zD&T

LEARNING WITH A PERSONAL MAINFRAME

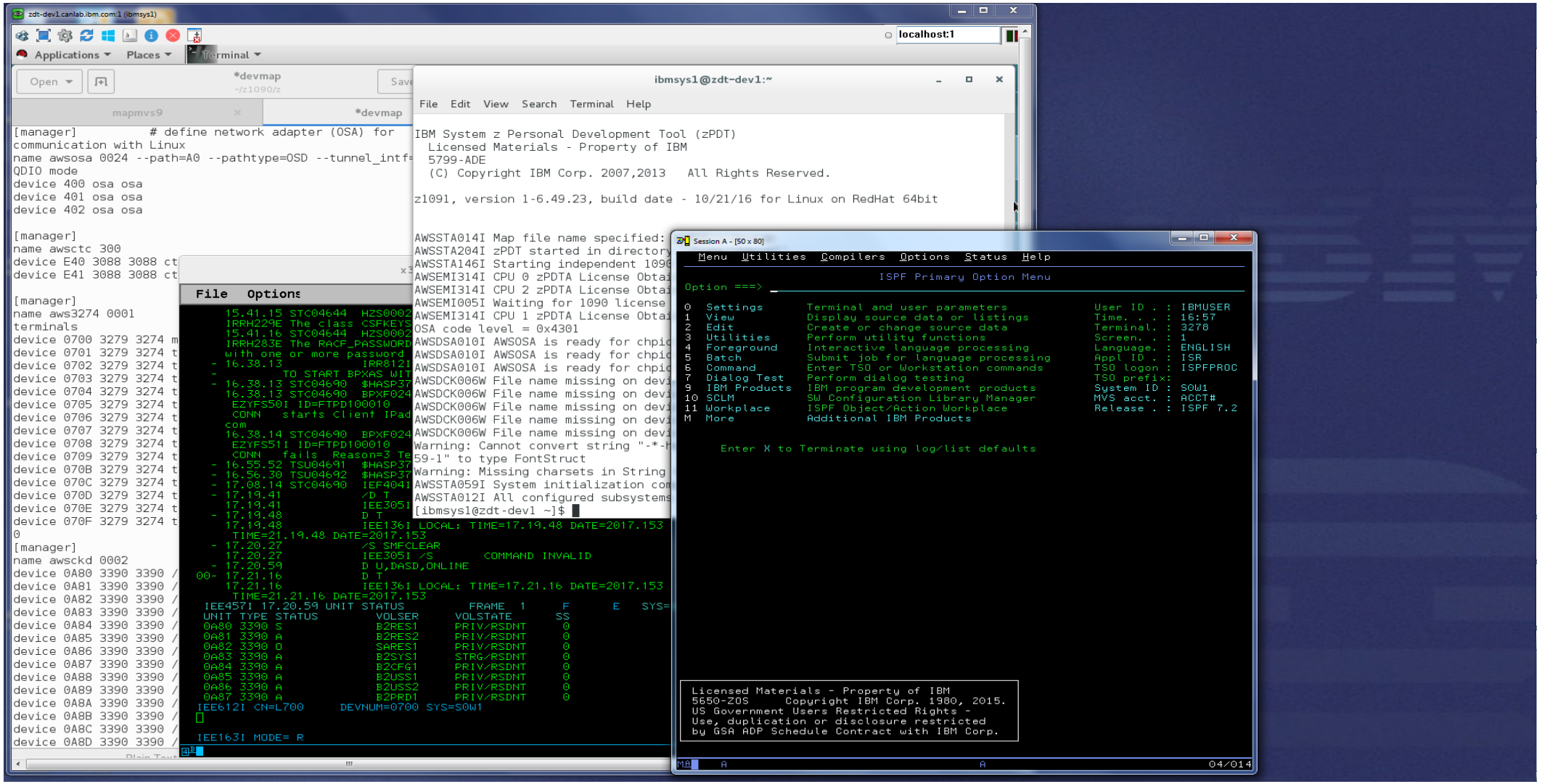
Innocent Question

```
17149 22:38:26.28 JACOB3   00000290  D T
17149 22:38:26.33 TSU04462 00000090  IEE345I DISPLAY  AUTHORITY INVALID, FAILED BY SECURITY PRODUCT
17149 22:38:26.35 TSU04462 00000281  ICH408I USER(xxxxxx  ) GROUP(SYS1    ) NAME(xxxxx xxxxxxxx     )
                      730 00000281    MVS.DISPLAY.TIMEDATE CL(OPERCMDS)
                      730 00000281    INSUFFICIENT ACCESS AUTHORITY
                      730 00000281    FROM MVS.* (G)
                      730 00000281    ACCESS INTENT(READ   )  ACCESS ALLOWED(NONE   )
```

Display Time: time is not secret, operator commands are protected.

Shared systems impose restrictions.

This is personal



zD&T user can

Administer

Modify the system

Examine internal organs

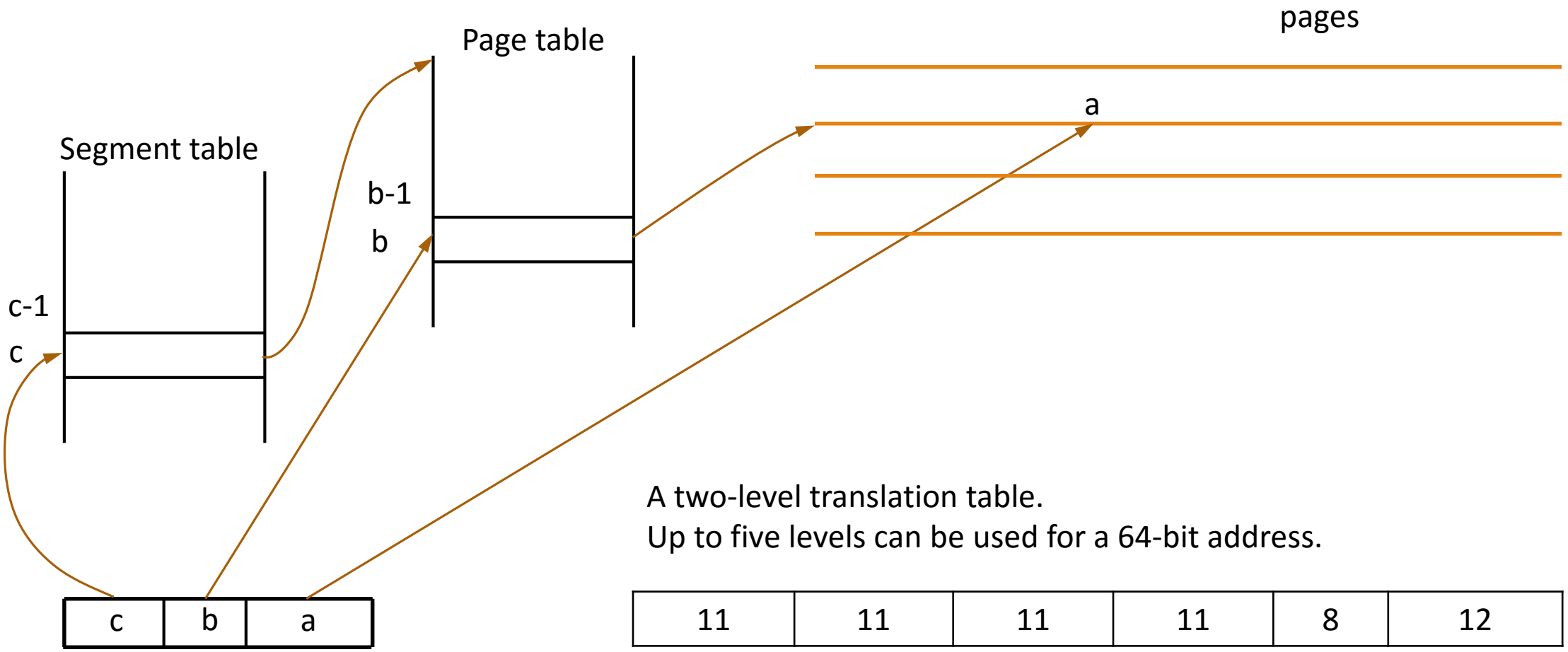
Problem set

Problem 1. A virtual address and a translation table define a name slot in a visitor book located outside your address space. Store your name in this slot.

Problem 2. Intercept SVC 35 (WTO). Write to the system log every time a WTO message arrives.

Problem 3. Define RACF resources for a filtering program that automates the mail work described in the opening pages of *Catch-22*.

Address translation



A two-level translation table.
Up to five levels can be used for a 64-bit address.

11	11	11	11	8	12

Visitor Book

```
         SYSEVENT TRANSWAP                    Make the book address space non-swappable

         STORAGE OBTAIN,LENGTH=4096,LOC=31    Obtain a page and fix it in real storage
         ST     1,PAGEADDR
         PGSER  R,FIX,(1)

         MODESET mode=SUP                     switch to supervisor state
         STCTG 1,1,TOKEN                      store ASCE into token
         MVC   TOKEN+8(4),=F'0'
         MVC   TOKEN+12(4),PAGEADDR           store 31-bit virtual address

         CALL  IEANTCR,(=F'4',                system-level pair
               =CL16'Visitor book',           pair's name
               TOKEN,
               =F'0',
               RETCODE)

TOKEN    DS    2AD
```

Translation

ASCE	52-bit number of real storage page for the top-level translation table		T	

T is the type of the table, tells what level is at the top

```
        MODESET MODE=SUP,KEY=ZERO      Arm for privileged code and protected storage
        SAM64                          set 64-bit addressing
        …
REGION2 DS    0H
        LG    R1,=x'001FFC0000000000'  mask for region-2 index
        NGR   R1,R10                   region index bits
        SRLG  R1,R1,64-22-3            region index times 8
        AGR   R11,R1                   point to table entry
        LURAG R11,R11                  load the entry
        LHI   R0,32                    1 to validity position
        NR    R0,R11                   is the entry valid?
        JNZ   BADRGN2
        NILL  R11,X'F000'              clear last 12 bits
```

After traversing the tables, R11 contains the real address of the target.

```
LG    R0,=CL8’Visitor’
STURG R0,R11                make a record
```

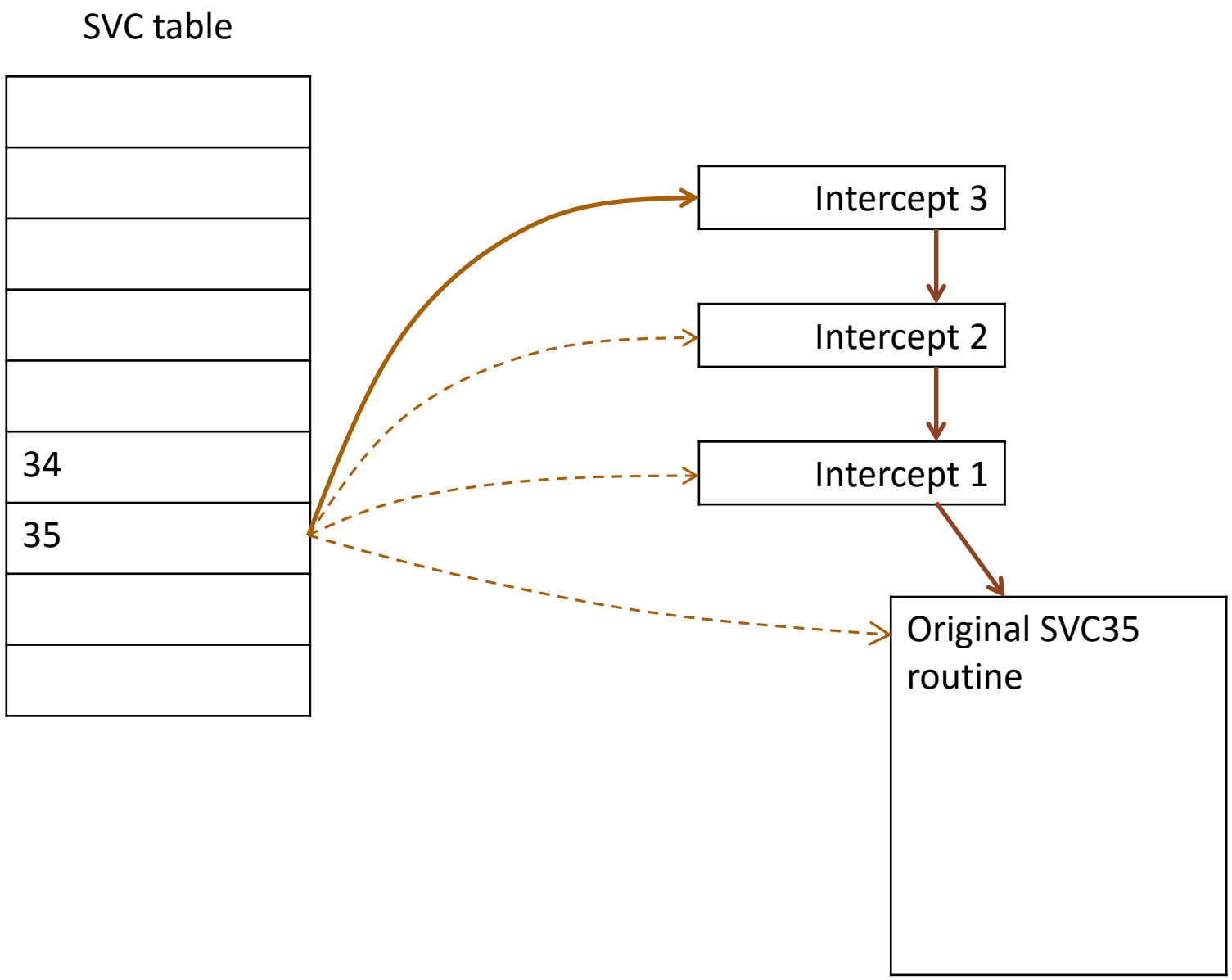
For debugging, this code can translate a virtual address in its own address space, where *load real address* (LRA) instruction will show the correct result

```
LRA   R3,0(,R10)            load real address
CLGR  R3,R11                compare to my result
JNE   NOTREAL
```

SVC Routine

```
SVCSTART L     R6,ORIGEP-SVCSTART(R6)           original SVC35 entry point
         BAKR  R6,0                             save registers
         WTL   'ZDT0001I A message is coming'   write to log
         EREGG R15,R1                           restore some registers
         PR    ,                                go to real SVC35
ORIGEP   DS    A
```

Make a record in syslog and pass control to the original routine.


SVC table
34
35
Intercept 3
Intercept 2
Intercept 1
Original SVC35 routine

Install

```
         STORAGE OBTAIN,LENGTH=SVCLEN,SP=241,LOC=(31,31)       CSA storage
         LR    R2,R1
         MODESET KEY=ZERO,MODE=SUP
         MVC   0(SVCLEN,R2),SVCSTART                  copy the code to CSA
         OILH  R2,X'8000'                             amode31 bit
         SVCUPDTE 35,REPLACE,TYPE=4,EP=(R2)           update the table
```

Install a second and a third routine and issue a D T command:

```
ZDT0003I A message is coming
ZDT0002I A message is coming
ZDT0001I A message is coming
         IEE136I LOCAL: TIME=10.43.11 DATE=2017.156  UTC: TIME=14.43.11
         DATE=2017.156
```

Questions

How to remove an intercept?

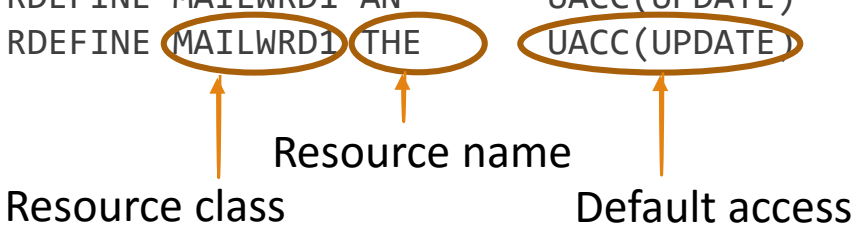
Why SVCUPDTE?

Can the interceptor modify the message?

Mail Filter With RACF Rules

Proscribe all but articles.

```
RDEFINE MAILWRD1 *        UACC(NONE)
RDEFINE MAILWRD1 A        UACC(UPDATE)
RDEFINE MAILWRD1 AN       UACC(UPDATE)
RDEFINE MAILWRD1 THE      UACC(UPDATE)
```



RACF is a string-matching engine. With multiple matches, the most specific one wins.

Resource class defines a name space.

Resource class

Class is created as a new resource in the CDT – Class Definition Table

```
RDEFINE CDT MAILWRD1 UACC(NONE)
  CDTINFO(MAXLENGTH(100) FIRST(ALPHA)       alphanumeric strings up to 100 characters
  OTHER(ALPHA,NUMERIC,NATIONAL,SPECIAL) POSIT(22)


SETROPTS RACLIST(CDT) REFRESH               refresh the table
SETROPTS GENERIC(MAILWRD1)                  enable generic matching
SETROPTS CLASSACT(MAILWRD1)                 activate the class
```

Filtering Goals

1. Reject every adverb and every adjective
2. Reject articles
3. Allow only the salutation
4. Reject a given city on the mail envelope

Name space needs three dimensions

1. Location in the message (envelope, salutation, signature or body)
2. Part of speech
3. Word

Access Check

The filtering program will have to ask RACF about every word it finds:

```
         RACROUTE REQUEST=AUTH,ATTR=UPDATE,                            x
               CLASS='MAILWRD1',ENTITYX=RSTRING,                       x
               WORKA=WORKAREA,                                         x
               RELEASE=77A0

RSTRING  DC    Y(100,25),CL100’SALUTATION.ADJECTIVE.DEAR'
```

With goal #1, RACF will deny access:

```
ICH408I USER(xxxxxx  ) GROUP(xxxx    ) NAME(xxxxx               )
  SALUTATION.ADJECTIVE.DEAR CL(MAILWRD1)
  INSUFFICIENT ACCESS AUTHORITY
  FROM *.ADJECTIVE.* (G)
  ACCESS INTENT(UPDATE )  ACCESS ALLOWED(NONE   )
```

Clean Slate

zD&T can take a snapshot of a disk. The emulator command on Linux to remember the current state of B2SYS1:

```
awsckd –ve z/disks/B2SYS1
```

When experiments are completed, a disk can be restored to the original state:

```
awsckd –vr z/disks/B2SYS1
```