с паравиртуальными доменами — им можно выделять устройства в монопольное использование без всяких проблем. Что касается HVM-доменов (доменов, использующих аппаратную виртуализацию), это:

1. Требует аппаратной поддержки;

2. Реализовано в Xen, начиная с версии 3.2.0, вышедшей в начале 2008 года.

Что касается аппаратной поддержки, она есть, но пока что достаточно редка.

Сейчас еть как минимум две платы производства Intel (*DQ35MP* и *DQ35JO*), которые подерживают собственную реализацию аппаратной виртуализации ввода/вывода известную как Intel VT-d (не путать с Intel VT!).

В AMD тоже ведётся работа над собственной реализацией аппаратной виртуализацией ввода/вывода, *IOMMU*.

6.3 Как включить поддержку VT-d в Xen

- `cd xen-unstable.hg`
- `make install`
- `make linux-2.6-xen-config CONFIGMODE=menuconfig`
- изменить `XEN->"PCI-device backend driver"` с "M" на "*".
- `make linux-2.6-xen-build`
- `make linux-2.6-xen-install`
- `depmod 2.6.18.8-xen`
- `mkinitrd -v -f -with=ahci -with=aacraid -with=sd_mod -with=scsi_mod initrd-2.6.18-xen.img 2.6.18.8-xen`
- `cp initrd-2.6.18-xen.img /boot`
- `lspci` – выбрать идентификаторы устройств, которые вы хотите назначить гостевым системам
- скрыть PCI-устройства от домена 0 (dom0) с помощью такой записи в GRUB:

```
title Xen-Fedora Core (2.6.18-xen)
        root (hd0,0)
        kernel /boot/xen.gz com1=115200,8n1 console=com1 vtd=1
        module /boot/vmlinuz-2.6.18.8-xen root=LABEL=/
                  ro console=tty0 console=ttyS0,115200,8n1
                  pciback.hide=(01:00.0)(03:00.0)
                  pciback.verbose_request=1 apic=debug
        module /boot/initrd-2.6.18-xen.img
```

- перезагрузить операционную систему
- добавить строку "pci" в файл `/etc/xen/hvm.conf`

```
pci = [ '01:00.0', '03:00.0' ]
```

* запустить гостевой HVM-домен и с помощью команды **lspci** посмотреть, пробрасывается ли устройство. Если это сетевое устройство, попробовать поработать с ним, например, с помощью **ifconfig**

6.4 Поддержка операционных систем

- Хост-система: PAE, 64-bit
- Гостевая система: 32-bit, PAE, 64-bit

Сейчас Xen не поддерживает MSI, поэтому для тех гостевых систем, которые по умолчанию используют MSI, нужно добавить опцию ядра

```
pci=nomsi
```

в загрузчик (GRUB)

6.5 Проверенные комбинации

- 64-битный хост: 32/PAE/64 Linux/XP/Win2003/Vista guests
- PAE хост: 32/PAE Linux/XP/Win2003/Vista guests

6.6 Аппаратные системы с поддержкой VT-d

Системы, в которых точно есть поддержка VT-d:

- HP Compaq: DC7800 http://h10010.www1.hp.com/wwpc/us/en/en/WF04a/12454-12454-64287-321860-3328898.html

Поддержка VT-d присутствует во всех компьютерах, поддерживающих технологию Intel vPro. Технология vPro базируется на двух технологиях: *AMT* (Active Management Technology) для удалённого управления железом и *VT* (*VT-x* + *VT-d*) для виртуализации процессора и систем ввода/вывода.

6.7 Дополнительная информация

- Использование VT-d в Xen[11]
- How to turn on VT-d in Xen[12] (англ.)
- Intel Virtualization Technology for Directed I/O[13] (англ.)
- Intel Virtualization Technology for Directed I/O (VT-d): Enhancing Intel platforms for efficient virtualization of I/O devices[14] (англ.)

[11] http://xgu.ru/wiki/xen/vtd
[12] http://wiki.xensource.com/xenwiki/VTdHowTo
[13] http://www.intel.com/technology/itj/2006/v10i3/2-io/1-abstract.htm
[14] http://softwarecommunity.intel.com/articles/eng/1416.htm