Network Security Considerations for ATM Services

Paul Groppel

Sean Boden

L3Harris Technologies

TABLE OF CONTENTS

LIST OF FIGURES

Network Security Considerations for ATM Services

EXECUTIVE SUMMARY

Telecommunication services have undergone drastic technological changes over the last decade, evolving from legacy voice services, such as point-to-point Time Division Multiplexing (TDM), to large-scale economical Internet Protocol (IP)-based networks using the latest networking technologies that provide data services globally. Through this evolution, organizations have had to address how to best leverage these new technologies to meet their business needs without compromising the safety and security of their most sensitive data. In many cases, organizations have turned to broadband Internet or Long-Term Evolution (LTE) wireless technologies for network transport using infrastructures offered by carrier service providers. In other cases, organizations have chosen to use private Multi-Protocol Label Switching (MPLS) infrastructures to protect their organization from exposure to threats found in the public domain. Ultimately, how organizations assess the criticality of their data and services will drive their decision to use a service provider that best supports their business and security goals.

Organizations handling mission critical data, such as Air Traffic Management (ATM) data, should be especially concerned about how well these emerging technologies guarantee the Confidentiality, Integrity, and Availability of their data. While there are several advantages to adopting technologies offered by carrier providers, there are also many risks.

Mission Critical

Since the early days of computers, information technology has become an integral part of our everyday lives. Today, whole industries have become so dependent on computers and networks that, without them, they would not be able to produce the services or products critical to their success. This is also true for U.S. Government (USG) organizations and the missions and services they support. Because of these dependencies, the USG identified cybersecurity as a significant risk to all 16 of the U.S. Critical Infrastructure Sectors. The USG defines critical infrastructures as:

"Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[1]

For this reason, the Government assigned federal organizations to aid in oversight and protection of these sectors. The 16 US critical infrastructure sectors are listed below.

Chemical Sector	Commercial Facilities Sector
Communications Sector	Critical Manufacturing Sector
Dams Sector	Defense Industrial Base Sector
Emergency Services Sector	Energy Sector
Financial Services Sector	Food and Agriculture Sector
Government Facilities Sector	Healthcare and Public Health Sector
Information Technology Sector	Nuclear Reactors, Materials and Waste Sector
Transportation Systems Sector	Water and Wastewater Systems Sector

Air Traffic Management systems fall within the Aviation mode of the Transportation Systems Sector. While all 16 critical infrastructures are important and dependent on each other, each have different approaches to how they implement security defense strategies to protect their critical systems and data. As an example, the approach for ensuring the protection of ATM systems and services include a higher-level of protection for the core infrastructure. However, retail organizations focus their defensive technologies on the protection of consumer transactions and private payment data. In the case of healthcare, health organizations build tighter security around systems that treat patients or store private health records. Ultimately, the goal for securing ATM systems and services is to ensure air operations remain functional to protect the safety and lives of nearly 950 million passengers who take to the skies annually. In addition, the U.S. military structure relies on commercial air transportation to support the transport of goods and supplies which makes ATM systems and services prime targets for U.S. enemies. For these reasons, careful consideration of cybersecurity risks is required for evaluating and implementing new technologies in support of ATM, especially with those programs that rely on the National Airspace System (NAS), which is part of the nation's critical infrastructure.[2]

Protecting Mission Critical Systems

With the recent attacks on our critical infrastructures, it is imperative that organizations implement a strong security posture to protect their most vital data and systems. Attackers are constantly looking for new ways to exploit vulnerabilities to compromise system and network architectures. Critical infrastructures present a high-value target for nation-state actors, cyber criminals and hacker groups who look to gain access to critical systems for malicious, financial or political gain. The development and dissemination of a large array of attacks by these groups has led to the need for additional safeguards to defend mission critical data, systems, and networks from ever-evolving, sophisticated cyber-attacks.

The National Institute of Standards and Technology (NIST) has defined mission critical as "Any telecommunications or information system that is defined as a national security system (FISMA) or processes any information the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency." Many ATM systems and services are considered mission critical since they serve as critical components to protecting flight safety for across the aviation ecosystem. This is a key factor which drives how the Federal Information Security Management Act (FISMA) impact rating is determined for ATM systems. Table 1 lists the impact levels defined for Confidentiality, Integrity, and Availability, as defined in the Federal Information Processing Standards (FIPS) Publication 199.

FISMA Impact Levels

Today, many ATM systems and services are rated as Moderate impact systems. However, recent government analysis determined that those deemed to be part of the critical infrastructure will be rated at a FISMA High impact level, primarily because of the potential for loss of life should these services become unavailable, impaired or modified. Another reason for the High impact rating is that the airline industry, and air transportation in general, would experience significant financial impacts if ATM services were inaccessible. This elevated FISMA rating has significant impact on how ATM systems and services are protected from cybersecurity threats.

A FISMA High impact level adds additional requirements for ATM data and resource protection, which also drives significant costs to implement. While many of these systems may already implement some High impact requirements as a cybersecurity best practice, additional security implementations will be required to further protect data from manipulation and ensure services remain available. These increased requirements are much easier to achieve when leveraging an integrator who can help manage risk impacts to protect critical systems and data. While the option to leverage a shared infrastructure through commercial carriers is being considered, there are inherent

[1] https://www.gpo.gov/fdsys/pkg/USCODE-2010-title42/pdf/USCODE-2010-title42-chap68-subchapIV-B-sec5195c.pdf

[2] https://www.gao.gov/assets/670/668169.pdf

risks in migrating ATM data to these infrastructures. To achieve FISMA High compliance on a public infrastructure, there would need to be more protection mechanisms in place to defend against the high volume of threats resident on the public Internet (as described later in this document). These additional implementations would increase costs associated with protecting ATM critical data from these continuously increasing threats.

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modifications or destruction of information could be expected to have **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modifications or destruction of information could be expected to have **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modifications or destruction of information could be expected to have **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Table 1: Potential Impact Definitions for Security Objectives

Cyber Security Risks

For decades, ATM systems and services have utilized TDM Wide Area Networks (WANs) to support voice services across the NAS. These WANs have enabled secure, high-quality, and highly reliable transport of a multitude of user applications including: basic telephony, trunked radio, low-to-medium rate data services and studio-to-transmitter links for broadcast audio and video.[3] However, advancements in networking technologies, coupled with the cost of maintaining aging legacy TDM devices and circuits, are driving organizations to consolidate data into a converged network architecture over more modern wireline circuits or wireless technologies. While these changes may be good for traditional digital businesses that operate in the commercial sector (retail, finance, etc.), this consolidation over shared IP networks exposes mission critical data to increased cyber threats traditionally not faced within closed networks and presents new challenges for the protection of ATM systems and services.

Cyber Security Threats to ATM Systems

As ATM systems transition their legacy services to a single network infrastructure, they need to be aware of cyber security threats that may impact their data. TDM infrastructures isolated critical services from the increasing number of cyber threats in which shared infrastructure networks are exposed to daily. Understanding these threats will help in building a mitigation and defense strategy to protect critical ATM systems and services from attack and being exploited by U.S. adversaries. The attacks listed below are just a small subset of attacks that threaten shared infrastructure networks.[4] They are categorized based on the three security objectives for information and information systems - Confidentiality, Integrity, and Availability (the CIA triad) – to show how they relate to the FISMA impact levels in *Table 1* above.

Confidentiality Attacks

Attacks against confidentiality provide an unauthorized means of capturing confidential data. Over an IP infrastructure, these attacks can occur anywhere in the network an attacker only needs to target a single weak point to perform the following attacks.

- Packet Capturing (Packet Sniffing) – These attacks capture data packets in transit on the network. Once data is captured, the attacker can read sensitive data.
- Port Scanning/Ping Sweeps – In this scenario, an attacker tries to discover services by scanning the TCP/UDP ports. Once an open port is found, an attacker identifies services and software and begins exploiting known flaws.
- Wiretapping – These are attacks where an attacker hacks the telecommunication devices to listen to voice communications.

[3] https://pdfs.semanticscholar.org/ca64/0b9acbd40dff032cc9b1b2c8044518081a73.pdf

[4] http://www.omnisecu.com/ccna-security/types-of-network-attacks.php

Integrity Attacks
Integrity attacks alter packets during transmission. These attacks present a significant risk to ATM systems and services where the malicious act of masking or spoofing aircraft data can have grave implications. There are several cyber security threats that impact integrity. A few of the more common ones are listed below.

- Man-in-the-Middle Attacks – In this attack, an attacker sits between two devices that are communicating and manipulates the data as it moves between them.
- Session hijacking Attacks – This is another type of network attack where the attacker hacks a computer session to gain unauthorized access to information or services in a computer system.
- Spoofing (Masquerading) – This attack is the ability to impersonate a user, device, or service to gain access to a network service, network element or information. Spoofing can provide access to sensitive data or lead to other attacks such as a Denial of Service (DoS).[5]

Availability Attacks
Availability attacks generally aim at disrupting communication services in the form of a DoS. Availability attacks present the highest level of risk to ATM services over a shared network due to the high number of network components that can be attacked to disrupt or disable services. However, availability impacts can also occur from non-malicious entities as described below.

- Denial of Service – DoS attacks are when a large number of service requests are directed at a target system or resource from a single device. Too many requests may cause a device or network to crash, preventing users from accessing services. DoS attacks are broken down into three types – Volume Based Attacks, Protocol Attacks and Application Layer Attacks.
- Shared Resource Impacts – When using a shared network infrastructure, commercial carriers place multiple customers and services on the same network core. Often, impacts to other customers may require a carrier to take actions that may impact critical services of other customers that share the same network infrastructure.

Wireless Security Risks
Availability attacks generally aim at disrupting communication services in the form of a DoS. Availability attacks present the highest level of risk to ATM services over a shared network due to the high number of network components that can be attacked to disrupt or disable services. However, availability impacts can also occur from non-malicious entities as described below.

LTE Security Risks
LTE technology has existed for several years and provides a valuable way to transmit data over airwaves. However, just like wired IP networks, wireless devices and networks have many similar threats that can be exploited. While they can be a little more sophisticated than attacking a wired network, tools and equipment required to exploit these devices are attainable online and provide how-to exploit guides that allow even novice users to successfully penetrate a network. The following threats are some of the most common threats to LTE, as defined by the National Institute of Standards and Technology (NIST).[6]

- General Cyber Security Threats – LTE components may run atop of commodity hardware, firmware or software making it susceptible to known software flaws in general purpose operating systems or other software applications. Malware attacks to devices that connect to an LTE architecture (mobile devices or core network infrastructure) can be crafted to create DoS attacks or even gain unauthorized access to network components.
- Rogue Base Stations – Rogue base stations are unlicensed base stations that are not owned and operated by an authentic mobile network operator. They broadcast a cellular network masquerading as a legitimate carrier network. The necessary hardware to construct these devices can be inexpensively obtained using Commercial Off-the-Shelf (COTS) hardware.
- Air interface Eavesdropping – A complex eavesdropping attack is possible if the operator does not encrypt LTE traffic. Eavesdropping on LTE devices definitely requires a significant level of expertise. An attacker would need the proper equipment to capture and store radio communication and the software to identify specific LTE frequencies and timeslots to demodulate captured traffic into IP packets.
- Radio Jamming Attacks – This is a method of interrupting access to networks by exploiting the radio frequency channel being used to transmit and receive information. Specifically, this attack occurs by decreasing the signal to noise ratio by transmitting static and/or noise at high power levels across a given frequency band. This classification of attack can be accomplished in a variety of ways requiring a varying level of skill and access to specialized equipment, such as unmanned aircraft, drones.
- Physical Attacks – While LTE devices are usually protected by various physical security measures, these protections can be circumvented, giving the attacker a chance to degrade or destroy services, causing a network outage or DoS situation.

[5] https://www.researchgate.net/publication/220449868_VoIP_Security_-_Attacks_and_Solutions
[6] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-187.pdf

Cyber Security Mitigation Strategies

The Internet is riddled with cyber security threats that continuously attack every layer of the Open System Interconnection (OSI) model. Organizations are constantly investing in hardware and software to aid their efforts in protecting vital systems and services from cyber threats. While these products offer many capabilities, they are often built with a common default enterprise configuration that are not tailored to specific needs of ATM system owners. For some businesses and organizations, this basic configuration is fine. However, for system owners who have unique challenges that need to be addressed, the level of service required to effectively build and integrate security products and solutions into their environment takes an increased level of support by these product vendors. While cost may increase for this level of dedicated service, the result is a tailored solution that provides a more effective protection capability against cyber threats. These same principles can be applied to how a network infrastructure is serviced and protected against the growing cyber threats ATM systems and services face as they adopt a network architecture for their application needs. While commercial carriers can offer flexible network offerings and decreased costs by leveraging their shared network infrastructure offered to their consumers, the level of service provided is bound by Service Level Agreements (SLAs) that are highly structured and difficult to modify to address unique ATM challenges. In contrast, using an integrator who understands customer needs can offer highly flexible service offerings to address unique challenges faced in protecting critical ATM systems and services.

Commercial Carrier Services

Commercial telecommunication carriers have built large network infrastructures to service customers across the country. From large organizations (Government, financial, retail, etc.) to residential consumers, these carriers offer varying service models to address each client segment needs. However, this also presents a challenge with the types of services they can provide to clients with unique needs and data requirements. While there are several benefits for leveraging commercial carrier infrastructures, there are also several weaknesses that can have a major impact on ATM critical systems and services.

Opportunities

- Cost Savings – Commercial carriers have large network infrastructures that offer various data path options. They are able to offer cost savings by sharing paths between all customers (a one size fits all approach). This shared infrastructure model keeps costs down for customers while providing a basic level of service and availability.
- Data Transport Options – Many carriers have a wide array of data path options available across their shared infrastructure, of which customers can take advantage. Technologies such as MPLS, broadband (Internet) or LTE are utilized, as needed, to pass data.

Challenges

- Data Protection – While many carriers have several mechanisms in place to protect their infrastructure, their service offerings are limited to a basic level of support for the underlying transport. Increased monitoring of applications or additional data protection services are typically available, but usually as a service enhancement. Without these additional services, application services are left exposed to attacks unless additional protections are implemented. A majority of network cyber threats described above can have real impact over a commercial carrier network because of their limited, base protection offerings. Carriers can offer increased security support, but typically this support is built around a “premium” service offering not included with base services.
- Shared Resources – While carriers do their best to reduce service impacts to their customers, they do not guarantee that services will not be impacted due to external factors presented by other customers sharing the infrastructure. With customers responsible for their own data protection, a compromise of another entity’s services may result in degradation or loss of critical services. For example, a compromise of an entity’s systems may result in a DoS on the network, which would then impact bandwidth across the network and access to services. System owners may lose control over service impacts, limiting their ability to ensure they remain available.
- Human Error – Human errors can have a direct impact on ATM services. According to a report by IBM security services, 95% of most security incidents are caused by human error. A few of the most common incidents include misconfiguration, patch management and use of default usernames and passwords.[7] When configuration changes are required on devices, an engineer may have to touch several devices to make a change to a single device configuration. This presents the opportunity for accidental misconfigurations to occur anywhere along the path. These misconfigurations could expose customers to having their data exposed to other customers sharing the same core, who are not authorized to receive or see this data (VLAN misconfiguration, MPLS label switching). Additionally, when technicians who lack knowledge of customer services and mission priorities make a change to a device they may not realize the impacts.
- Insider Threat – While ATM system owners may have strict requirements for personnel with regards to background checks and citizenship, commercial carriers may not have the same level of requirements. At any time, a potential insider could have access to critical data pipelines exposing them to connections and data in which they would not otherwise have access.
- Lack of Control – While commercial carriers offer insight into the management and configurations of edge devices, they typically do not offer insight into the management and operations of their core infrastructure. They control all aspects of maintenance and configuration which, for ATM systems and services, presents challenges when maintenance on one network segment impacts critical services and air operations without their knowledge.

[7] https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf

- Lack of Dedicated Support – Commercial carriers have thousands of customers and all have unique needs and services. Often times, when a support call is received it is balanced against competing priorities amongst all of the carrier's customers. Call center technicians may not have dedicated or intimate knowledge of systems or services being impacted and treat calls as any other call they receive.

Dedicated Managed Services
Unlike commercial carriers, a dedicated managed service provides an all-inclusive service model the ensures critical ATM systems and services are given the appropriate level of support needed to maintain operations and ensure protection of critical data. While transport offerings may not be as cheap as a commercial carrier, the dedicated support and services are far superior. An integrator with intimate knowledge of customer's needs and unique mission requirements can offer tailored offerings.

Opportunities
- Dedicated Protection – A dedicated managed security service is designed around the mission and provides the appropriate support required for ATM systems and service to be protected against adversarial threats. Network and data protection solutions and configurations can be designed to protect vital air traffic services without having to worry about impacts to, or from, other external customers. Additionally, a managed service can offer a holistic view into the network and aid in the protection of critical system components.
- Enhanced Services – When services do not have to share a network with other customers, the level of service availability is increased significantly. Maintenance impacts are coordinated and controlled which helps prevent inadvertent outages to critical ATM systems and services.
- Higher Level of Control – While commercial carriers limit insight into how the network infrastructure is maintained and operated, a dedicated managed service provider can offer a holistic view over the entire network providing complete visibility into management and operations. This insight allows ATM services to be included in decisions that may impact operational capabilities.
- Dedicated Service Support – A dedicated managed service provider has service technicians who understand the customer mission and will ensure their application and mission needs are appropriately prioritized to ensure quick resolution of any issues. There are no competing priorities.

Challenges
- Cost – Compared to commercial carriers, a dedicated managed service provider can seem pricier, due to the commercial carrier's shared cost model that offers services across their shared network infrastructure. However, provided service level is no different than that of other customers. A dedicated managed service provider offers a full-service capability, tailored to the unique mission of ATM systems. Much like the security product vendor who tailors their solution to provide the best protections their solution can offer, a dedicated service provider can provide tailored support and address their customer's unique challenges.
- Human Error – As mentioned previously, human errors can have a direct impact on ATM services. Any time manual configuration changes occur on a device, there is a potential risk for a mistake that will impact services. While a challenge regardless of service provider, a managed service will have better insight into how to address and correct these errors to build processes to limit them in the future.
- Insider Threat – Unfortunately, insider threats are a reality whether intentional or not. Even if a managed service provider had complete control over personnel used to support the core infrastructure, there is no guarantee this will eliminated an insider threat.

Technologies to Enhance Security
Protecting critical ATM systems and services is a vital role for any service provider. However, there is an added value of having a dedicated service to protect against today's growing cyber threat landscape. As networking technologies evolve and the need for better performance of services is required, organizations will look for new ways to achieve security while enhancing operational capabilities. Two technologies that can enhance service protection while increasing performance, reliability and availability are dark fiber infrastructures and Software Defined-Wide Area Networks (SD-WAN). Each offers unique capabilities that increase the security services a dedicated service provider offers to ensure ATM systems and services are protected against cyber threats.

Dark Fiber
Unlike the "Dark Web", dark fiber does not support the criminal underworld of the hidden Internet. Dark fiber is simply the unused, or "dark", fiber optic network infrastructure that has been placed by large telecommunication companies. When fiber optic cables are provisioned, many companies overestimate the amount of infrastructure and cabling required in order to future-proof their networks from exponential data growth. This overestimation, coupled with technical advances in the way in which data is packaged, means that many optical fiber networks have extra capacity not being used. This extra, unused, capacity is leased out to offer a private network infrastructure protected from public (Internet) access.

As bandwidth demands increased, newer techniques to deliver increased bandwidth and performance expanded the opportunity to create dedicated channels for customers over existing fiber runs. Dense Wavelength Division Multiplexing (DWDM) is a technique to turn a single fiber into several virtual fibers, usually referred to as channels -- colors of laser light -- and each color or virtual fiber can be dedicated to a customer or a service because of its protocol independence. With DWDM, one strand of fiber can support 80 virtual fibers, each carrying its own independent stream of traffic. Dark fiber can carry multiple wavelengths, significantly increasing bandwidth. When ordering a wavelength, customers receive a virtual fiber for themselves with the added advantage of low latency and high security. It can also be fortified with AES-strength encryption, meaning even with a break the data cannot be intercepted. With an entire wavelength

dedicated to a customer's use, there's added flexibility to use a different protocol for other customers on the fiber -- for example, running Ethernet while others are running SONET. If running multiple lower speed legacy services, customers can also multiplex these into one higher capacity wavelength.[8]

Leveraging dark fiber for the network core offers a higher level of control over the supply chain of hardware used, ensures tighter control over bandwidth usage and scaling for critical ATM services, and allows for finer control over mitigating physical security concerns and personnel, or insider threat, challenges. Dark fiber provides a higher level of security protection from increasing threats found across shared network infrastructures.

Software Aware Networking

Many advancements have been made over the past decade in networking technologies thanks to the adoption of virtualization technologies. Focus shifted from building network architectures to support systems to network technologies designed to support applications and services. Data centers have begun using Software Defined Networks (SDN) to provide a way to automate provisioning of application services to consumers. To support larger infrastructure connections, SD-WAN technologies are being used to bring more focus to application performance and automating network resource management across the WAN to better support application services. These technologies remove the need to physically manage network devices independently, and create the ability to orchestrate network resource management and provisioning by creating virtual overlays across the underlays (Layers 1-3 of OSI Model), thus separating the upper stack from the lower stack of the OSI Model. A recent addition to the Software Defined networking model is the idea of an SD-Branch which integrates (at the code level) SD-WAN evolving technologies with SD-Security technologies into a single device that automates network management and security protection.[9]

There are several important components that make up an SD-WAN configuration. Each component plays a vital part in building the application aware intelligence that optimizes network resources to better support application performance.[10] Figure 1 depicts an example SD-WAN configuration and breaks out the different components of an SD-WAN deployment.

- SD-WAN Edge - This is where the SD-WAN tunnel is initiated or terminated and provides the SD-WAN service demarcation, similar to how an Ethernet Network Interface Device (NID) provides the service demarcation for a Carrier Ethernet service. The SD-WAN Edge creates and terminates secured (encrypted) tunnels over different types of wired or wireless underlay networks. It also performs application-based Quality-of-Service (QoS) and security policy enforcement, application forwarding over one or more WAN connections, and QoS performance measurements over each WAN to determine WAN path selection. The SD-WAN Edge may also perform WAN optimization functions such as packet buffering/reordering, data deduplication, data compression, and forward error correction. SD-WAN Edges can include some NAT and firewall capabilities as well.

- SD-WAN Gateway - The SD-WAN Gateway is a special case of an SD-WAN Edge that also enables sites to connect to other sites interconnected via alternative Virtual Private Network (VPN) technologies, e.g., Carrier Ethernet or MPLS VPNs.

- SD-WAN Controller - The SD-WAN Controller provides physical or virtual device management for all SD-WAN Edges and SD-WAN Gateways associated with the Controller. This includes configuration and activation, IP address management, and pushing down policies onto SD-WAN Edges and SD-WAN Gateways. The SD-WAN Controller maintains connections to all SD-WAN Edges and SD-WAN Gateways to identify the operational state of SD-WAN tunnels across different WANs and retrieve QoS performance metrics for each SD-WAN tunnel. These metrics are used by the Service Orchestrator. In some SD-WAN configurations, the SD-WAN Controller and Orchestrator can be combined.

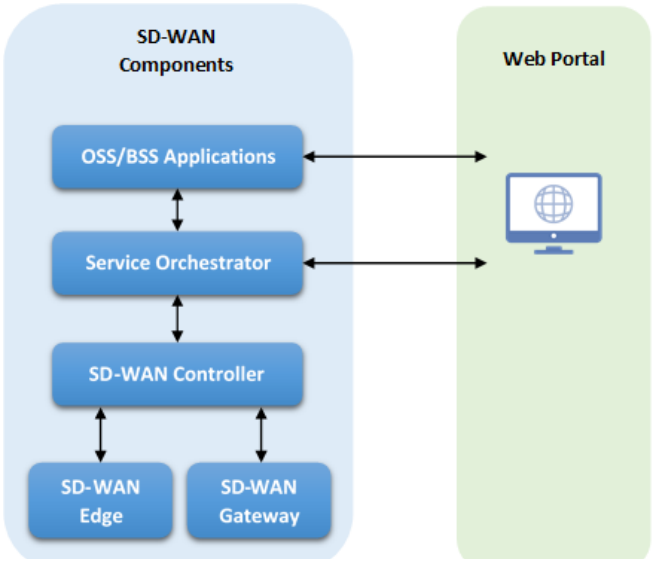

Figure 1: Example SD-WAN Design

- SD-WAN Orchestrator - The Orchestrator provides service management of the SD-WAN service lifecycle including service fulfillment, performance, control, assurance, usage, analytics, security and policy. For example, the Service Orchestrator is responsible for configuring end-to-end SD-WAN managed service between SD-WAN Edges and SD-WAN Gateways over one or more underlay WANs, (e.g., Internet and MPLS, setting up application-based forwarding over WANs based on security, QoS or business or intent-based policies). The Orchestrator also communicates between the Operations Support Systems (OSS) and Business Support Systems (BSS) to best optimize service performance.

[8] https://www.networkcomputing.com/networking/dark-fiber-embracing-dark-side/1084652357

[9] https://www.versa-networks.com/enterprise/sd-branch/

[10] Understanding SD-WAN Managed Services, Published July 2017, MEF Forum. https://wiki.mef.net/display/CESG/SD-WAN+Service+Orchestrator

- Web Portal - The Web Portal is used to access the SD-WAN Orchestrator for management and reporting. It can also communicate with OSS/BSS systems for service activation (as required by SD-WAN deployment options).

Understanding these components allows for better understanding of benefits gained in using SD-WAN and SD-Branch technologies. Several benefits include:[11]

- Optimum Network Usage — SD-WANs are designed to optimize the best network paths based on application or service needs. It will determine the most optimum network path for a service continuously. SD-WAN will select between available transports, using the "best" transport for a given application.
- Network Reliability — SD-WANs connect locations with multiple data services running in active/active configurations. Sub-second network failover allows per packet or session to move to new transports in the event of a brownout or blackout without disrupting the application.
- Manageability — While initial adoption costs may be higher, operating costs are reduced; and better control over the network resources provides a level of network visibility unmet with conventional networks. SD-WAN also provides a single interface, or single pane of glass, that gives network administrators a holistic view of the network eliminating the need for multiple tools and scripts to manage or capture metrics on the network.
- Security — Security is no longer a separate device. SD-WAN controllers are now being integrated with protection services such as stateful firewalls, intrusion detection/prevention, network flow analysis, and behavior analytics. They also offer encrypted connectivity designed to secure traffic in transit across multiple transports.
- Flexibility and Scalability — Scale bandwidth up or down on a moment's notice. Redistribute bandwidth to accommodate flash conditions or new applications. The SD-WAN — not a carrier — automatically controls bandwidth allocation. Therefore, businesses can ensure critical applications receive bandwidth when they needed.

In addition to these benefits, SD-WAN technologies provide better network analytics to help understand network utilization and impacts over time. SD-WAN provides a more comprehensive view of the WAN from an application and network performance perspective, and better oversight into the network security posture. An SD-WAN can operate across several data services (MPLS, LTE, etc.) and can provide the following analytics:

- Gather and share statistics regarding locally attached services providing performance conditions across the virtual overlay
- Provide application intelligence within nodes to identify application traffic flows as they enter the SD-WAN
- Manage customer-defined policies to determine how to steer application flows, defining network conditions to be used to identify the best path across the virtual overlay
- Perform traffic steering or dynamic path control to direct traffic to the best available path

Features offered by these evolving technologies present new opportunities to optimize how network architectures can be designed to better support application availability, while providing a high degree of security protection without impacting performance. This is a paradigm shift from how traditional network architectures are designed and protected.

In the past, to protect the Confidentiality, Integrity and Availability of network resources, integrated security hardware solutions (firewalls, IDS/IPS, malware analysis) were required to protect the boundary. As SD-WAN technologies matured, vendors added security features through Application Programming Interface (API) integrations. While this is a great step towards ensuring security is included with orchestration and automation of the network, it presents performance and configuration challenges. However, SD-Branch solutions have taken these application-focused security features and integrated them with SD-WAN code to present a more efficient and secure solution. This tight integration within the software of the SD-Branch Edge device eliminates the need for purpose built hardware solutions, which tend to drive up costs and potentially have interoperability issues. The SD-Branch device offers optimization of security monitoring, policy enforcement, encryption, and alerting by integrating these features into automation code of a centrally controlled Orchestrator for optimal management and analysis. This takes security monitoring from a reactive, issue-based alerting system to a proactive security monitoring solution which is more robust and better prepared to identify threats within the network.

A defense-in-depth approach offered by SD-WAN technologies is the ability to dynamically provision and harden network devices. The SD-WAN Orchestrator can automate configuration changes and hardening of devices routinely. This automation supports the ability to maintain patch levels on network devices to ensure compliance with FISMA mandates and configuration management policies. Network engineers no longer must manually manage each network device independently which can result in a baseline of differing patch and version levels on devices. It also helps minimize risk or human error. Configuration changes are reduced as the system dynamically steers application traffic to the best path, which ultimately decreases the amount of changes necessary within the infrastructure. Work-flow management provides additional safeguards when pushing configurations to Edge devices; if an error occurs, changes can be backed out, reverting the network to its previous operational state.

Another added benefit that supports service and data availability is how SD-WAN technologies build diversity into the infrastructure. With the ability to see the holistic view of the network, Controllers can make all packet and routing decisions as it pertains to supporting the application performance and priorities. The Controller measures network performance and then chooses the best network paths to

[11] https://www.sd-wan-experts.com/the-ultimate-sd-wan-guide/

send packets, ensuring application performance requirements defined in the application overlay are met. Several features include but are not limited to:

- Dynamic Path Switching
- Per-flow load balancing
- Per-packet load balancing
- Unidirectional measurement and steering
- Forward Error Control (FEC)
- Packet Duplication (Use multiple links to send the same packet)

These aid in optimizing application performance and security by ensuring services remain active while network anomalies are investigated, thus preventing application service downtime and increasing overall availability.

Conclusion

With over 140,000 flight operations per day, the security and functionality of critical ATM systems and services must be a top priority for air transportation industry leaders. For decades, separate networks for voice services and IP were the most secure method for organizations to protect sensitive data and services. However, to reduce management costs of maintaining separate network architectures, organizations are beginning to consolidate these traditionally separate data types into a single infrastructure. When using a shared network infrastructure, commercial carriers typically place multiple customers and services on the same network core. Often, an issue for one or more customers may require a carrier to take actions that may impact critical services of other customers that share the same network infrastructure. As significant pressure exists to be an early adopter of emerging technologies, a strong focus should be on the success of the past with an ability to responsibly adapt to the ever-changing threat landscape.

L3HARRIS™
FAST. FORWARD.