Network migration

Merging, renumbering, and migrating networks has traditionally been largely a cumbersome manual process. The Network Controller automates many of these changes via its real-time inventory and reporting modules. The result is lowered cost and risk.

Companies buy, sell, and merge with others as part of normal business operation. Each change in the corporate structure has a corresponding change in the network topology[1]. Changes to the topology have high risk and cost due to the need for "live" migration of the network.

The Mancala Network Controller assists with this process through its features which implement inventory, migration, and audit.

> Inventory

The first step of any migration is an inventory that is up to date and lists all of the devices on the network. The inventory should record as much information as possible about each device, including MAC address, IP address, host name, device type, OS type, etc. This data will be used as the basis for all future work, so it should be as accurate and comprehensive as possible.

The Network Controller can record all of this information without affecting the functionality of the existing network. It will automatically detect networks, servers, laptops, virtual machines, smart phones, VoIP phones, printers, and classifies them by network location, switch port, and operating system.

The Network Controller can then be used to produce reports of devices and network architecture which form the basis for migration planning and risk assessment.

[1] http://www.ietf.org/rfc/rfc2071.txt

> Plan

The next step is to plan the actual migration. The migration should be split into multiple phases, where each phase starts and ends with a functional network. Each phase can be further split into portions which migrate one device, or one class of devices. This partitioning ensures that the risk of any one change is known, quantified, and acceptable.

Where the networks have conflicting address ranges, one phase may include migration to an intermediate and temporary set of addresses. Similar intermediate steps may include the deployment of temporary staging servers on the intermediary network.

This plan should use the inventory information to classify devices into multiple categories. Each category of devices should be migrated separately to ensure network continuity. The plan should include the action items which constitute each step, the prerequisites for each action item, the expected time frame, and the expected outcome.

The plan should also include user operational requirements, which classify devices into categories such as "required", or "low priority". Different stakeholders should be identified, so that they can contribute to the plan, and be informed as to its progress.

The Network Controller can provision networks during the planning stages before they are

needed. This capability allows more portions of the migration to run in parallel.

> Migration

The devices should be migrated gradually, starting with the lowest risk items. Lessons learned during that migration will help reduce the risk of migrating more critical systems.

The Network Controller will perform dynamic address reassignment for protocols such as DNS and DHCP. This feature allows the servers to exist in the "old" network without any change to their configuration. At the same time, the devices are migrated to the "new" network. Dynamic address reassignment allows devices in the "new" network to access services in the "old" network.

Dynamic address reassignment is a feature where the Network Controller acts as a transparent re-writing proxy on the new network. It offers a service such as DHCP to the new network, but forwards the traffic to the existing DHCP server in the old network. Required fields of the protocol are re-written on packet reception and transmission, to ensure consistent behavior on both networks.

The migration process can be monitored in real time, and any anomalous events flagged for immediate correction. The event notification system will notify the migration administrator if a particular device has not been migrated within the expected time frame.

> Audit

The inventory system can then be used to audit the devices which have been migrated, in real time as the migration is proceeding. Any of the devices which have not followed the migration process can be flagged, and fixed at this time.

When a particular class of devices has been migrated, the next step of the migration process can begin. At the same time, the global inventory and policy system monitors the network to ensure that previously migrated devices do not re-appear in the "old" network.

Once the audit shows that no devices exist in the "old" network, the current step of the migration process is complete. A new and updated report is generated which provides the basis for planning the next stage of the migration.

> Summary

The Network Controller integrates inventory, migration, reporting, and services into one common platform. This global integration gives it capabilities which are unmatched in any other product. The capabilities have a direct impact on lowering the time, cost and risk associated with network migration.

> About

Mancala Networks has made our corporate tag line *making networks manageable* for a simple reason: it is the guiding principle behind everything we do.

We believe that businesses should be able to manage their network as a network, rather than as a collection of individual systems and services.

We have made it possible today with the Mancala Network Controller - a consolidated platform providing Network Migration, services, IP address management, Intrusion Detection, Network Access Control, Inventory, monitoring and Guest Access services among others.