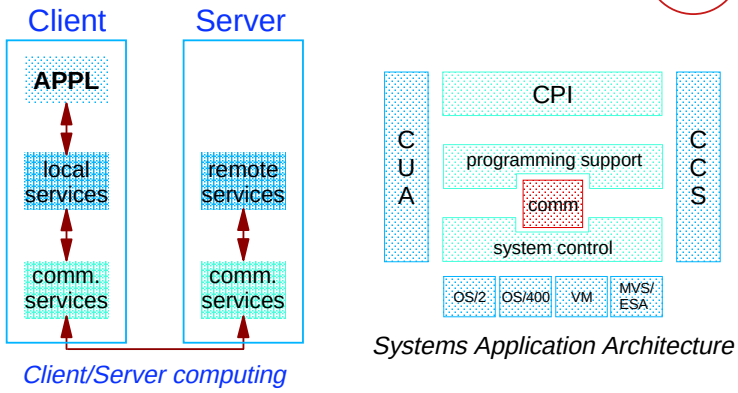
## Vanguard Enterprise Security Expo '99

APPC & RRSF Technical Cookbook
Walt Farrell

RACF Development BWVA/P385
IBM Corporation
522 South Road
Poughkeepsie, NY 12601
wfarrell@us.ibm.com
(914) 435 - 7750

## Cooperative Processing




Cooperative processing is a technique for implementation of application functions across two or more platforms.

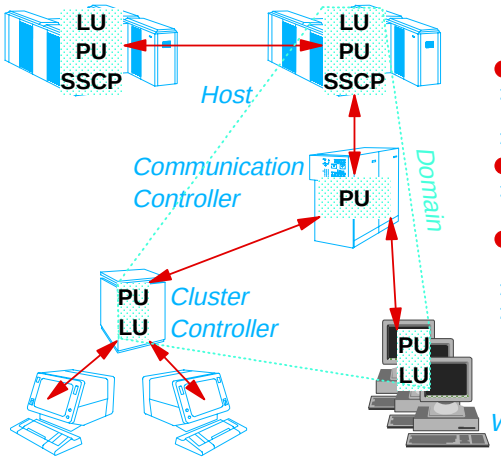


## Some Definitions

- **Common Communication Support (CCS)**
  - *Interconnection protocols between systems*
- **System Network Architecture (SNA)**
  - *Description of the logical structure, formats, protocols, and operational sequences for transmitting information units through networks*
- **SNA Logical Unit 6.2**
  - *LU 6.2 is a set of rules and protocols that handle communication between application programs*
- **Common Programming Interface (CPI)**
  - *Defines a set of building blocks that enable an application to be consistently developed and implemented across the supported platforms*
- **Advanced Program to Program Communication (APPC)**
  - *Implementation of LU type 6.2 on a given system*

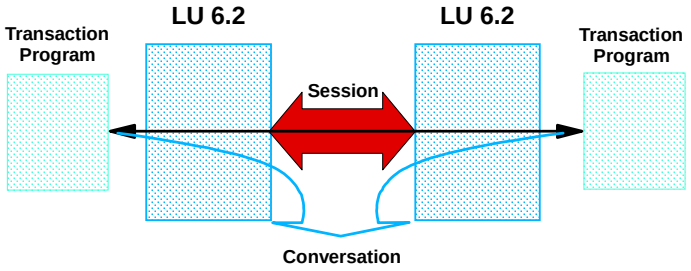


## SNA Network Components




- Node
  - *HW + SW that implements SNA functions*
  - *Various types*
- Links
  - *Connect adjacent nodes to one another*
- Network Addressable Units (NAU)
  - *Physical unit (PU)*
  - *Logical Unit (LU)*

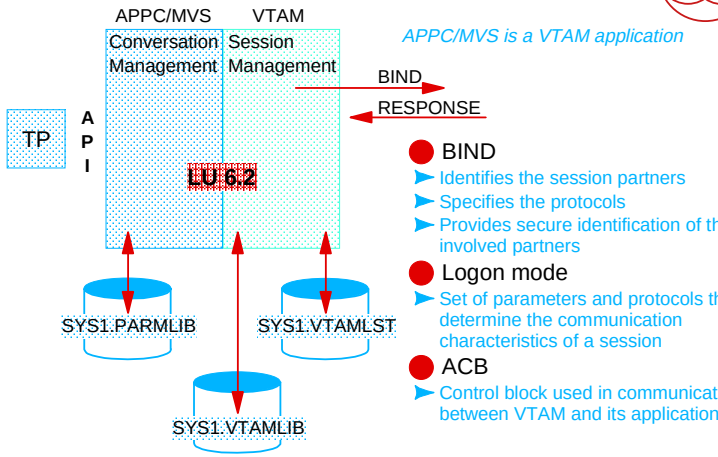
## APPC Basics




- Session is a logical connection between LUs (logical units).
- End-user applications are called ***Transaction Programs*** (TPs).
- Conversations flow between the Transaction Programs connected in a session.



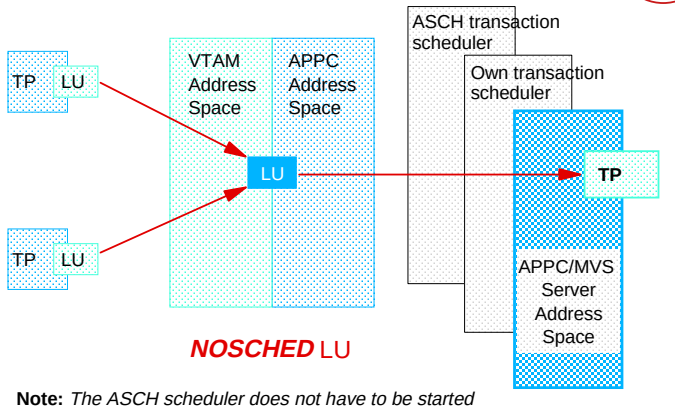
## VTAM and APPC/MVS




- BIND
  - Identifies the session partners
  - Specifies the protocols
  - Provides secure identification of the involved partners
- Logon mode
  - Set of parameters and protocols that determine the communication characteristics of a session
- ACB
  - Control block used in communication between VTAM and its applications



## APPC/MVS Inbound Request

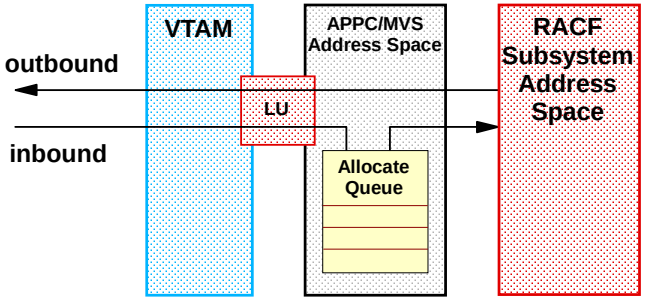



***NOSCHED*** LU

**Note:** *The ASCH scheduler does not have to be started*



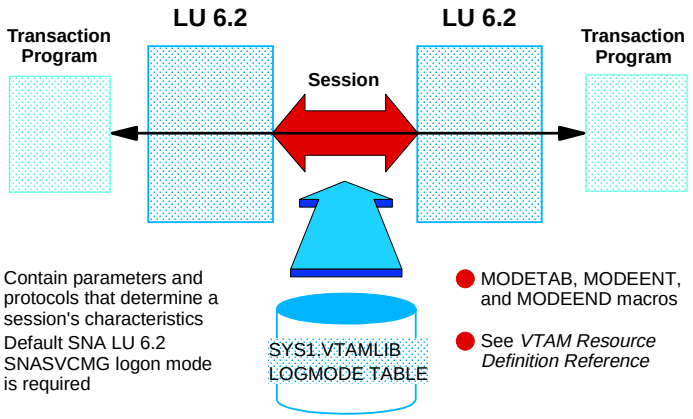
## RRSF Use of APPC/MVS




The server issues a **Register_For_Allocates** to indicate to APPC/MVS what inbound requests it is to service.

The server specifies the name of the local TP and the LU that are targeted by the allocate request.

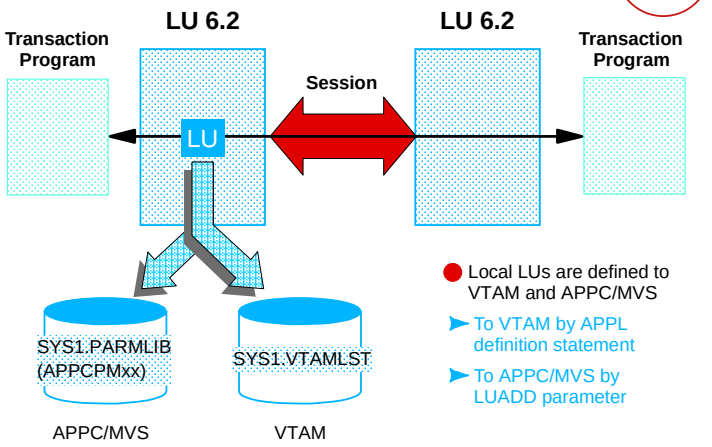
## APPC Logon Mode




- Contain parameters and protocols that determine a session's characteristics
- Default SNA LU 6.2 SNASVCMG logon mode is required
- MODETAB, MODEENT, and MODEEND macros
- See *VTAM Resource Definition Reference*



## Local Logical Unit




- Local LUs are defined to VTAM and APPC/MVS
  - To VTAM by APPL definition statement
  - To APPC/MVS by LUADD parameter



## LU Definition

- **Define local LU to APPC**
  - SYS1.PARMLIB(APPCPMxx)

```
LUADD ACBNAME=(SCRACFRR)
      NOSCHED
      TPDATA(SYS1.RACF.APPCTP)
```

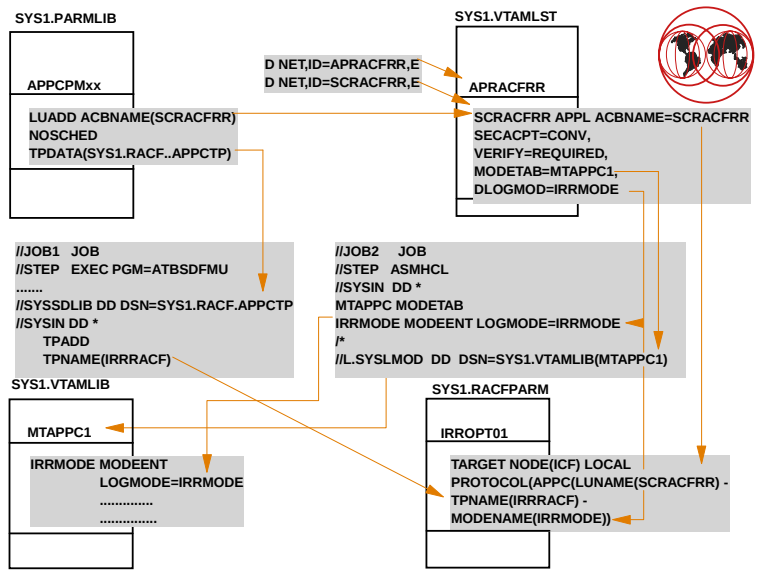
- **Define local LU to VTAM**
  - SYS1.VTAMLST

```
SCRACFRR  APPL  ACBNAME=SCRACFRR,      X
                APPC=YES,              X
                DLOGMOD=IRRMODE,       X
                MODETAB=MTAPPC1,       X
                SECACPT=CONV,          X
                VERIFY=REQUIRED
```

- **Define local LU to RACF**
  - SYS1.RACF.PARMLIB

```
TARGET NODE( )  PROTOCOL(APPC(LUNAME(SCRACFRR))
```





## Administrative Data

- **Two types of administrative data help to control the flow of conversations in an APPC/MVS environment.**
  - ***TP Profile data*** **Contains scheduling and security information**
  - ***Side Information data*** Contains the translation of symbolic destination names
- Server programs do not need a TP Profile data set, but one is required to define ***DBTOKEN***. DBTOKEN is required for RACF protection of the RRSF server.
- APPC/MVS Administration Utility (ATBSDFMU) to create the data sets and to maintain the data.
- Side Information data is not used in this environment.



RACF-RRSF

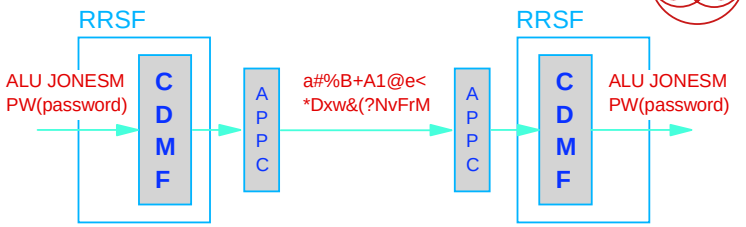
# Implement Security for RRSF-APPC

## RRSF Security Features

- **RRSF protection:**
  - RRSFDATA
  - OPERCMDS
  - DATASET
- **APPC protection:**
  - APPCLU
  - VTAMAPPL
  - APPL
  - APPCPORT
  - APPCTP
  - APPCSERV
- **CDMF**



## RRSF Confidentiality



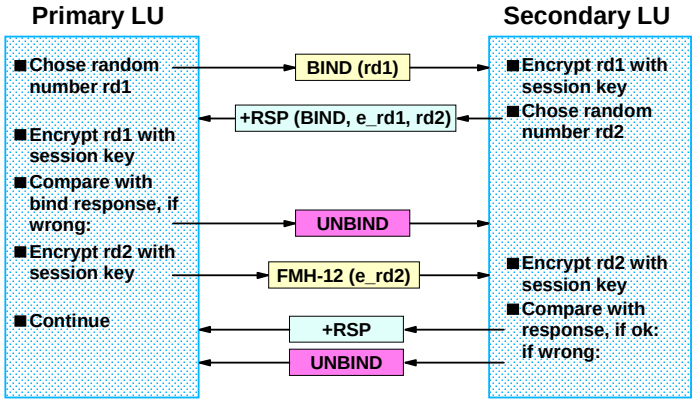

- Protection against inadvertent casual viewing
- CDMF may be freely exported to any customer in most of the countries
- CDMF key has an effective strength of 40 DEA-key bits
- RACF provides the CDMF algorithm and the key

## RACF Classes for APPC/MVS

- **VTAMAPPL** Control use of VTAM ACBs
- **APPCLU** LU 6.2 partner verification, conversation security
- **APPCPORT** Control port-of-entry (remote LU)
- **APPL** Control use of local LUs
- **APPCSERV** Control use of APPC/MVS server TP names
- **APPCTP** Control use and maintenance of TP names
- **APPCSI** Control side information maintenance
- **FACILITY** Control DBTOKEN maintenance
- **PROGRAM** Control execution of APPC/MVS utilities

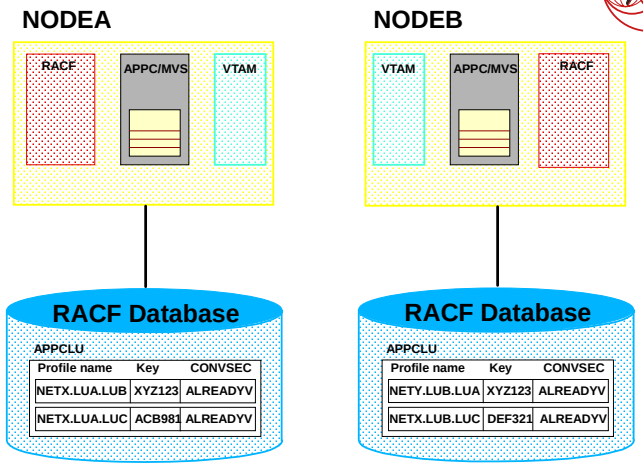


## LU 6.2 Partner Verification






## APPCLU Profiles for RRSF Nodes






## RRSF Application Security

**ALLOCATE** *tpname luname*

SECURITY_TYPE=

- *NONE* (no access security information will be included in the request)
- **SAME** (the same user ID that was used to start the local program plus an ALREADYV indicator are passed on the allocate)
- *PGM* (the source application is responsible for supplying a user ID and password)

## LU Access Authority

VTAM: APPL SECACPT

*(default level of acceptable conversation security)*

- *(NONE)*
- **(CONV)**
- *(ALREADYV)*
- *(PERSISTV)*
- *(AVPV)*

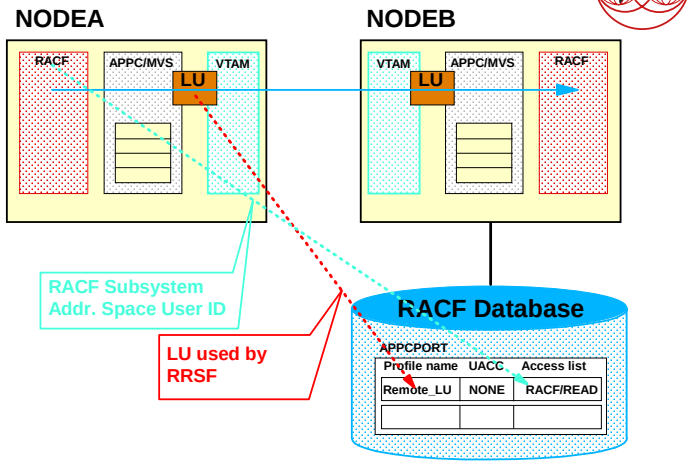
RACF: APPCLU CONVSEC

*(Overrides VTAM APPL SECACPT)*

- *(NONE)*
- *(CONV)*
- **(ALREADYV)**
- *(PERSISTV)*
- *(AVPV)*



## Control Port-of-Entry for RRSF






## Classes VTAMAPPL and APPL

- **VTAMAPPL**

SYS1.VTAMLIST

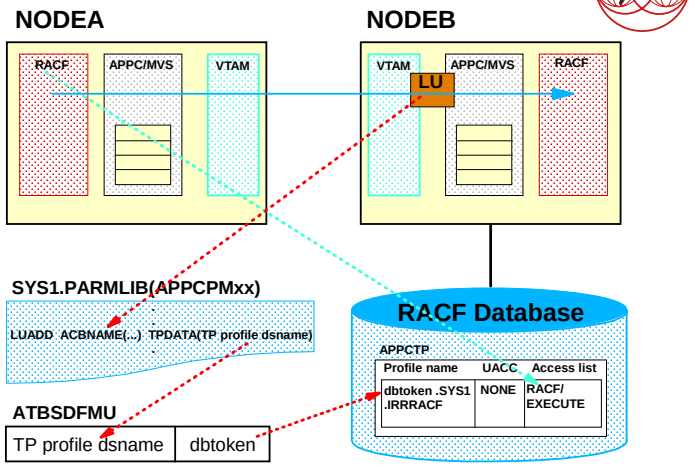
```
.
.
.
RACFRRSF  APPL   ACBNAME=RACFRRSF,
                 APPC=YES,
.
.
.
```

RDEFINE VTAMAPPL RACFRRSF UACC(NONE)

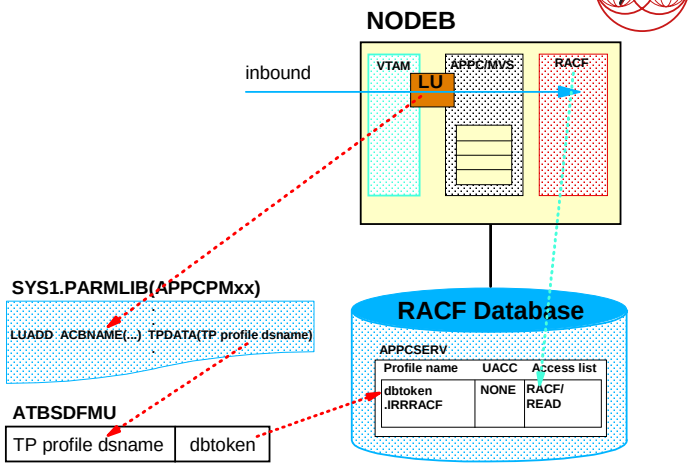
- **APPL**
  - ►There is no need for this level of control for RRSF



## Control Use of RRSF Server



## Control RRSF Server Registration






## Control APPC/MVS Maintenance

RACF Database

FACILITY

| Profile name | UACC | Access list |
|---|---|---|
| APPCMVS.DBTOKEN | NONE | APPCADM / UPDATE |

PROGRAM

| Profile name | Member name | UACC | Access list |
|---|---|---|---|
| ATBSDFMU | 'SYS1.MIGLIB' / volser | NONE | APPCADM / READ |
| ATBSDEPE | 'SYS1.MIGLIB' / volser | NONE | APPCADM / READ |
| ATBINMIG | 'SYS1.MIGLIB' / volser | NONE | APPCADM / READ |



## RRSF Software Requirements

- RACF Version 2 Release 2, or OS/390 Security Server
- MVS/ESA Version 4 Release 3
  - Or a later release
- VTAM Version 3 Release 4 or
  VTAM Version 3 Release 3 with PTF UY59772
  - Required for APPC/MVS support
- TSO/E Version 2 Release 3
  - Or a later release
- ISPF/PDF Version 3 Release 3
  - Or a later release



## Configure VTAM and APPC/MVS

- If only local mode is used, no VTAM or APPC configuration is needed.
- LU must be defined for RRSF with NOSCHED.
  - Do not specify BASE for this LU
- TP profile data set must be specified.
  - Required to define DBTOKEN; TP profiles are not used.
  - Can specify same TP profile data set as for other APPC/MVS scheduler LUs.
- DBTOKEN should be defined.
  - Required for RACF protection of the RRSF server

## Implement Security for APPC

- Use of LU-LU Session Security is highly recommended.
  - Protects against attempts to masquerade as an RRSF system.
  - Requires specification of "VERIFY=REQUIRED" for LUs used by RRSF in SYS1.VTAMLST concatenation.
  - Session key must be installed in APPCLU profiles.
- Specify Conversation Security for RRSF.
  - CONVSEC(ALREADYV) is required.
  - Use discrete profiles in APPCLU class to limit ALREADYV to RRSF sessions.
- Define VTAMAPPL profile to protect VTAM ACB.
- Define APPCSERV profile to control RRSF server registration.

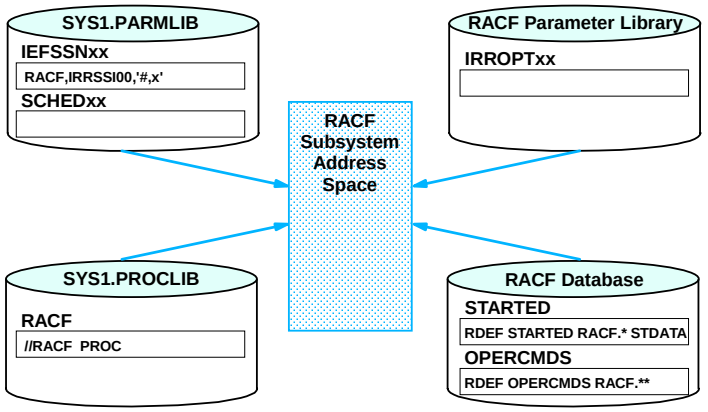


## Implement Security for APPC ...

- Define APPCTP profiles to control who can allocate a transaction for the RRSF server.
- Define APPCPORT profiles to control use of RRSF LU from remote systems.
  - Limit access to RRSF server to defined remote RRSF nodes.
- Define FACILITY profile APPCMVS.DBTOKEN to control the definition of a DBTOKEN.
- Define profiles in PROGRAM class for APPC/MVS utility programs to control the use of utilities.
  - Optionally, define DATASET profiles for TP profile and side information data sets with conditional access lists for PADS.
  - Not required for RRSF.



## Activate RACF Subsystem

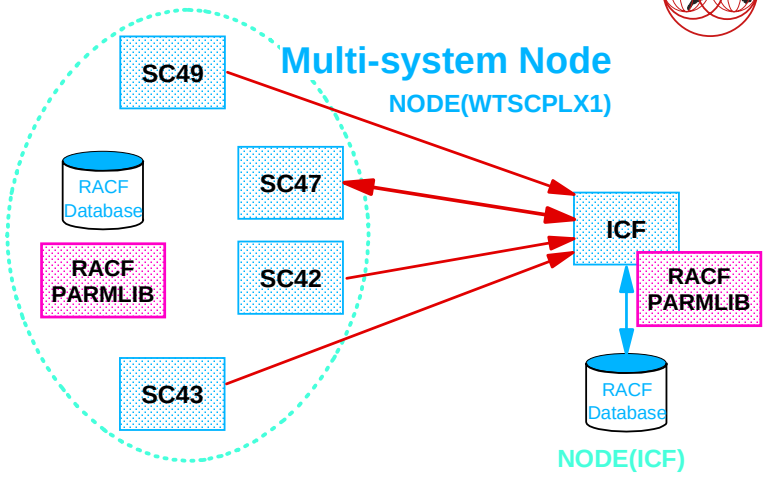





## Define RRSFDATA Profiles

- **RACLINK** *(defining user ID associations)*
  - RDEF RRSFDATA RACLINK.DEFINE.***node*** UACC(READ)
- **AT (***directing commands)*
  - RDEF RRSFDATA RACLINK.DIRECT.***node*** UACC(????)
- **Password Synchronization**
  - RDEF RRSFDATA RACLINK.PWSYNC.***node*** UACC(READ)
  - RDEF RRSFDATA PWSYNC UACC(READ)
- **Automatic Command Direction**
  - RDEF RRSFDATA AUTODIRECT.***node***.class.command UACC(????)
- **Automatic Password Direction**
  - RDEF RRSFDATA AUTODIRECT.***node***.USER.PWSYNC UACC(????)

## APAR OW13567






## APAR OW13567.....

TARGET **NODE**(*nodename*) **SYSNAME**(*sysname*) **MAIN**

Specify name for the entire multisystem node

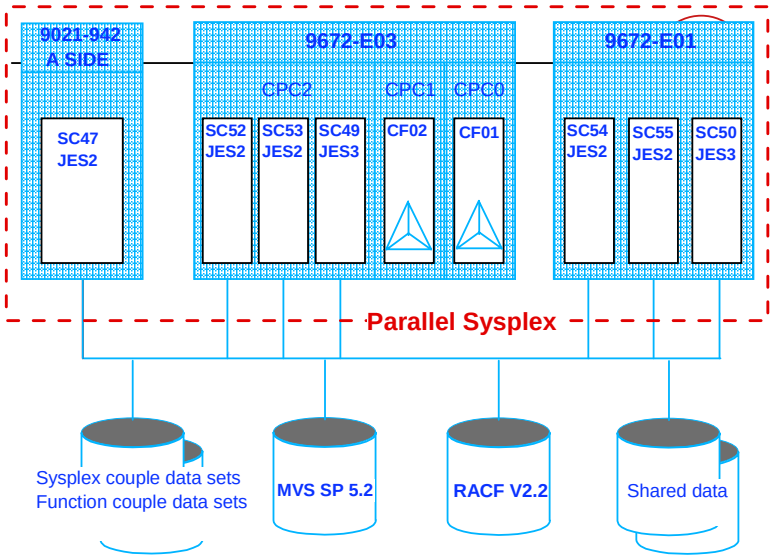
Used with the NODE keyword to identify which system on a multisystem node the commands pertains to

*SYS1.PARMLIB(IEASYMxx)*
*SYS1.PARMLIB(IEASYSxx)*

*On shared PARMLIB in Parallel Sysplex:*

```
TARGET NODE(WTSCPLX1) SYSNAME(SC49) LOCAL
TARGET NODE(WTSCPLX1) SYSNAME(SC47) LOCAL MAIN
TARGET NODE(WTSCPLX1) SYSNAME(SC42) LOCAL
TARGET NODE(WTSCPLX1) SYSNAME(SC43) LOCAL
TARGET NODE(ICF)
```








## MVS 5.2.2 Shared Parmlib Member Support

### Symbolic substitution - Static System Symbols

SYS1.PARMLIB(IEASYMxx)

```
SYSDEF   SYSCLONE(&SYSNAME(3:2))
         SYSPARM(XX)
SYSDEF   HWNAME(ITSO942A)
         LPARNAME(T5)
         SYSNAME(SC47)
```

- IEASYMxx read once during IPL (at NIP time)
- HWNAME is used to specify the HCD processor name
- LPARNAME is used to specify the LPAR partition name
- SYSNAME specifies the name of the processor configuration defined for this SYSDEF statement

## VTAM and APPC/MVS

SYS1.PARMLIB(APPCPMxx)

```
LUADD   ACBNAME(&SYSNAME.RACF)
        NOSCHED
        TPDATA(SYS2.APPCTP)
```

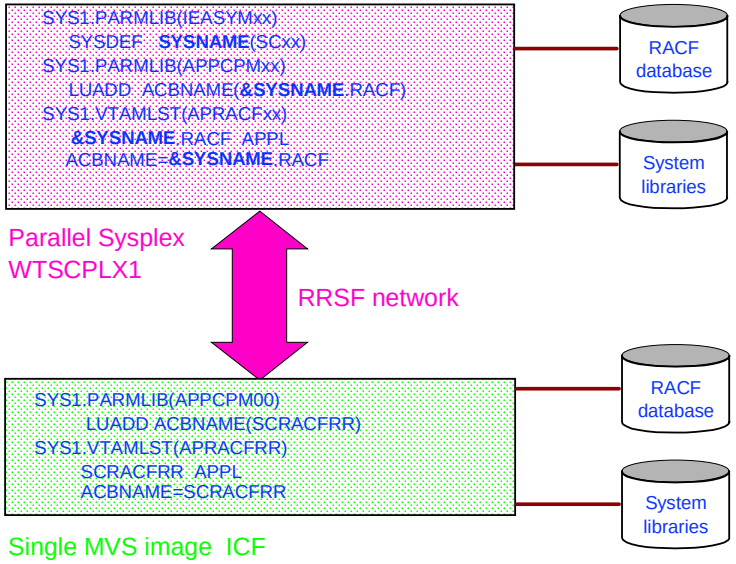
APPC/MVS local LU definition

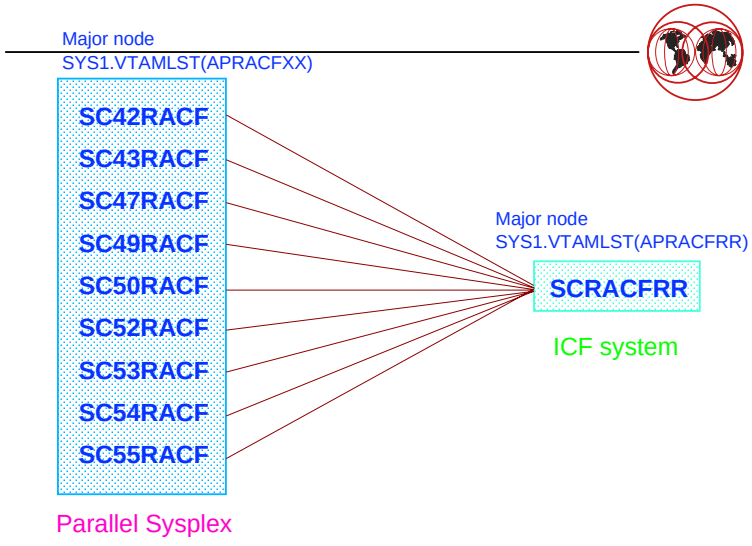
SYS1.VTAMLST(APRACFxx)

```
        VBUILD TYPE=APPL
&SYSNAME.RACF  APPL  ACBNAME=&SYSNAME.RACF
        APPC=YES
        ..............
```

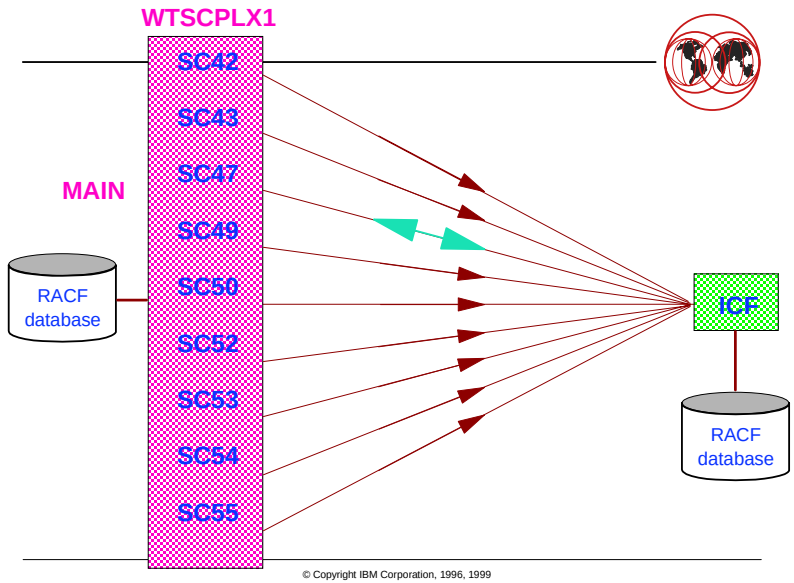
Define APPC/MVS local LU to VTAM







## PARMLIB Definitions with OW13567

```
TARGET NODE(WTSCPLX1) SYSNAME(SC47) LOCAL MAIN PROTOCOL(APPC(LUNAME(SC47RACF)....
TARGET NODE(WTSCPLX1) SYSNAME(SC42) LOCAL PROTOCOL(APPC(LUNAME(SC42RACF)....
TARGET NODE(WTSCPLX1) SYSNAME(SC43) LOCAL PROTOCOL(APPC(LUNAME(SC43RACF)....
TARGET NODE(WTSCPLX1) SYSNAME(SC49) LOCAL PROTOCOL(APPC(LUNAME(SC49RACF)....
TARGET NODE(ICF) PROTOCOL(APPC(LUNAME(SCRACFRR)....
```

Shared parmlib in Parallel Sysplex

```
TARGET NODE(ICF) LOCAL PROTOCOL(APPC(LUNAME(SCRACFRR)....
TARGET NODE(WTSCPLX1) SYSNAME(SC47) MAIN PROTOCOL(APPC(LUNAME(SC47RACF)...
TARGET NODE(WTSCPLX1) SYSNAME(SC42) PROTOCOL(APPC(LUNAME(SC42RACF)....
TARGET NODE(WTSCPLX1) SYSNAME(SC43) PROTOCOL(APPC(LUNAME(SC43RACF)....
TARGET NODE(WTSCPLX1) SYSNAME(SC49) PROTOCOL(APPC(LUNAME(SC49RACF)....
```

Parmlib on the single MVS image



## Command Direction & PWSYNC

```
RDEFINE RACLINK.DEFINE.ICF UACC(READ)
RDEFINE RACLINK.PWSYNC.ICF UACC(READ)
RDEFINE PWSYNC UACC(READ)
```

**On one of the members of the Parallel Sysplex**

```
RDEFINE RACLINK.DEFINE.WTSCPLX1 UACC(READ)
RDEFINE RACLINK.PWSYNC.WTSCPLX1 UACC(READ)
RDEFINE PWSYNC UACC(READ)
```

**On the single MVS image**

```
RACLINK ID(ROBBYM) DEFINE(WTSCPLX1.KINGMA)
   PEER(PWSYNC)
```

**On the single MVS image**



## ACD & APD with APAR OW13567

```
RDEFINE RRSFDATA AUTODIRECT.WTSCPLX1.USER.* UACC(READ)
RDEFINE RRSFDATA AUTODIRECT.WTSCPLX1.GROUP.* UACC(READ)

RDEFINE RRSFDATA AUTODIRECT.WTSCPLX1.USER.PWSYNC UACC(READ)
```

**On the single MVS image**

```
RDEFINE RRSFDATA AUTODIRECT.ICF.USER.* UACC(READ)
RDEFINE RRSFDATA AUTODIRECT.ICF.GROUP.* UACC(READ)

RDEFINE RRSFDATA AUTODIRECT.ICF.USER.PWSYNC UACC(READ)
```

**On one of the members of the Parallel Sysplex**