ABS Tech Note: SNA•ps14 APPC Security (2/93)

Article Created: 26 February 1993

TOPIC ----------

LU 6.2 provides a powerful transaction processing facility . Along with this power comes the responsibility for verifying access to network resources (that is LUs, TPs). This technical note describes two functions SNA•ps provides to assist the administrator in providing APPC security, namely: LU-LU verification and end user verification.

DISCUSSION ----------

Introduction

SNA•ps provides several levels of security for APPC users. LU-LU verification is a session-level security protocol, invoked at the time the session is activated. End-user verification is a conversation-level security protocol, taking place at the time a conversation between two TPs is started. This technical note describes the procedure for configuring and using these security features.

Note: it is only necessary to configure for end user verification when LU 6.2 applications are being remotely started at the Macintosh (that is the SNA•ps gateway is receiving attaches, that is FMH–5's).

LU-LU Verification

Partner-LU verification is accomplished during session establishment, with each LU using an LU-LU password and the Data Encryption Standard (DES) algorithm. LU-LU passwords are defined on a partner -LU basis: one LU-LU password is established between each LU pair and used for all sessions involving the pair.

To configure SNA•ps to use LU-LU verification, use SNA•ps Config to edit the remote LU resource. Enter the session password parameter matching the partner LU's password. If the passwords match exactly, the session is established; if not, then no session is enabled.

Note: LU-LU passwords are established by installation and implementation-defined methods outside of SNA. Example: for the AS/400 set the LOCPWD parameter associated with the AS/400 device description.

End User Verification

Partner end user (for example, transaction program) verification is a conversation-level security protocol used to control access to remote TP applications. When a TP wishes to access another TP, it must supply adequate security information in the allocate conversation request to satisfy the requirements at the remote LU, or the request will be rejected. A user ID, password, and profile may be specified in the allocate request that will cause the receiving LU to check an authorization list before a specific TP is started. Each LU indicates at session activation time whether it will accept LU security parameters on allocation requests the partner LU sends.

It is only necessary to configure SNA•ps for end user verification when LU 6.2 applications are being started at the Macintosh (that is the Macintosh TP is receiving attaches (that is FMH-5's).

To configure SNA•ps for end user verification, use SNA•ps Config to set up user IDs and profiles for a local LU. Next assign user IDs and profiles from the associated local LU to the specified transaction programs. This is done after selecting the TP security level you wish to use. Specifying conversation level security indicates that the userid, password and profile in the allocate request will be checked, but that no TP access verification is to be performed. If one of the Access level security selections are made, this specifies that resource-level security will be validated using the authorization list specified for the TP. Next, use SNA•ps Config to edit the remote LU resource so that conversation security is selected. The pre-verified selection indicates that the local LU will accept conversation-level security without requiring a password Therefore, pre-verified should only be used if the sender is trusted by the receiver to have performed the proper verification of the user ID.

Note: the APPC protocol does not encrypt end-user passwords.

Keywords: <None>

==========

This information is from the Apple Technical Information Library.

19960215 11:05:19.00
Tech Info Library Article Number: 11738