IP Transition Best Practices

Networks and Telecommunications Community of Interest

FTI-2 Working Group

Transition and Implementation Subcommittee

Date Released: April 14, 2017

Synopsis

All networks organically grow and develop over time. This property of networks leads to the introduction of divergent elements in various locations, such that the different portions of the network are qualitatively different in capability, access, and administration. Further, as networks age organically, they tend to ossify, and develop a resistance to new features, and the introduction of a new process, security approach, or application becomes problematic. When transitioning, understanding and documentation of the existing network is vital. Undiscovered aspects of the existing network can cause delays in transitioning.

This paper discusses best practices for transitioning the FAA FTI infrastructure to an IP-based architecture and provides suggestions on tactics and strategies that may be used to minimize operational disruption during the transition process.
American Council for Technology-Industry Advisory Council (ACT-IAC)

The American Council for Technology (ACT) – Industry Advisory Council (IAC) is a non-profit educational organization established to create a more effective and innovative government. ACT-IAC provides a unique, objective and trusted forum where government and industry executives are working together to improve public services and agency operations through the use of technology. ACT-IAC contributes to better communications between government and industry, collaborative and innovative problem solving and a more professional and qualified workforce.

The information, conclusions and recommendations contained in this publication were produced by volunteers from industry and government advisors supporting the objective of more effective and innovative use of technology by federal agencies. ACT-IAC volunteers represent a wide diversity of organizations (public and private) and functions. These volunteers use the ACT-IAC collaborative process, refined over thirty years of experience, to produce outcomes that are consensus-based. The findings and recommendations contained in this report are based on consensus and do not represent the views of any particular individual or organization.

To maintain the objectivity and integrity of its collaborative process, ACT-IAC does not accept government funding. ACT-IAC welcomes the participation of all public and private organizations committed to improving the delivery of public services through the effective and efficient use of IT. For additional information, visit the ACT-IAC website at www.actiac.org.

The ACT-IAC Networks & Telecommunications (N&T) Community of Interest (COI)

The N&T COI mission is to provide clarity, impartial feedback, and points for consideration on networks and telecom issues identified in collaboration with the federal government and industry. The N&T COI provides a forum where government and industry executives are working together on key telecommunication issues such as interoperability, information sharing, communications architectures, wireless technologies, converged internet protocol based services, security, and continuity of service.

The N&T COI established a working group to facilitate collaboration between government and industry on matters concerning the upcoming FTI-2 effort.

Disclaimer

This document has been prepared to contribute to a more effective, efficient and innovative government. The information contained in this report is the result of a collaborative process in which a number of individuals participated. This document does not – nor is it intended to – endorse or recommend any specific technology, product or vendor. Moreover, the views expressed in this document do not necessarily represent the official views of the individuals and organizations that participated in its development. Every effort has been made to present accurate and reliable information in this report. However, ACT-IAC assumes no responsibility for consequences resulting from the use of the information herein.
This paper was prepared by ACT-IAC after consultation with the Federal Aviation Administration. The information and opinions contained herein are those of the ACT-IAC and are not reflection of any planned strategy or approach to FTI-2 by the FAA.

Copyright © American Council for Technology, 2017. This document may not be quoted, reproduced and/or distributed unless credit is given to the American Council for Technology-Industry Advisory Council.

For further information, contact the American Council for Technology-Industry Advisory Council at (703) 208-4800 or www.actiac.org.
Contents

Introduction and Executive Summary ........................................................................................................... 5
Scope .................................................................................................................................................................. 5
  Making the Transition .......................................................................................................................................... 5
  Technical considerations ......................................................................................................................................... 6
  Standardization .................................................................................................................................................. 6
Operational Considerations ................................................................................................................................. 6
  Tactics to Achieve Minimal Disruption .............................................................................................................. 7
Contingency Planning ......................................................................................................................................... 8
  Network Operations Center (NOC) Transition .................................................................................................... 8
Security Considerations ......................................................................................................................................... 9
Recommendations .................................................................................................................................................. 9
Introduction and Executive Summary

All networks organically grow and develop over time. This property of networks leads to the introduction of divergent elements in various locations, such that the different portions of the network are qualitatively different in capability, access, and administration. Further, as networks age organically, they tend to ossify, and develop a resistance to new features, and the introduction of a new process, security approach, or application becomes problematic. This calcification is often described as “cruft,” and preventing the buildup of cruft is the task of system and network administrators. Cruft prevention by administrators is as much of an ongoing process as trash removal is by janitorial staff.

When transitioning, understanding and documentation of the existing network is vital. Undiscovered aspects of the existing network can cause delays in transitioning.

Scope

This paper identifies processes, issues, and concerns that the FAA may have in moving from an existing IP network to that provided by a new vendor.

In FAA, the total network should be considered in transition. This not only includes the FAA Telecommunications Infrastructure (FTI) nationwide IP network but all sub networks, such as Local Area Networks (LANs), metropolitan networks and interfaces to other networks, internet, test networks, gateways, etc.

While all carriers provide IP networks, a key choice for FAA will be to select an existing commercial network, a private IP network or a hybrid approach. Each of these options provides cost benefit tradeoffs. A single-threaded, commercially-provided IP network may not provide the performance the FAA requires for its critical air traffic control functions, so it seems logical that, for critical services some type of hybrid or private network could be required. In either case, the transition concerns remain the same regardless of the number of separate networks. However, the complexity grows proportionally.

However, a commercially available network can provide the FAA with a constantly updated network for its non-critical users. Carriers cannot permit their network to become obsolete as an existing client could move to another vendor and new clients, rather than use an obsolete network. FAA may not have funding for network upgrades and continuous technology refresh.

Making the Transition

To complete any network transition, a complete operational network should be established or be in existence. For a commercial network, that’s a given. The concern here is threefold, (1) establishing a functioning gateway with the incumbent network, (2) providing authentication services for a Virtual Private Network (VPN) and (3) getting connectivity to all the required customer locations. This latter concern is the major constraint to transitioning the FAA service.

In a private network, a VPN may not be required. However, the added security can offer benefits that FAA should consider for its most critical services. A VPN on a private network adds an additional layer of security.
Layered security is a defense in depth capability and should be implemented for increased security. This should be part of an overarching cyber security architectural framework.

**Technical considerations**

Availability in a single IP network can achieve 99.999% or better from pop-to-pop on the network. Last mile segments can lower overall availability leading to not achieving the required total performance level for FAA critical services. FAA requires not only the total end-to-end performance, but also the prevention of large segments of the network becoming unusable due to single point failures. A single large network router or system software failure can cause FAA significant impacts to its air traffic. However, there are architectural alternatives that can alleviate these weaknesses. Dual networks, with different underlying fabrics, for example alternative architectures and software, can achieve both the required diversity and performance, but at a significant increase in cost and complexity.

For non-critical services, a single IP network can achieve the network availability required for FAA critical services, as availability exceeds 99.999%.

**Standardization**

Currently IP networks have reached a high degree of standardization and should work collaboratively to deliver service. As such establishing gateways between networks is relatively straightforward. Transitions from one IP network to another, is not a complex undertaking. However, transitioning users and systems can be a challenge. FAA has experience transitioning from ADTN2000 to the Harris IP network.

Interfaces to local area networks are routine, but could pose a problem. Networks can be locally “enhanced” as an example a firewall may have been added which is not managed by the network vendor. Additionally the Agency managed Local Area Networks (LANs) could pose bandwidth issues.

**Operational Considerations**

The time involved in transitioning the IP network is a major factor for the consideration. With more than 4,000 locations that need new connectivity, and in excess of 40,000 users, the magnitude of the work is daunting. This is complicated by FAA requirements for diversity of access and coordination requirements for transitioning “live” air traffic control systems. The selected vendor should have a very disciplined and practiced program management approach to effectively provision the access circuits. And, since they may be in many different Telco territories, the tested ability to effectively interface with the Local Exchange Carriers (LECs) is critical to timely transition.

Timely transition is directly linked to the cost to transition. Transition requires funding for duplicate network, personnel costs, management, overhead and NOC fees. Cost savings cannot be achieved until services of the incumbent can be terminated. As long as a few circuits or users are attached to the expiring network these charges continue to accrue. Meanwhile as a new network is stood up, tested and users and services are cut over, charges from the new vendor begin to be billed. It is in the best interest of the FAA and selected vendor
to minimize the transition time. The incumbent provider has no advantage in shortening that time; rather the incentive is to lengthen that time.

Therefore, the FAA should stress a well-managed and short duration of the transition. FAA air traffic continuity of operations may drive a slow and safety conscious transition. A balance should be struck to achieve the best solution for FAA. A requirement for a detailed transition plan along with a safety management plan should assure completeness, and not permit undisciplined transition strategies. A strong past performance record of timely transitions with minimum disruption of service should be a key FAA requirement.

The proposed transition plan should quantitatively balance minimizing cost at the same time assuring continued safety. The plan should be detailed enough to show realistic installation times, provide disciplined oversight of ordering, provisioning, testing and turn-up, and guard against gaming of the process. Proven provisioning techniques and escalation process and history should be a required demonstrated capability.

While it may be enticing for FAA to ask for creative ways to minimize transition costs and schedule, the FAA requires very high safety margins in its critical services. Vendors should be required to provide realistic, demonstrated performance in transition plans: ones that can be repeated and provisioned at high levels of performance.

The implementation plan should clearly demonstrate adequate detail and realistic projection. It should also include techniques for reducing technical risk and minimize special work. Good bandwidth estimates for all facilities will be a necessity, especially with a transition schedule that is several years away from starting. While it is most likely that the potential exists for many facilities to “special construction” to improve access to meet existing and future requirements, FAA should strive to make the new network as flexible as possible as bandwidth requirements of customers is growing at higher rates. FAA should not underestimate the initial bandwidth requirements in order to minimize initial cost at the expense of needing additional bandwidth a few years in the future.

**Tactics to Achieve Minimal Disruption**

Advance planning is the most critical factor in preparing for a transition. The requirement for FAA to require these plans in detail, with proven success cannot be over emphasized. Their sheer size and scope of the transition is a daunting task. This ranges from engineering the network, estimating bandwidth, providing bandwidth services increases and decreases on demand, testing and turn up, site surveys, experience installation technicians and qualified personnel to guide the FAA in the planning that the FAA should take to prepare sites and minimize schedule conflicts. These are a few of the complex activities that should take place. A flexible scheduling plan is required to meet conflicting program demands such as other FAA NextGen acquisitions (e.g. the NAS Voice System) that will come on line with yet to be defined schedules. Other NextGen programs will progress through their acquisition cycles and future capabilities will be added to the NAS.

All programs require telecommunication connectivity to provide their benefits to FAA. Other non-NAS systems may undergo transitions as technology improvements become available over the projected lifespan of the
contract period of performance. As the FAA makes improvements to its financial, procurement, payment, payroll, and other systems, flexibility in scheduling may be needed along with sensitivity to FAA and its internal and external customers and stakeholders. FAA should require a proven ability to meet very large and demanding customers and manage demanding, large-scale transition schedules. Not only should the plans be detailed and achievable, they should also be adaptable to both the changing needs of the FAA and to integrate changes in the rapidly changing telecommunications marketplace.

FAA needs a telecommunications partner that has the foresight and engineering capability to help FAA avoid telecommunications obsolescence as this market is changing. There needs to be flexible and adaptable designs that can minimize disruptive events that can impact or compromise FAA safety. As FAA moves to incorporate resiliency into its systems, that same resiliency needs to be incorporated into its future telecommunications system, minimizing future transition impacts and providing easier recovery in the event of catastrophic events.

Contingency Planning

Delays in transitioning may occur. Even the best planning efforts cannot eliminate unforeseen conditions and events. These delays can occur in all facets of deployment including carrier, LEC, and customer. Understanding and knowing the pitfalls should allow the minimization of the impact to timelines and scheduling. Having a robust plan to include a contingency plan around delays should position the FAA to counter the adverse impacts of delays more quickly.

FAA should require the development of multiple migration options. In evaluating its risk appetite, different levels of risk should be associated with migration options. Then when developing and evaluating sequencing and corresponding infrastructure changes, an associated risk for each migration options can be established.

A robust test plan is a requirement for each transition. It cannot be assumed that a standard test plan will work. Attention to detail in developing test plans can make a significant contribution to minimizing the impact of transition.

Including operations, both technical operations personnel (NAS and non-NAS) and air traffic operations personnel can yield significant benefits to the planning and transition for seamless handover. These operations personnel understand the details of the operation and can be valuable to coordinating. They understand the services provided to the end user, know their language and culture and can assist in overcoming barriers.

Fall back provisioning is essential to providing a level of security when engaging in cutovers, especially when dealing with critical services. Failure of a cutover that cannot be corrected quickly jeopardizes the customer’s trust in future transition efforts. Knowing there is fallback plan that can be quickly invoked may assure the FAA operations personnel that they will not be in an intolerable situation.

Network Operations Center (NOC) Transition

The potential transitioning of the NOC operations from the existing provider to a new vendor poses a multitude of issues. Different processes, cultures, and approaches will pose hurdles for the FAA and the vendors to overcome. Establishing good communications between the two operations is vital to success. The
incoming vendor should take on the challenge of understanding the current NOC operation and adapting to minimize the differences. The NOC operations depend on people and the losing vendor’s staff will be concerned with the loss of employment, and the vendor the loss of revenue, and will lack motivation to go the extra mile. Incumbent capture may provide a resolution, but may not be possible. The FAA should maintain a high level of performance from both operations during the transition. Coordination and cooperation are requirements that should be established and maintained. Communications is essential in efficiently transitioning this operation. A detailed plan should be in place to assure that this part of the implementation works smoothly. Unhindered sharing of information should be a key factor in the day-to-day operation. Attention to how the NOC transition is planned and executed has a huge effect on successful transitioning.

A key factor in NOC operation is a help desk function. This key interface provides the link between operations personnel and the telecom vendors operation. Both tend to have different languages and cultures. It is important to have a help desk that can bridge that gap.

Security Considerations

A vital concern is the security of the transition. FAA should not allow gaps to develop in its security posture during and after the transition. A security plan should be an integral part of the transition plan. It should address all government security orders and standards. This should address both technical operations and personnel security practices.

Recommendations

A Virtual Private Network (VPN) approach with encryption is recommended as a means of enhancing and continuously improving an information security posture. This should be in concert with a strategy for an evolving cyber security plan. It is not solely a telecommunications function to provide a robust cyber security framework. However, the telecommunications organization should provide the operational infrastructure to implement, operate, and continuously improve the FAA cyber security posture. While telecommunications can provide the tools and operational elements to enhance cyber security, it alone cannot implement an integrated security environment with all the affected NAS and non-NAS systems to effectively provide end-to-end security.

FAA should consider establishing a dedicated transition team to plan and execute the transition from FTI to its replacement. Planning is the key to developing a schedule that can be implemented with a goal to minimizing costs, and transition risk. The team should be assembled and begin work as the solicitation is being prepared. As FAA works through assembling the details of the number, type, and locations to be transitioned, it will be able to ask industry for detailed plans and effectively evaluate them.

The variety of users and disparate systems, all being actively acquired, modified and enhanced during the acquisition and implementation of FTI-2 should also be managed by the FAA transition team. Transitions risk in these systems is effectively manages by including these organizations in the development of the Screening Information Request (SIR), and in the planning for transition. While the air traffic systems should be known and the technical resources managing them easily identified, this may not be true for all the non-NAS systems. All
these systems should have technical resources from their operation organizations as members of the FAA FTI-2 transition team.

Another area posing risk to FAA in the transition is an over optimistic estimate of provisioning times. While not always technically challenging, coordinating multiple companies’ activities to provision circuits is a task not to be underestimated. Circuit ordering and provisioning involves assembling and validating a large amount of data for each circuit order then coordinating the many organizations (i.e. design, equipment provisioning, construction, installation, testing, etc.) to deliver service. FAA should ask for historical transition times and not rely on estimated or nominal transition times.
Contributors and Affiliations

David Lantzy – AT&T
John L. Lee – Internet Associates, LLC
Tom Cuneo - Vision Technologies, Inc.