



## Temporary Local Area Networks (TempLANs)

Temporary Local Area Networks (TempLANs) are a collaborative effort with the Navy (Fleets, TYCOMs, and NAVSEA) providing a temporary off ship tagout and Consolidated Afloat Network Enterprise Server (CANES) network for when a ship is no longer habitable during their maintenance availability. These TempLANs allow Ship's Force to continue their required day-to-day work as well as support the maintenance availability. Most of the time, these networks are located on the berthing barge but can be setup in other temporary quarters (trailers or building) when a barge is not available. Approximately 100 ships undergo Local Area Network (LAN) migrations annually and require the transfer of 2,000 Terabytes ( $2 \times 10^{15}$ ) worth of data.

TempLANs have historically been executed by removing shipboard ISNS equipment and relocating it to a barge or other temporary structure. This method executes easily, requires very little system specific knowledge, and results in minimal network down time. However, with the introduction of CANES and its Virtual Machines (VMs), this method is no longer feasible. Since removing the equipment is no longer a viable option, data and their corresponding VMs must be planned and migrated to an extension of that ship's network. By assigning Commander, Naval Regional Maintenance Command (CNRMC) the responsibility to manage TempLANs, this allows consolidation and standardization of these TempLANs to better support the Fleet's operational requirements during maintenance availabilities. TempLANs also help overcome certain geographic network availability issues (remote locations, DoD vs host country rules) plus other situations such as lack of secure facilities and non-use of berthing barge. TempLANs ensure the necessary network services are delivered consistently and uniformly across all platforms. Interoperability requirements along with essential information assurance / cybersecurity requirements are additionally provided to effectively and efficiently support Ship's Force and maintenance personnel.

With CANES fielding and the inability to remove network equipment from the ship for remote use, Fleet Commanders must now procure, install, and support CANES compatible equipment on berthing barges or other identified support facilities (CONEX box, trailer, etc.). This TempLAN equipment needs to be maintained to include modernization upgrades, physical security, cybersecurity requirements (management controls, operational controls, technical controls), equipment storage, inventory control, and help desk support.

Before a ship network can be migrated to a TempLAN, networks (both SIPR and NIPR) must be tested and configured to support ship specific software and hardware configurations. A Pre-Installation Check-Out (PICO) is performed with the ship to verify functionality and data integrity of the ship's LAN prior to data migration to their TempLAN. The PICO also identifies the VMs it wants migrated to their TempLAN. A comprehensive tagout audit is completed to ensure no tagouts are lost during the transition to and from the ship. At the conclusion of the migration back to the ship, verification and acceptance testing is performed to ensure proper operation of all VMs. A Standard Operating Procedure (SOP) provides the training and additional details of TempLANs. In addition, while in the availability, weekly wellness checks are coordinated to further ensure sustained performance.

