# IBM® Hidden Protected Area
## Access IBM Predesktop Area

# Introduction

IBM is changing its disk-to-disk recovery solution to improve customer usability and to further protect important user data. This paper presents an overview of the former disk-to-disk solution which was partition-based, and then provides an in-depth description of the new hidden protected area (HPA)-based disk-to-disk solution. Most new IBM computers available in 2003 will come with the HPA-based solution. The hidden protected area, also referred to as PARTIES, enables IBM to provide a disk-based recovery solution that provides greater flexibility and that enhances the security for recovery data, diagnostics and potential future applications.

# Partition-based recovery solutions

IBM systems currently use a hidden primary partition on the hard drive to store recovery, diagnostics, Rapid Restore PC (if it is installed), and data. This hard disk-based recovery is commonly called disk-to-disk. The figure below illustrates the space used and disk layout on a typical hard drive with a hidden primary partition, called a "service partition."

Service partition

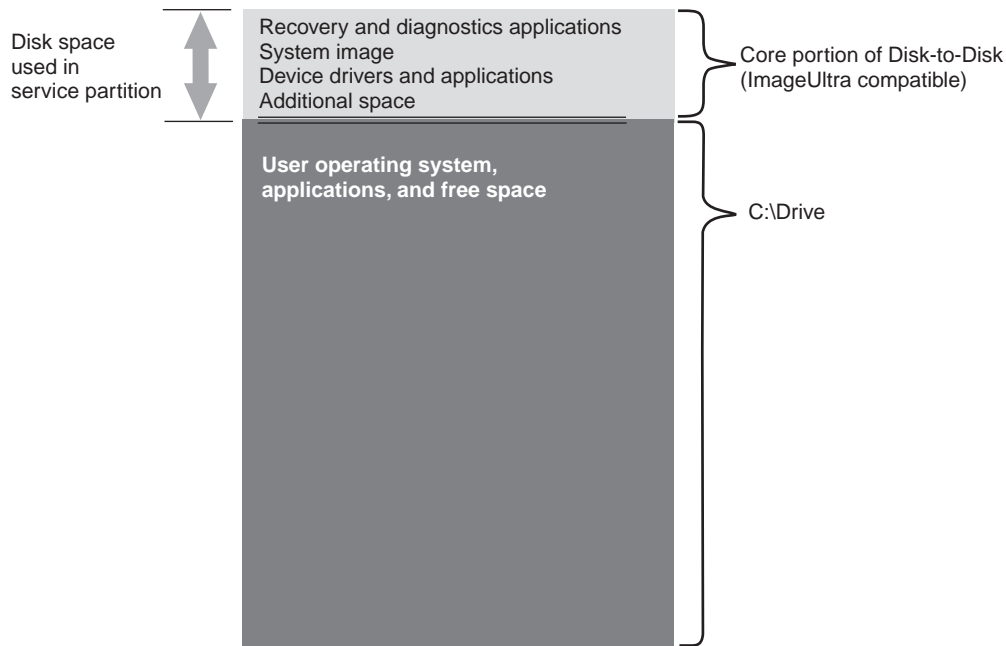**User operating system, applications, and free space**
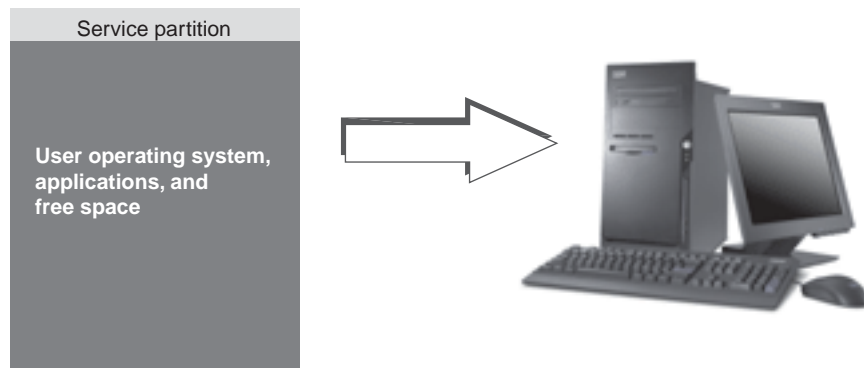
Hard disk-based recovery and diagnostics has many advantages over CD-based recovery solutions. With this recovery solution, a backup system image is always present on your hard drive in the service partition. No additional hardware or software is needed to restore your system, so there is nothing to lose or misplace. Consequently, any necessary waiting time is minimized and, in most cases, no technician is required. To access the recovery image, you simply interrupt the startup process by pressing F11.

A disadvantage of a partition-based solution is that it requires the use of a primary partition. This might cause problems for some users because Microsoft® Windows® operating systems are limited to four primary partitions on each hard disk. Also, a hard disk-based solution must use some hard disk space to store the recovery image.

## Hard-disk layout for a partition-based recovery solution

The service partition is simply a bootable area that holds the recovery image, including Rapid Restore PC (if it is installed), and all the data needed for a recovery process. The figure below illustrates the components of a computer using the former partition-based recovery solution.

Disk space used in service partition

Recovery and diagnostics applications
System image
Device drivers and applications
Additional space

Core portion of Disk-to-Disk
(ImageUltra compatible)

**User operating system, applications, and free space**

C:\Drive

# Hidden protected area-based recovery solutions

Upcoming IBM systems use a firmware-secured area of the hard disk known as the hidden protected area (HPA). The HPA is a standard from the ANSI/ATAPI committee (ANSI+NCITS+346-2001) that affords several advantages. With an HPA-based solution, each function can be stored in its own area. This enables each function to be individually protected and accessed. For example, by using an HPA-based recovery format, system diagnostics, Rapid Restore PC, or recovery data can each be accessed separately.

An HPA-based recovery solution provides a level of flexibility and security that is not available with the partition-based disk-to-disk recovery solution. Simply by separating the data in the hidden protected area, this solution provides greater protection from data loss and unauthorized access. Each of the areas is protected by firmware locking, which effectively hides the area from unauthorized software. Future enhancements to the HPA will continue to increase the security and flexibility of the hidden protected area. For example, a future release might include the option to selectively install or

uninstall features. Users also get more flexibility from a hidden protected area-based solution because all four primary partitions are still available for customer use.
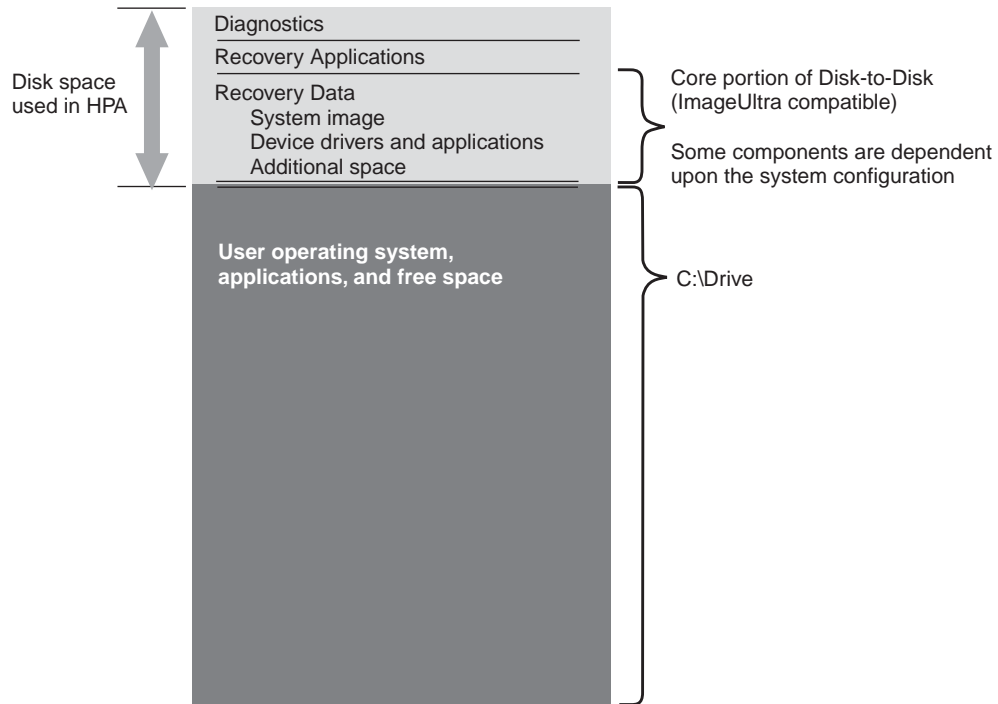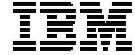
As with the former disk-based recovery solution, some disk space is needed to store the factory recovery image.  The amount of space needed to store the applications and data is based on the system ordered and the number of options.  On computers using the hidden protected area-based recovery solution, the total amount of disk space will reflect only the storage space available to the user.  The space used by the hidden protected area is subtracted from the total disk space.  For example, a 20 GB drive that has a 2 GB HPA will display as an 18 GB drive.  To access the contents of the HPA, you simply interrupt the startup process by pressing the Enter key.  ThinkPad computer users can also press the Access IBM button to interrupt the startup process.

The figure below illustrates the space used and disk layout on a typical hard drive using the HPA-based recovery solution.
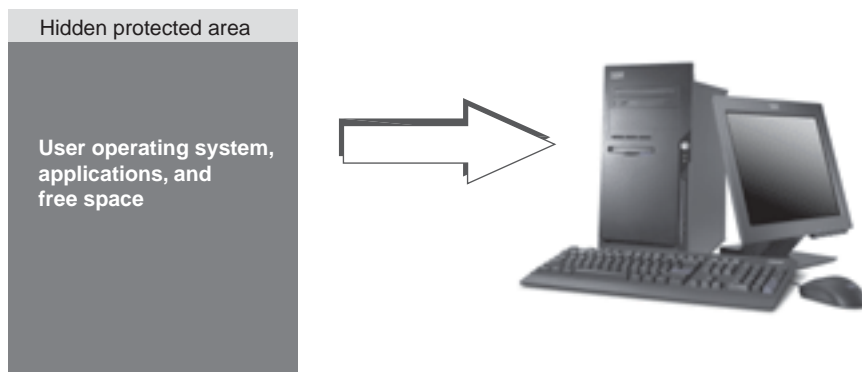


## Hard-disk layout for a hidden protected area-based recovery solution

The hidden protected area is separated into several areas. These areas store the recovery applications, Rapid Restore PC (if it is installed), and all the data needed to recover. Some extra disk space is also included.  The hard-disk layout of a typical computer with this solution includes the Access IBM Predesktop Area and additional space for storing startup information and security data.  Separate areas exist for diagnostics, recovery applications, and recovery data.  The figure below illustrates the components and disk layout of a system using an HPA-based recovery solution.
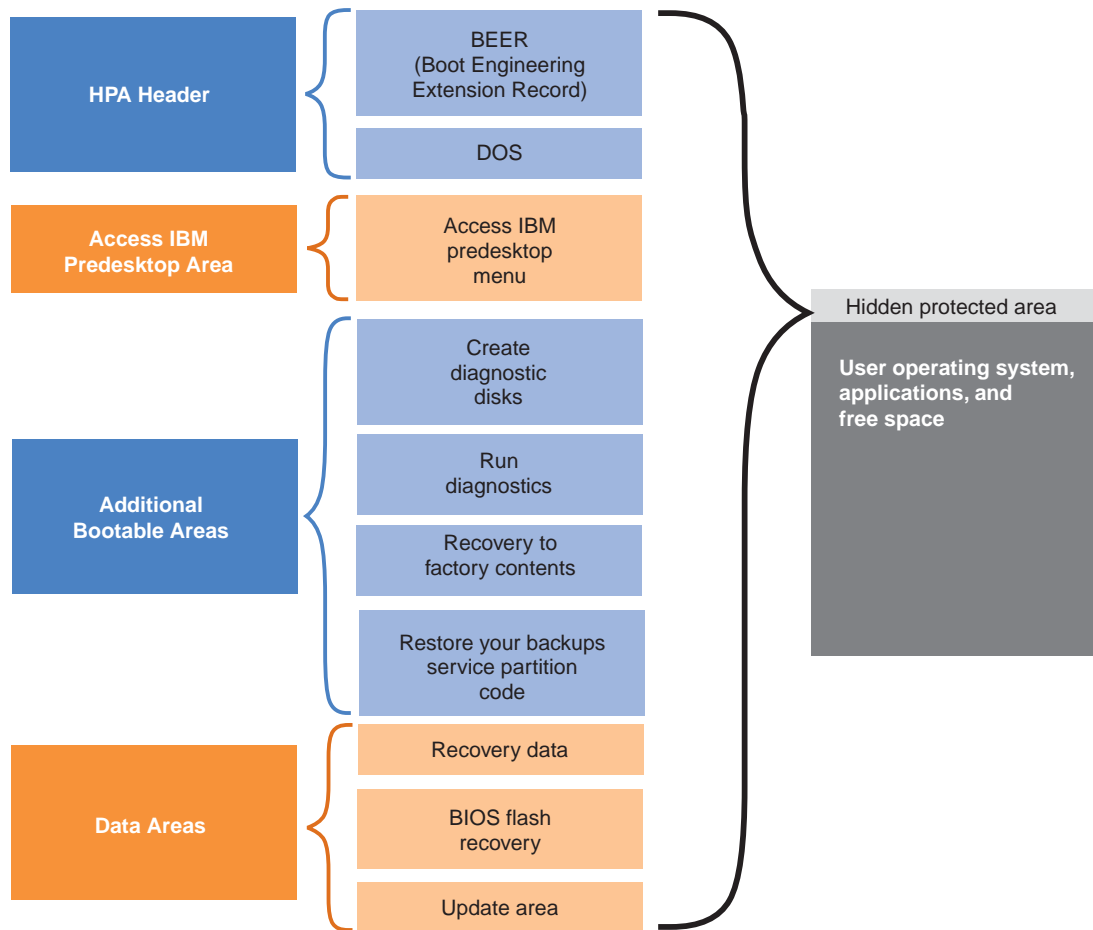
Diagnostics

Recovery Applications

Recovery Data
  System image
  Device drivers and applications
  Additional space

Disk space used in HPA

Core portion of Disk-to-Disk (ImageUltra compatible)

Some components are dependent upon the system configuration

**User operating system, applications, and free space**

C:\Drive

## HPA main areas

The hidden protected area space contains four main areas:
  HPA header
  Access IBM Predesktop Area
  Additional bootable functions areas
  Data areas

The diagram below provides details about the various sections.

| HPA Header | BEER (Boot Engineering Extension Record) |
| Access IBM Predesktop Area | DOS |
| | Access IBM predesktop menu |
| Additional Bootable Areas | Create diagnostic disks |
| | Run diagnostics |
| | Recovery to factory contents |
| | Restore your backups service partition code |
| Data Areas | Recovery data |
| | BIOS flash recovery |
| | Update area |

Hidden protected area

**User operating system, applications, and free space**

## HPA header

The HPA header consists of two parts: a boot engineering extension record (BEER) and a directory of services (DOS). For complete treaties on the hidden protected area, see the ANSI/ATAPI committee document (ANSI+NCITS+346-2001).  The HPA header is similar to a partition table.  It contains a listing of all the areas in the HPA, along with their sizes.

## Access IBM Predesktop Area

The Access IBM Predesktop Area is the main entry point for the user.  Press the Enter key during startup to access the Access IBM Predesktop Area.  (ThinkPad computer users can also press the blue Access IBM button during startup to access the Access IBM Predesktop Area.)  This area presents the user with a number of selections, as shown in the task-based interface below.
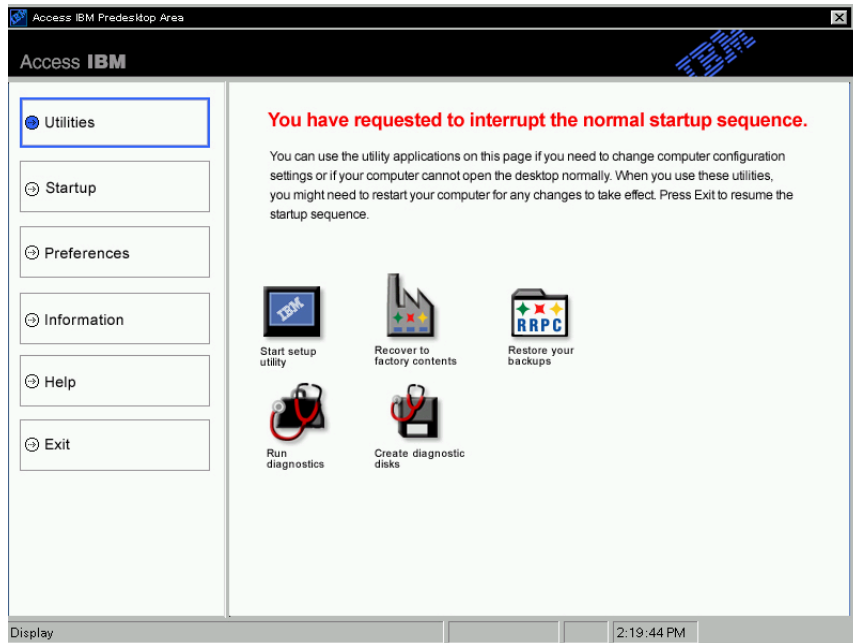
To select an activity, click the desired task or use the Tab key to highlight the desired task and then press Enter.  Each icon represents a separate function which has its own area within the HPA.  These functions are performed independently of the operating system.

## Additional bootable areas

The hidden protected area enables additional bootable areas to be established. Future releases will enable customers to create an additional bootable area by installing a bootable image into the hidden protected area. An icon representing the area will then be added to the Access IBM Predesktop Area.

Each bootable area is digitally signed to deter tampering and to prevent viruses.  Every time an area is booted its signature is checked. Only validly signed areas are allowed to boot.

## Data areas

Data areas provide storage and additional space for the bootable areas. Data areas store recovery data, flash repair and recovery data, and Rapid Restore PC data (if it is installed).  An update area also exists that enables IBM to supply patches and updates to the HPA areas.

# Keys used during startup

Depending upon the model and configuration of your IBM system, different keys might
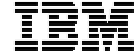
be used to interrupt the startup sequence and to access various functions. The table below lists the keys and functions that are available when the BIOS screen is displayed. The new default factory-installed configuration is highlighted.

| Key | System Configuration | | | | |
|-----|-------|-------|-------|-------|-------|
| | New HPA-based recovery configurations | | Former partition-based recovery configurations | | |
| | HPA no service partition no RRPC BIOS: HPA enabled | HPA **with** service partition **with** RRPC BIOS: HPA enabled | No HPA **with** service partition BIOS: **not** HPA-enabled | No HPA **with** service partition BIOS: HPA-enabled | No HPA No service partition BIOS: HPA-enabled |
| F1 | BIOS Setup | BIOS Setup | BIOS Setup | BIOS Setup | BIOS Setup |
| F11 | Disabled | RRPC (NetVista) Disabled (ThinkPad) | Recovery | Recovery | Disabled |
| F12 | Alt Boot menu (text mode) | Alt Boot menu (text mode) | Alt Boot menu (text mode) | Alt Boot menu (text mode) | Alt Boot menu (text mode) |
| Enter | Access IBM Predesktop Area | Access IBM Predesktop Area | Nothing (ThinkPad) BIOS menu (NetVista) | BIOS menu | BIOS menu (no recovery choice) |
| Access IBM Button (ThinkPad only) | Access IBM Predesktop Area | Access IBM Predesktop Area | Nothing | BIOS menu | BIOS menu (recovery choice) |

# BIOS Access IBM predesktop security levels

Along with the startup options, the hidden protected area also has some configuration options. The configuration options can be accessed using in the BIOS setup screen. The table below lists the available security settings for the hidden protected area.

| Setting | HPA | | | Attributes | | | | |
|---------|--------|--------|----------|------------------|------------------|-----------------|----------------|--------------|
| | Locked | Hidden | Bootable | Cloning Enabled | Protected from Removal | Support User Updates | Security Level | User Profile |
| High Security | Yes | Yes | Yes | Cloning not possible. | Removal not possible. | Updates not yet possible. | Highest security. | Security conscious users. |
| Normal Security (Default) More secure than the current solution. | No | Yes | Yes | Cloning possible. Industry tools must be modified to issue clone commands. | IBM provides a tool for removing the HPA, if requested. | Updates possible. | Medium security. The HPA can be made visible. | Manageability conscious users. |
| Security Disabled | No | No | No | Cloning possible. | Removal is possible. | Updates possible. | No security. The entire HPA is open and visible. | Customers who want to clone sector-based images. |

Notes:

1.  If you are using the high security setting, be sure to verify that the high security mode has been restored in BIOS settings after a service action is required (for example, the system board is replaced).

2.  Do not disable security to remove the hidden protected area. IBM provides a Web tool that can be downloaded from the IBM web site for this purpose. The Security Disabled setting is only intended to be used when creating an image of the drive using a sector-based imaging tool. Security should be restored after the image has been created.

# Conclusion

A hidden protected area-based service space offers numerous advantages. The Access IBM Predesktop Area provides users with a less confusing and more usable interface, which will reduce the anxiety many users feel when working in a preboot environment.

Each function of the Access IBM Predesktop Area has its own reserved space that is separate from the other functions. This provides a level of flexibility and security that previously was not available. Future enhancements will continue to increase the security and flexibility of the hidden protected area. Also, limitations caused by the Microsoft Windows operating system are avoided because all four primary partitions are still available for customer use.

Along with the improved security, usability, and flexibility, an HPA-based recovery solution has the advantages of IBM's existing hard disk-based solution. As stated earlier, a hard disk-based recovery solution enables a backup system image to be present on the hard drive in the service partition. No additional hardware or software is needed to restore the system, so there is nothing to lose or misplace. Consequently, any necessary waiting time is minimized and, in most cases, no technician is required.

# Appendix

## Creating an image of the hard drive

The procedure for creating and delivering an image of the hard drive with an HPA-based system is different than the procedure for creating and delivering an image of the hard disk with a hidden partition.

To create an image of a hard disk using an HPA-based system, you must complete the following procedure using IBM-supplied tools and a third party disk-imaging tool, such as Phoenix ImageCast, PowerQuest DriveImage, or Symantec Ghost.

1. Ensure that the Access IBM Predesktop Area security level is set to Normal. This is the IBM default setting.

2. Copy the FWBACKUP and FWRESTOR tools from the factory recovery area in the HPA using the following procedure:

   a. Start the system and press the Enter key or the Access IBM button during startup.
   b. Double-click the Recover to Factory Contents icon. The Recovery Menu is displayed.
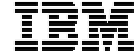
c. Press the F3 key. A command prompt is displayed.
d. Change to the A: drive. (This is a virtual diskette drive in the hidden protected area.)
e. Change to the recovery directory.  The command prompt displays `A:\RECOVERY>`
f. Insert a diskette into the diskette drive, which is mapped as the B: drive.
g. Type `copy fwbackup.exe b:`
h. Type `copy fwrestor.exe b:`
i. Eject the disk and turn the system off.
j. Follow the directions below for using FWBACKUP and FWRESTOR.

3. Create an image of the hidden protected area using a command prompt to run the FWBACKUP tool.

   FWBACKUP has the following format:
   ```
   FWBACKUP size=<span file size must be between 25MB and
   640MB> file=<Path and name of file set>
   ```

   If you are creating an image of the HPA to a network drive, it must have a drive letter assigned. For example, if you want to store an image of the HPA space to drive D: that is of span size 640MB, the command is
   ```
   FWBACKUP size=640 file=d:\IMGSET
   ```

   The image set consists of files `IMGSET.001…IMGSET.nnn`.

4. Create an image of the main partition using a third party imaging tool to capture first the C: partition, and then the main partition.

5. Restore the hard drive image using the following procedure:

   a. Make sure the destination hard drive is blank.
   b. Make sure that the master boot record is deleted and that no partitions exist on the hard disk.
   c. Run FWRESTOR from a command prompt. FWRESTOR has the following format:
      ```
      FWRESTOR file=<name of span file set>
      ```

      If you are restoring an image of the HPA from a network drive, it must have a drive letter assigned. For example, if you want to restore an image from the D: drive that was created using the above example.  The command would be:
      ```
      FWRESTOR file=D:\IMGSET
      ```

This loads all the files in the image set (`IMGSET.001 ...`
`IMGSET.nnn`). All of the files in the image set must be in the same
subdirectory.

    d.  When this is complete, perform a power cycle.

6.  Restore the main partition using the normal procedure of your imaging tool.

7.  Restore the security setting to High Security, if this setting was changed in
Step 1.

# Notices

make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

## Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:
   IBM
   NetVista
   ThinkPad

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.