

access into the LAN by means of physically servicing only the physical layer interfaces which are providing connectivity to authorized end systems (PCs, servers, etc.). All other non-used physical layer interfaces are not connected back to the centralized LAN equipment.

- d. Furthermore, the planned local subnetwork architecture (i.e., physical, data link, and network layers) enables the implementation of LAN equipments employing special security related mechanisms. For example, there are commercially available 10BaseT hub products which overwrite the data field of all packets not destined for the end system connected to a particular port.³

6.2.2 Wide Area Subnetwork

- a. In general, the wide area subnetwork connectivity will utilize the services of MITNet. All information transmitted across the wide area subnetwork normally undergoes encryption/decryption using government approved encryption devices on MITNET. MITNET is currently evaluating bulk encryption technologies which will reduce the general requirement for encryption on a per input circuit basis.
- b. A decision has been made to not use KG encryption devices for SIGNET input circuits.
- c. No additional security related requirements are assigned to the wide area subnetwork.

6.2.3 Internetwork Elements Security

- a. All network elements deployed into SIGNET must employ adequate access security to allow access to device configuration and monitoring to authorized personnel only. Authorized personnel should be limited to the organizations responsible for the operations and maintenance of the SIGNET internetwork.

6.2.4 Access External to the SIGNET Local/Wide Subnetworks

- a. Access external to the SIGNET local/wide area subnetworks may be provisioned in at least three forms:
 - 1) Point-to-point connections, either dedicated or switched and through the public telephone network (eg. Bell Canada network), between External Affairs devices and devices operated by other departments or service corporations. For example, connections between External Affairs and Employment and Immigration for exchanging CAIPs related information; service contracts with SHL Systemhouse for FINEX; and an X.400 MTA - MTA gateway between SIGNET and the GTA e-mail services.

³Such a capability is not a requirement for the concentrators in the Network Element RFP.