

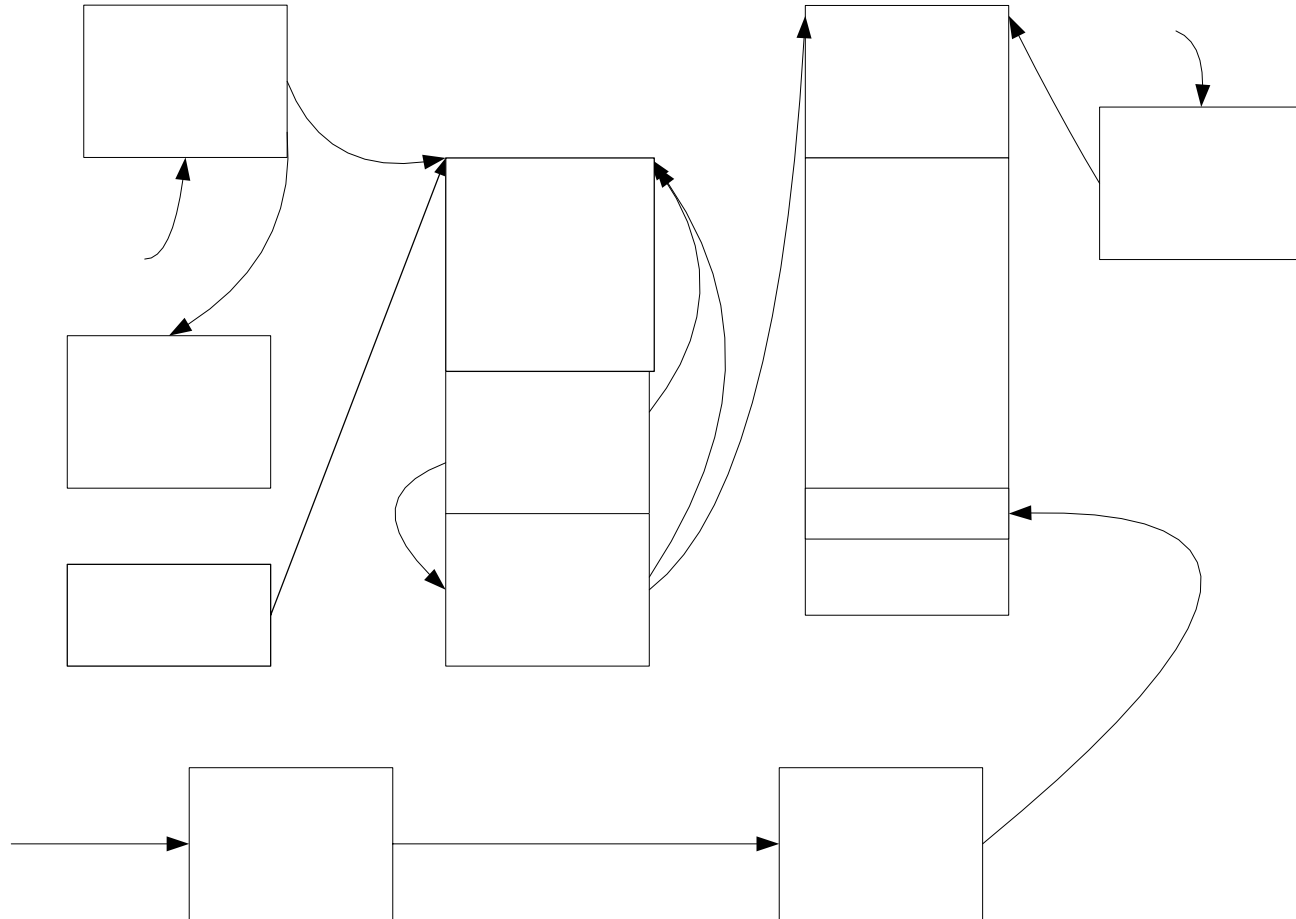
Windows Kernel Internals

Advance Virtual Memory

*David B. Probert, Ph.D.

Windows Kernel Development
Microsoft Corporation

Shared Memory Data Structures



File Ob

PFN: Working Set Page

WorkingSetIndex					
PteAddress					
ShareCount					
Flags			RefCount		
OriginalPTE					
PteFrame	iperr	vrfy	awe	kstk	cach

PFN: Free Page

ForwardLink					
PteAddress					
ShareCount					
Flags			RefCount		
OriginalPTE					
PteFrame	iperr	vrfy	awe	kstk	cach

PFN: Standby Page

ForwardLink					
PteAddress					
BackLink					
Flags			RefCount		
OriginalPTE					
PteFrame	iperr	vrfy	awe	kstk	cach

PFN: Transition page

Event					
PteAddress					
ShareCount					
Flags			RefCount		
OriginalPTE					
PteFrame	iperr	vrfy	awe	kstk	cach

PFN Fields

PteAddress: VA of PTE referencing page

RefCount: count of WS or IO locks

OriginalPte: PTE to restore on soft-fault

PteFrame: PageFrame for PteAddress

Flags:

Modified : 1

ReadInProgress : 1

WriteInProgress : 1

PrototypePte: 1

PageColor : 4

PageLocation : 3

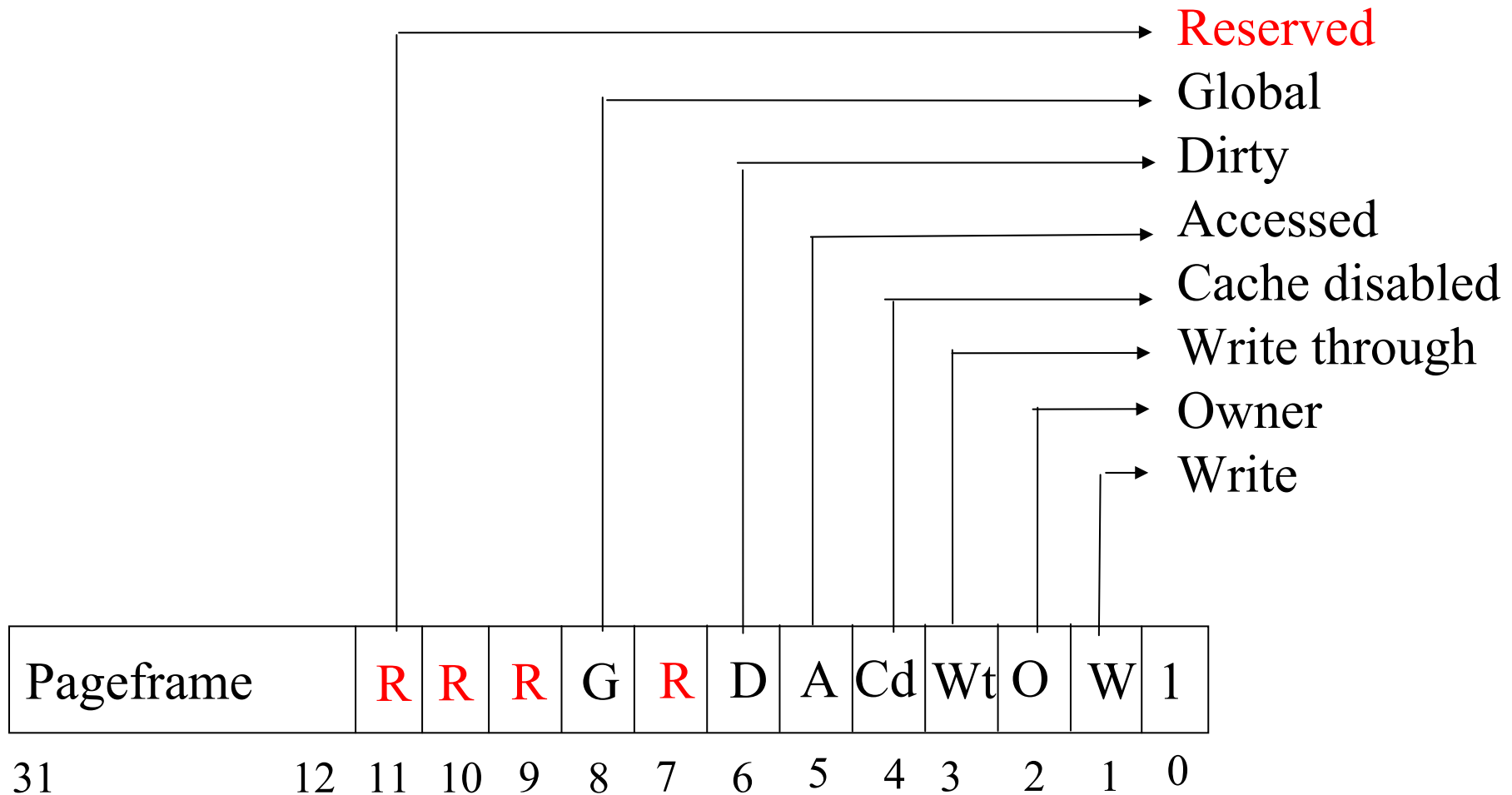
RemovalRequested : 1

CacheAttribute : 2

Page Table Entries

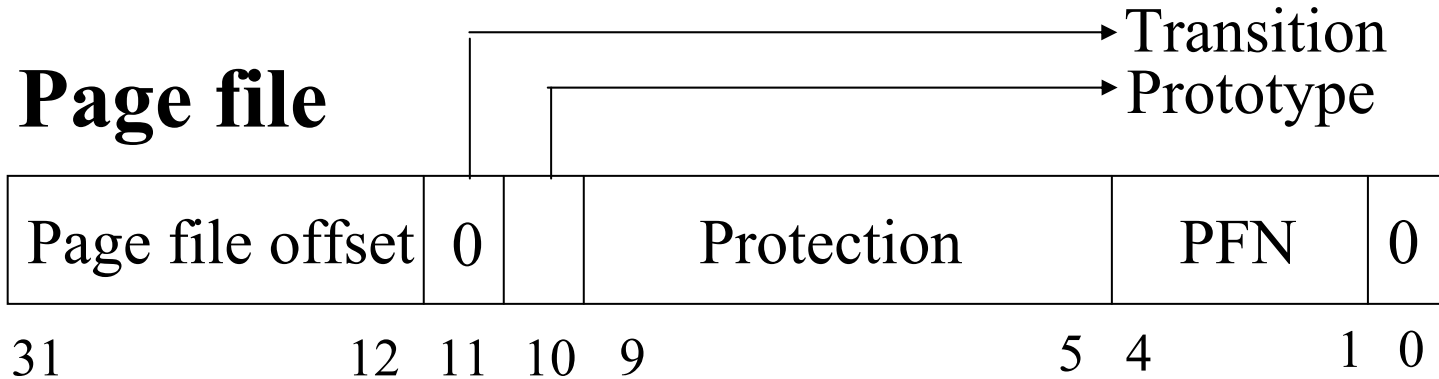
- Some fields defined by hardware
- Six PTE states:
 - Active/valid
 - Transition
 - Modified-no-write
 - Demand zero
 - Page file
 - Mapped file

Valid x86 Hardware PTEs

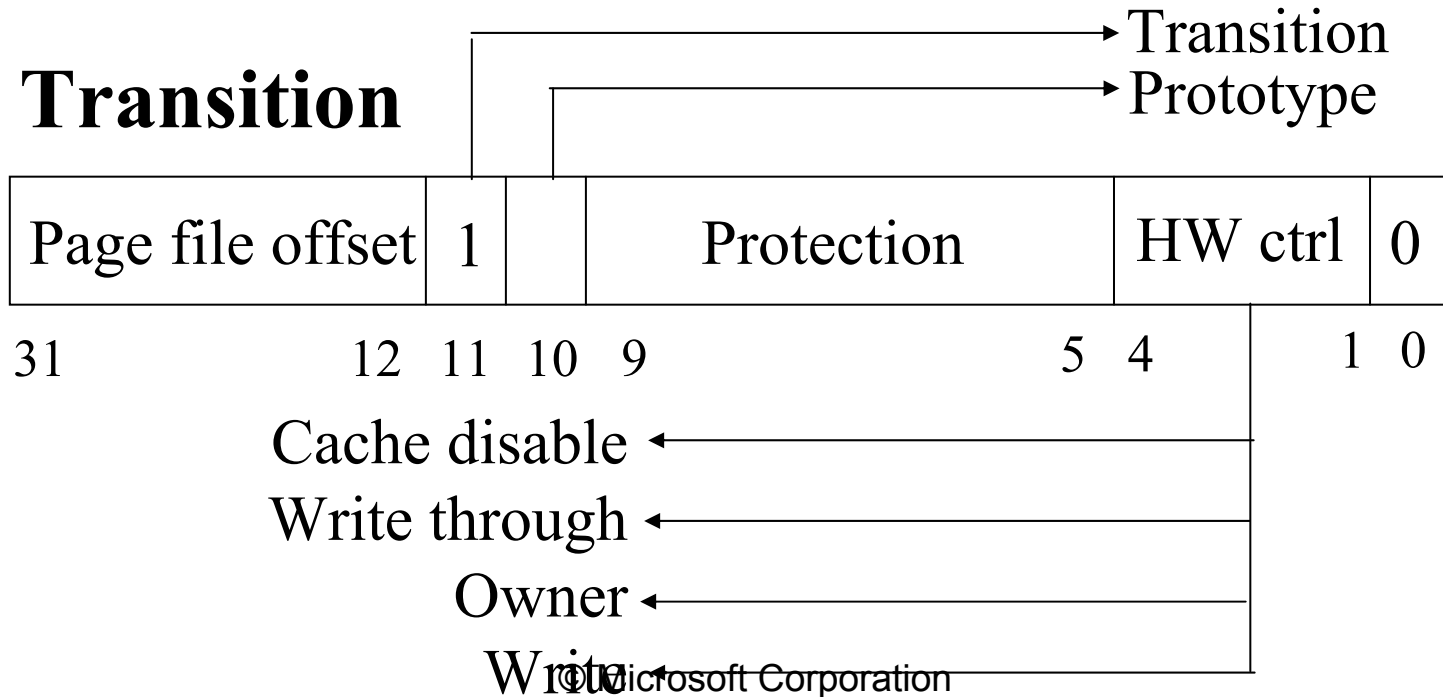


x86 Invalid PTEs

Page file



Transition

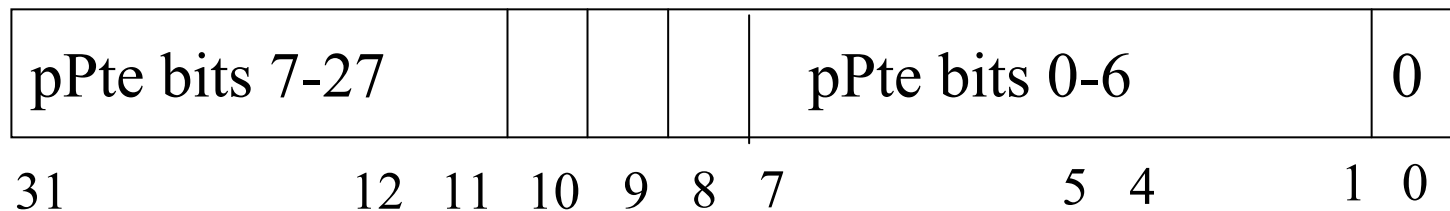


x86 Invalid PTEs

Demand zero: Page file PTE with zero offset and PFN

Unknown: PTE is completely zero or Page Table doesn't exist yet. Examine VADs.

Pointer to Prototype PTE



MMPAGING_FILE

- **PFN_NUMBER** Size, MaxSize, MinSize, FreeSpace, CurrUsage, PeekUsage, HighestPage
- pFileObject
- ModWriterMdlEntries[]
- pPageFileName
- pAllocationBitmap
- **Flags:**
 - PageFileNumber, RefCount, BootPart

MMSUPPORT

// embedded in EPROCESS

- WorkingSetExpEntry[2]
- LastTrimTime
- Flags
- PageFaultCount, PeakWorkingSetSize, GrowthSinceLastEstimate
- MinimumWorkingSetSize, MaximumWorkingSetSize
- pVmWorkingSetList
- **WSLE_NUMBER** Claim, NextEstimationSlot, NextAgingSlot, EstimatedAvailable, WorkingSetSize

MMADDRESS_NODE

- pParent, pLeft, pRight
- StartingVpn, EndingVpn

MMVAD

- **MMADDRESS_NODE** AddressTreeNode
- pControlArea
- pFirstProtoPte
- pLastContigPte
- **Flags:**
 - CommitCharge, PhysMap, ImageMap, Awe, Prot, MemCommit, Private, LargePages, WriteWatch, NoChange, FileOffset64k, SecNoChange, ReadOnly, Extendable, Inherit, CopyOnWrite

CONTROL_AREA

- pSegment
- DereferenceListEntry[2]
- nSectRefs, nPfnRefs, nMapView, nCacheViews, nUserRefs
- nModWrites, nFlushesActive,
- Flags
- pFileObject
- iPfnBase
- Subsections[]

SUBSECTION

- pControlArea
- Flags:
 - ReadOnly, ReadWrite, SubsectionStatic, GlobalMemory, Protection, StartingSector, SectorEndOffset
- StartingSector
- nFullSectors
- pSubsectBasePtes
- nUnusedPtes
- nPtesInSubsection
- pNextSubsection
- nMappedViews

SECTION

- **MMADDRESS_NODE** AddressTreeNode
- pSegment
- Size
- InitialPageProt
- **Flags:**
 - BeingDeleted, BeingCreated, BeingPurged, NoModifiedWriting, FailAllo, Image, Based, File, Networked, NoCache, PhysicalMemory, CopyOnWrite, Commit, FloppyMedia, WasPurged, UserReference, GlobalMemory, DeleteOnClose, FilePointerNull, DebugSymbolsLoaded, SetMappedFileIoComplete, CollidedFlush, NoChange, HadUserReference, ImageMappedInSystemSpace, UserWritable, Accessed, GlobalOnlyPerSession, Rom

SEGMENT

- pControlArea
- nPtes
- nWritableUserRefs
- Size
- PteTemplate
- nCommittedPages
- Flags
- BasedAddress
- PrototypePte
- ProtoPtes[]

Discussion