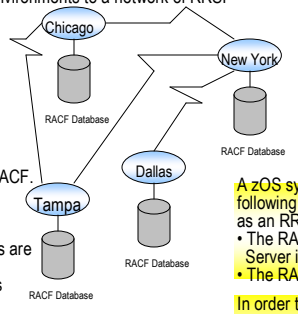
Overview of the RACF remote sharing facility (RRSF)

• The RACF remote sharing facility (RRSF) exploits the networking services provided by APPC/MVS and TCP/IP to extend RACF functionality beyond the single host and shared DASD environments to a network of RRSF nodes capable of communicating with each other.
- Using the function provided by RRSF, it is possible to administer RACF databases distributed throughout an enterprise from any location in the enterprise.



Understanding the RRSF concepts

• RRSF nodes and the RRSF network
- The RACF remote sharing facility is built on the concept of a network of RRSF nodes.
- An RRSF node is a zOS system image, or several zOS system images sharing a RACF database, that has been defined as an RRSF node to RACF.
- Before you can use the functions provided by RRSF, you must configure your zOS system images into a network of RRSF nodes.

The RRSFDATA class

• Profiles in the RRSFDATA class determine which remote sharing functions are available on a node, and which users have access to them.
- The RRSFDATA class must be active in order for the functions it protects to be available

User ID associations

• Some RRSF functions require a previously established user ID association.
- A *user ID association* is an association between two user IDs, on the same or different RRSF nodes, that is defined to RACF using the RACLINK command.
- Typically user ID associations are established between user IDs used by the same person.

• There are two types of user ID association: peer and managed:
- A *peer association* allows either of the associated user IDs to direct commands to the other and allows the associated user IDs to synchronize their passwords and password phrases
- In a *managed association*, one of the user IDs is designated as the *managing* ID, and the other is designated as the *managed* ID.
  NOTE: The managing user ID can direct commands to the managed ID, but the managed ID cannot direct commands to the managing ID. The user IDs in a managed association cannot synchronize their passwords.
- Profiles in the RRSFDATA class control whether user ID associations can be defined, to which nodes they can be defined, and which users can define them.

The RRSFDATA class determine which remote sharing functions are available on a node, and which users have access to them.
NOTE: The RRSFDATA class must be *active* in order for the functions it protects to be available.

RRSF nodes

• An RRSF node is a zOS system image, or a group of zOS system images sharing a RACF database, that has been defined as an RRSF node to RACF by a TARGET command.

A zOS system image must meet the following requirements to be defined as an RRSF node:
• The RACF component of the z/OS Security Server is enabled.
• The RACF subsystem address space is active.

NOTE: In order to direct commands or application updates from one MVS system image to another, or synchronize passwords between two MVS system images, both of the system images must first be defined to RACF as RRSF nodes that can communicate with each other.

Local and remote RRSF nodes

• The terms local and remote can be useful when discussing RRSF nodes.
- The *local* node is the node whose viewpoint you are speaking from.
- Its *remote* nodes are the other nodes in the network with which it communicates.
  For example, in the network shown above, from the Chicago node's point of view, the Chicago node is the local node and the Tampa and New York nodes are remote nodes. The Chicago node cannot communicate with the Dallas node. From the New York node's point of view, the New York node is the local node and the Chicago, Tampa, and Dallas nodes are remote nodes. From the Tampa node's point of view, the Tampa node is the local node and the Chicago and New York nodes are remote nodes. The Tampa node cannot communicate with the Dallas node. From the Dallas node's point of view, the Dallas node is the local node and the New York node is a remote node. The Dallas node cannot communicate with the Tampa and Chicago nodes.

• RACF creates a ***listener*** process on the local node for each protocol that the node uses.
- The listener process listens for incoming connection requests from remote nodes.
- The local node cannot establish new remote connections for a protocol unless its listener for the protocol is active.
- The listener for a protocol can be in one of the following states:
  active The listener has been established and is listening for connection requests from remote nodes. New connections can be established with remote nodes.
  inactive The listener is not currently available. This state can occur when the local node has been made dormant, or, for the TCP/IP listener, if there is a problem with z/OS UNIX. Remote connections that are already active remain active and continue to communicate, but new connections cannot be established. To make the listener active, issue a TARGET OPERATIVE command or a RESTART CONNECTION command for the local node.
  initializing The listener is attempting to start, but has not been able to start successfully. The listener will retry periodically until it starts successfully or the local node is made dormant. If the listener cannot start within a time period of approximately 30 minutes, it stops retrying and goes into inactive state. The initializing state can occur when there is a problem with TCP/IP, or if a host name was specified for the local node and the domain name server (DNS) is not responding for host name resolution, or if an incorrect host name or IP address was specified. Remote connections that are already active remain active and continue to communicate, but new connections cannot be established.

RRSF provides the following functions:

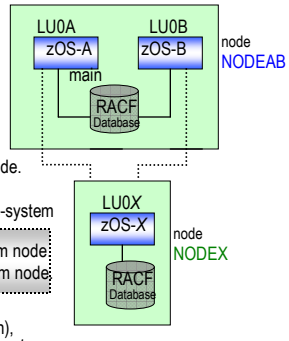
• **Command direction**
A user logged on to one user ID can issue a RACF command and *direct* that command to run under the authority of the same or another user ID on the same or another RRSF node.
- A user directs a command by using the AT keyword on the command to specify the RRSF node & user ID the command is to be directed to.
-The command runs asynchronously in the RACF Subsystem address space, and the output is returned to the issuing user's RRSFLIST dataset.
-Before a user can direct a command to run under another user ID, a user ID association must be established between the two user IDs.
NOTE: Profiles in the RRSFDATA class control to which nodes command direction is allowed, And which users can direct commands.

• **Password synchronization**
- If password synchronization is enabled between two user IDs, when the password or password phrase is changed for one of the user IDs, RACF automatically changes the password or password phrase for the other.
-Password synchronization is enabled between two user IDs by creating a peer user ID association between the two IDs that specifies password synchronization.
-Profiles in the RRSFDATA class control who can define user ID associations with password synchronization enabled, whether password synchronization occurs on an RRSF node, and for which users.
NOTE: The SETcommand activates and deactivates password synchronization.

• **Automatic direction**
Automatic direction allows you to have RACF automatically direct updates made to the RACF database on an RRSF node to one or more other RRSF nodes.
-If profiles on two or more RRSF nodes are already synchronized, you can use automatic direction to have RACF automatically keep the profiles synchronized.
NOTE: Automatic direction does not require user ID associations. Instead, automatic direction assumes that if the same user ID exists on two different nodes, those user IDs belong to the same person. RACF provides the following types of automatic direction:
Automatic command direction. Profiles in the RRSFDATA class control which commands are automatically directed, and to which nodes.
Automatic password direction. Profiles in the RRSFDATA class control for which users pass word and password phrase changes are automatically directed, and to which nodes.
Automatic direction of application updates. Profiles in the RRSFDATA class control which application updates are automatically directed to which nodes.
The SET command activates and deactivates automatic direction.

Single-system nodes and multisystem nodes

• An RRSF node can be either a single-system node or a multisystem node.
- A *single-system RRSF node* consists of only one z/OS system image.
- A *multisystem RRSF node* consists of multiple z/OS system images that share a RACF database.
- For a multisystem RRSF node, you designate one of the z/OS system images to be the *main system*.
  > The main system receives most of the RRSF communications sent to the node.
  > The other systems in the node are known as *nonmain systems*.
  NOTE: This illustration on right shows an RRSF network containing a single-system node and a multisystem node.



NODEAB is a multisystem node
NODEX is a single system node

• **Main** systems in a multisystem RRSF node can send RRSF requests to main systems on remote multisystem RRSF nodes, and to single-system RRSF nodes.
- When main systems receive requests from remote systems (main or nonmain), they send output and notifications back to the system that originated the request.

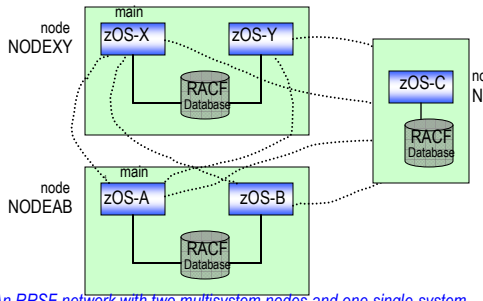
• **Nonmain** systems in a multisystem RRSF node can send RRSF requests to main systems on remote multisystem RRSF nodes, and to single-system RRSF nodes.
- They cannot send RRSF requests to other remote nonmain systems, or to other local systems (nonmain or main).

• Most RRSF communications sent to the multisystem RRSF node are received by the main system, including:
- All commands directed to the multisystem node
- All RACLINK requests sent to the multisystem node
- All password and password phrase changes sent to the multisystem node
- All output and notifications from automatically directed commands and application updates.

• The following types of RRSF communications can be received by any system in a multisystem node:
- Output and notifications from commands that were directed by way of the AT or ONLYAT keywords
  > These are returned to the system on which the directed command was issued.
- Notifications from RACLINK commands.
  > These are returned to the system on which the RACLINK command was issued.
- Output from password and password phrase changes when automatic password direction is used.
  > These are returned to the system on which the password or password phrase was changed.

Two RRSF nodes are said to be *logically connected* when they are configured to communicate by way of APPC/MVS or TCP /IP, their RACF subsystem address spaces are active, and they have been defined to RACF as RRSF nodes that can communicate ith each other.
At a high level, there are two types of connections between nodes: operative and dormant.

• The display below shows an RRSF network containing two multisystem nodes, NODEXY and NODEAB, and one single-system RRSF node, NODEC.
- Multisystem node NODEXY contains two systems, zOS-X and zOS-Y.
- Multisystem node NODEAB contains two systems, zOS-A and zOS-B.



On NODEAB, from the perspective of system zOS-B:
• NODEAB is the *local RRSF node*.
• zOS-A and zOS-B are the *member systems* of node NODEAB.
• zOS-B is the *local system*.
• zOS-A is a *local peer system*.
•zOS-A is the *local main system*.
• NODEXY and NODEC are *remote RRSF nodes*.
• zOS-X is a *remote main system*.
• zOS-Y is a *remote nonmain system*.

An RRSF network with two multisystem nodes and one single-system

Local and remote modes of operation

• An RRSF node can operate in either local mode or remote mode.
- When an RRSF node operates in *local mode*, it is not configured to communicate with other RRSF nodes.
  > A node operating in local mode provides limited remote sharing functions:
  >> Users with multiple user IDs on the node can synchronize passwords and password phrase between those user IDs.
  >> Users with multiple user IDs on the node can direct commands to run under the other user IDs.
  >> Users can direct commands to run in the RACF subsystem on the local node.

• When an RRSF node operates in *remote mode*, it is configured to communicate with other RRSF nodes.
- A node operating in remote mode provides the full power of the RACF remote sharing facility to perform RACF functions across a network.
- If you define a node to communicate with another node using the APPC/MVS protocol, both the local mode functions and the remote mode functions must initialize successfully before the connection can enter the operative active state.
- An error in initializing the local mode functions (for example, a VSAM error on the local nodes's workspace data sets) prevents remote connections from being established.
  NOTE: An error in initializing the remote mode functions (for example, an APPC server initialization failure) prevents local mode functions from being performed.
- If you define a node to communicate with another node using the TCP/IP protocol, an error in initializing the local mode functions (for example, a VSAM error on the local nodes's workspace data sets) prevents remote connections from being established.