Rebuilding the Core Network Infrastructure

Title: Enterprise IT Management Initiatives

State: Maine

Contact: Jon Richard, Network Services Director

Project Dates: January 2015 to December 2016

Executive Summary

The State of Maine's legacy data network dated from the late 1990's when the uptime, security and throughput requirements were far less demanding. Budget constraints of the last decade left the antiquated core of the network, (the devices that switched and routed all the State data, voice and video traffic), in place for more than 15 years, many years longer than the expected useful life.

In 2015, the State of Maine began the overhaul of this legacy network and over a 23-month period, three non-redundant legacy switch/routers were replaced by 14 more specialized, redundant network devices. The most significant impacts of this project included:

- Assuring that the citizens of the state would not experience an extended outage of State government services due to a failure of the deteriorating IT network infrastructure.
- Improving off-hours system availability to programmers and operations personnel by eliminating the need to take portions of the network down for periodic servicing of network devices, thus improving the speed of application development and testing and the efficiency of nightly operations.
- Conducting a successful two-way communications campaign with State agencies to earn their trust and cooperation with several day-long outages needed to implement the new core network.
- Applying best-practice project management principles that resulted in highly organized outages that typically finished in less time than predicted.

This core network upgrade represents a giant leap forward for the State of Maine that required:

- The strong backing of OIT senior leadership;
- The commitment of precious financial resources and;
- A determined effort by a small, dedicated team of IT professionals.

Goals

Security

Scalability

Availability

Manageability

Concept

Background

Maine is a geographically large, rural, state of 1.3M citizens, like many other states with limited funds and opportunities to keep pace. Thus, Maine's Office of Information Technology (OIT) is regularly challenged to do more with less, and the staff takes pride in what it continues to accomplish within tight financial constraints.

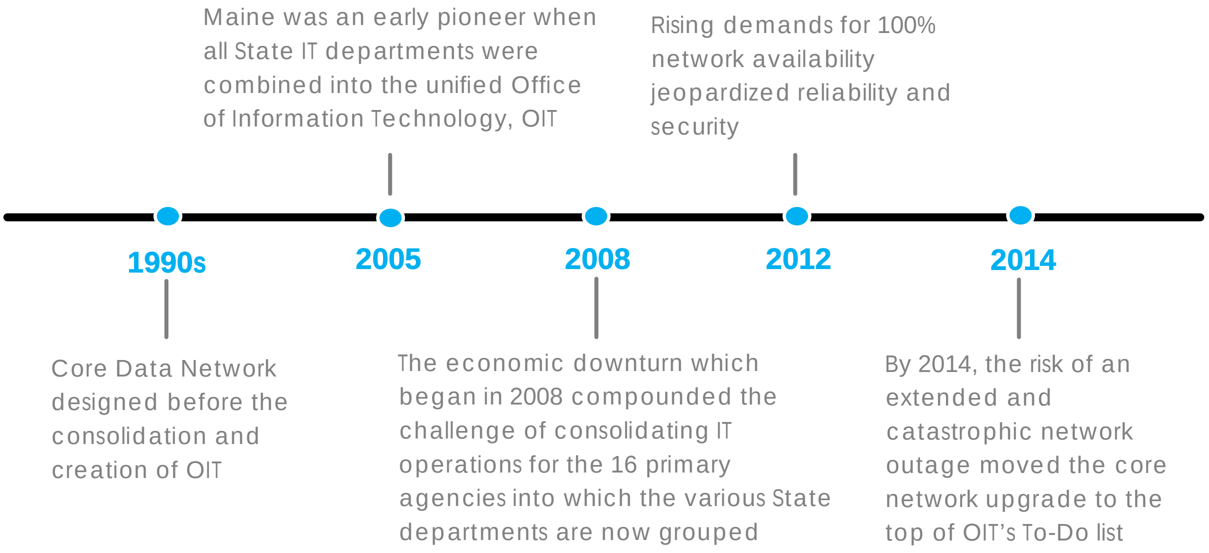
Tight budgets meant making difficult decisions regarding which projects to fund and which to defer, and modernizing the data network simply was not as high of a priority as other critical initiatives during these lean years.

The core of the data network had been designed in 1990's before the consolidation and creation of OIT and for a very different computing era. Three non-redundant Nortel 8600 data switches/routers provided connections to everything:

- 13,000 desktop devices;
- All resources at the primary and back up data centers; and
- The Wide Area Network connecting to 450 remote sites and the Internet and other foreign network connections.

While this design was cost-effective and appropriate in its day, the failure of any one of these devices would have had catastrophic consequences for State government.

As time passed, the risks increased. Due to rising demands for 100% network availability from agencies with public web portals and from Application Development teams, Network Services was finding it more difficult to schedule regular maintenance windows for the basic patching of these devices. Both the reliability and security of the network were now in jeopardy … and it was only 2012!



1990s

Core Data Network designed before the consolidation and creation of OIT

2005

Maine was an early pioneer when all State IT departments were combined into the unified Office of Information Technology, OIT

2008

The economic downturn which began in 2008 compounded the challenge of consolidating IT operations for the 16 primary agencies into which the various State departments are now grouped

2012

Rising demands for 100% network availability jeopardized reliability and security

2014

By 2014, the risk of an extended and catastrophic network outage moved the core network upgrade to the top of OIT's To-Do list

Time for Action

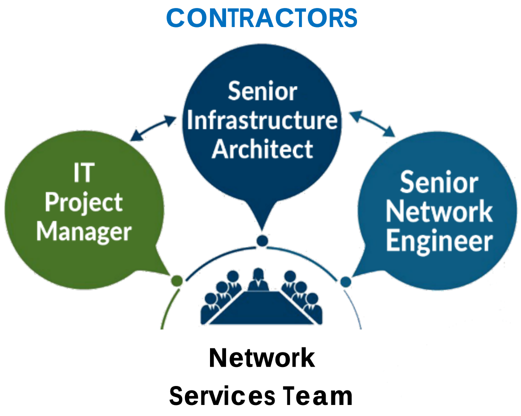
By 2014, the risk of an extended and catastrophic network outage moved the core network upgrade to the top of OIT's To-Do list. The consulting firm NTT DATA was engaged to produce a new core network design which they based around state-of-the-art Cisco network architecture and hardware. In this new design, the three core network devices were replaced by 14 devices that provided redundancy and device specialization.

Once the installation was accomplished, a new era would begin for Network Services wherein:

- The failure of any single device would not impact network availability.
- Any device could be taken off-line at any time for servicing without impacting network availability.
- Access to the Internet and non-State networks could be accommodated in a manner that incorporated much-needed security mechanisms.
- With the addition of new network monitoring tools and a properly equipped test lab, OIT could move from a reactive to a proactive posture in managing the network.

The Team

Due to the existing workload facing the small Network Services staff, OIT engaged three outside contractors to assist with this effort. The addition of these individuals was critical to the success of the project which was equated to change a tire on a moving car. With the contractors solely focused on project success, the Network Services team members could "keep the lights on" and provide critical input on the current network environment to the project team.



OIT engaged three outside contractors to assist with this effort

Technical Preparation

Success depended heavily on documenting in fine detail every aspect of the network. Over the years, network documentation had not been kept current so every aspect of the current network functionality had to be revisited, vetted and documented in Visio and other formats. A highly experienced Cisco engineer was assigned to this task for months to prepare the way for a successful deployment.

Project Management

Network changes of this magnitude involved not only the Network Services team but all of OIT. Application development team were consulted extensively to understand how changes to the network would affect application performance. IT Security was consulted to discuss how the modern environment should be configured to meet evolving security policies. Likewise, the Storage and Server groups were consulted for their input and concerns. As the finer details of design and configuration were finalized, dates were set for the four-stage implementation of the 14 new devices. Each day-long outage would require a detailed "play-book" that documented step by step what the engineers would do hour by hour through the day, and how the team would back-out of the implementation if a major roadblock was encountered.

Agency Outreach

A minimum of 3 day-long network outages were going to be necessary to move traffic off the legacy platform onto the new platform. What would the State Police do without access to their data networks? How would the State hospitals operate without access to their electronic health records and pharmacy system? How would the Department of Labor clients cope without its online unemployment filing systems? Fishing licenses, campground reservations, vehicle registrations, application testing, electronic funds transfers – the list was long.

Starting early, the project team held open meetings with large groups as well as with specific agencies to hear their concerns and develop the best possible plans to accommodate them.

Thus, when the actual day-long outages occurred, agencies were well-prepared and took advantage of the opportunity to test their internal Business Continuity/Disaster Recovery plans. On the day of each outage, audio bridges were kept open all day long to field questions and concerns from agency personnel and an externally-hosted website provided status updates. OIT overall earned significant positive recognition from agencies as a result.

Network Monitoring/Lab

As the new core network equipment was being installed, the team implemented a new test lab that proved to be essential in testing the planned network changes prior to actual implementation. Many pitfalls were avoided through this testing process. After the cutovers, new network monitoring tools were implemented that dramatically enhanced the ability of the network team to monitor network health and identify issues before they occur.

Costs

One-time direct costs for these upgrades exceeded $5M with an increase of more than $1M in operating expenses.

Significance:

The significance of the successful implementation of the State of Maine core network upgrade cannot be overstated. As the **most** foundational component of the State's IT infrastructure, 100% of the State's business relies on this network core in one way or another.

Goals

Five outcomes comprised the goals of the core network upgrade project:

Reliability:	99.999% (less than six minutes/year) reliability with no single points of failure at the core.
Availability:	100% availability – no maintenance activities should render the network unavailable to any part of state government or OIT at any time.
Security:	The new core must provide a foundation for state-of-the-art security mechanism such as encryption and network segregation that the State needed to implement in the future.
Scalability:	The new core could accommodate all increases in utilization generated by existing applications and new uses including video, cloud and Internet of Things (IoT).
Manageability:	Through network components, monitoring tools and the test lab, the OIT network team can identify nascent problems and remediate them before they became service-affecting, allowing the team to make the shift from being reactive (break/fix) to proactive/predictive in its approach to network management.

Larger Policy and Strategy Goals

This core network upgrade aligns with many State, Federal and NASCIO goals including:

- The State's "Cloud First" strategy;
- State and federal regulatory agency mandates regarding security;
- Agency needs for greater availability and scalability; and
- Six of NASCIO's Top Ten 2017 State CIO priorities (Security and Risk Management; Consolidation/Optimization; Cloud Services: Budget, Cost Control, Fiscal Management: Legacy Modernization: Enterprise Vision and Roadmap for IT).

Impact

The impact to State operations is dramatically improved because of the core network upgrade. Just a few examples of the improvements:

Impact	Before Core Network Upgrade	After Core Network Upgrade
Reliability	Network outages	The risk of catastrophic network outage has been eliminated
Security	Higher risk of security breaches	The new network is much more secure than the legacy network which reduces the risk of a security breach and improves regulatory compliance
Availability	Agencies and application development teams faced downtime due to network maintenance outages System components being serviced interrupted network access	The new core network has provided 100% availability since the upgrades were completed Access to the Internet is now fully redundant and system components can be serviced without interrupting network access
Portability	The file replication/tiering between datacenters used to take days	The file replication/tiering between datacenters now takes just a few minutes
Performance	High latency	Enormous throughput improvements at the core network now provides network latency at less than 1 millisecond. New applications on-premise, in the cloud or hybrid can be deployed without concern that the throughput will degrade

As stated previously, the success of this project has significantly improved the perception of OIT's Network Services team:

- By successfully accomplishing the upgrades and communicating extensively with all State agencies, a new confidence in the team's abilities was established throughout State government.
- With less time spent on break/fix and with new monitoring tools, the Network Team is building on this success by anticipating problems before they occur and further improving uptime to our customers. Finally, the project more than justified the financial expenditure - the State simply could not move forward and meet its obligations to the State's citizens and State agencies without remediating the risks and limitations inherent in the legacy core network.