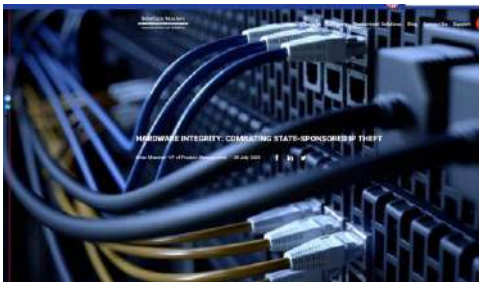
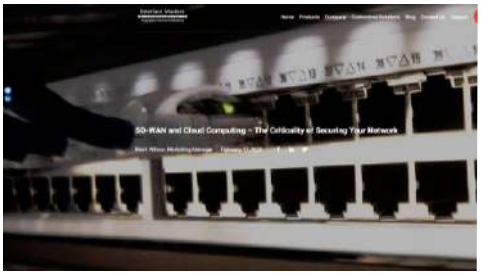




Top 5

Interface Masters

Blog Downloads

- The Migration to 400 Gigabit Ethernet (400GBE)
- Hardware Integrity: Combating State-Sponsored IP Theft
- Tamper-Evident, Intrusion-Resistant Networking Solutions (FIPS140-2)
- SD-WAN and Cloud Computing—The Criticality of Securing Your Network
- Network Appliance: Why Custom?

Interface Masters
TECHNOLOGIES
Innovative Network Solutions

The Migration to 400 Gigabit Ethernet (400GbE)

Updated December 16, 2020

Speed, flexibility, and cost savings are generating the migration for most companies to move IT over to cloud computing. In addition to expansion propelled by businesses, consumers are also driving cloud computing growth through accelerated adoption of mobile applications like maps, social networking, search, and photo/video sharing, which all utilize hyper-scale cloud data centers to provide the speed and agility to meet the needs of these applications.

Projecting out, many businesses are using the innovation and speed of cloud computing to their advantage with new opportunities. One such opportunity has businesses performing data mining /data analytics on large datasets to gain valuable insights, make astute choices, and offer this data for premium services. These analyses are typically run-on mammoth server farms in hyper-scale data centers using innovative AI techniques, and require high throughput and low-latency network performance. Additional opportunities include streaming HD and 4K video available for consumers and for security applications, storage and ease of use have become critical aspects of innovative cloud computing.

As a result of these trends, Cisco predicts that by 2021, 628 large-scale cloud data centers will account for 55 percent of all servers deployed in data centers. This represents a 27%+ compound annual growth rate over a five-year period, which excels beyond the most market metrics.

400 Gigabit Ethernet (400GbE) Emergence in Hyper-Scale Data Centers

Within hyper-scale data centers, network traffic has consistently shown exponential growth. This growth, encouraged by data-rich applications and new information technology architectures, has placed a heavy demand and forced businesses to modernize their data center assets. Similarly, Amazon Web Services (AWS) views data center networking outlays as a critical situation as expenditures accelerate compared to other infrastructures. And, Cisco predicts that traffic within large scale data centers will triple by the end of 2021.

As hyper-scale data centers transition to faster more scalable network architectures, such as the 2-tier leaf-spine, the need for higher bandwidth with efficient connectivity becomes more critical. The leaf-spine architecture requires a considerable amount of cable and interconnects as each leaf switch fans-out to every spine switch, maximizing connectivity between servers. Hardware accelerators, artificial intelligence, 5G, edge computing, and deep learning functions in data centers all consume high bandwidth, forcing high-end data centers to quickly move to next generation interconnects operating at higher data rates.

Most hyper-scale data centers have used 100 Gigabit Ethernet (100GbE) links and are in the process of transitioning to 400 Gigabit Ethernet (400GbE) links to achieve higher throughput. Per Crehan Research, 400G deployments started in 2018 and will become routine in data centers by 2020 as rapid 400GbE adoption by cloud vendors enables dramatically lower unit pricing in the initial phase of its lifecycle.

As 400GbE deployments grow in hyper-scale data centers, the price-sensitive enterprise data center market will start taking advantage of the latest generation Ethernet technology and initiate their own transition from existing 10/40/100GbE networking to 400GbE.

Enterprise Applications for 400GbE

In enterprise networks, traffic from mobile devices has consistently migrated from mobile networks to Wi-Fi, placing added strain on wireless networking campus networks and branch offices in the enterprise. Enterprise IT organizations have been consistently struggling to increase network capacity to meet these mounting throughput requirements.

Simultaneously, developments in enterprise storage, such as all-flash arrays (AFAs) and Remote Direct Memory Access (RDMA) interfaces, are requiring dramatic improvements in network latencies and throughput. The benefits of these new storage technologies are completely dependent on the underlying network infrastructure.

New types of applications are also driving improvements in network performance. Throughput-sensitive rich media enterprise applications require higher bandwidth. Stored and live streaming video and digital marketing all benefit from 400GE becoming the de facto networking standard.

400GbE Standardization and Product Development

The Institute of Electrical and Electronics Engineers (IEEE) officially approved the 802.3bs standard for 200GbE and 400GbE on December 6, 2017. The standard defines the technical requirements to support 200 Gb/s and 400 Gb/s Ethernet data rates at distances for intra and inter-data center applications. Specifically, the IEEE 802.3bs project defines physical layer specifications for 400GbE operation over 100m, 500m, 2km, and 10km distances.

Beyond a four-fold performance boost, the transition to 400GbE promises both power and area savings, as 400GbE optical modules are expected to consume only 2.5x the power of a 100 Gigabit Ethernet links and maintain the same small form factors, increasing interconnect densities.

Consistent with 400GbE standardization, networking ASIC, router, test, and optical modules vendors have developed products supporting the 400GbE standard. For example, during 2018 and 2019, top-tier networking vendors formally launched products and made the news in the 400GbE market. Juniper Networks announced plans to roll out 400 Gigabit Ethernet (400GbE) in 2018 along with news of its QFX data center and MX WAN product lines. In 2019 Juniper Networks achieved an industry milestone for longest 400GbE deployment. While in October 2018, Arista Networks announced 400GbE support across its line of data center switches, in 2019 they delivered the new Arista 7800R family part of their highlighted Universal 400G Platforms for cloud network transformation. Similarly, Cisco launched 400GbE support across its line of switches targeting cloud and enterprise data centers in November, 2018.

Hardware Integrity: Combating State-Sponsored IP Theft

July 30, 2020
Brian Shannon—VP of Product

Previously Interface Masters posted a blog focused on State-Sponsored IP Theft along with the mounting evidence that a significant portion of the Asian hardware contains hidden data tracking capabilities. The objective for these attacks? Targeting and obtaining intellectual property from government, private enterprise and educational institutions. The attacks noted in the blog were the forerunners to those of the present.

One well-known example of a State-sponsored cyberattack that became news in October of 2018 is when Bloomberg uncovered a state-sponsored network hack enabled through 'off-the-shelf' Asian built network appliances. This attack exposed confidential data from more than thirty leading US based technology companies. (article: https://bit.ly/IMT-blog)

With cyberattacks increasing, news cyberattacks in the media provide a timeline of ongoing threats within every market that uses or shares data. Banking and finance have been hit especially hard with threats on financial investors and bank members' data. In 2019 U.S. Federal Reserve Chairman Jerome Powell noted that cyberattacks were the biggest risk for financial institutions. (article: https://reut.rs/2WYGM2g) The risks continue to impact financial institutions with news of continued cyberattacks.

The Cybersecurity & Infrastructure Security Agency (CISA), an agency in the Department of Homeland Security publishes recommendations and tips on preventing cyberattacks. Updated June 30, 2020, Security Tip ST18-001 notes that validating the integrity of hardware and software can improve the security of network infrastructure devices. Moreover, CISA recommends resellers to enforce integrity checks of the supply chain to validate hardware and software authenticity. (Security tip: https://us-cert.cisa.gov/ncas/tips/ST18-001)

Needing to ensure the integrity of network appliance hardware? Validate it directly with the seller designing the hardware, the software and controlling the supply chain. Customize it with that seller for a step further toward a secure network.

US Networking Appliance Hardware

Network hardware is the ideal target because all traffic must pass through these critical hardware devices. For cybersecurity professionals protecting their company's systems, it is important to understand where and how the network is designed, manufactured and travels through the supply chain. According to Nathan Palmer, a security researcher for Raytheon Technologies' Cyber Offensive and Defensive group, "Cyberattacks against hardware are becoming far more destructive and are more common." (article: https://bit.ly/HRDware)

"Cybersecurity is all about staying ahead of threats rather than managing them later," notes Gaurav Belani in his 5 Cybersecurity Threats to be aware of in 2020. With that in mind, Interface Masters network appliance hardware is always US designed and

manufactured. Extreme care is taken when designing and manufacturing our network solutions. All components are qualified and validated to ensure that the network hardware safely guards even the most sensitive data. Additionally, Interface Masters' custom services network solutions can be designed and manufactured to desired specifications with safeguards put in place.
(article: https://bit.ly/5cyber2020)

Tamper-Evident, Intrusion Resistant Networking Solutions (FIPS140-2)

September 14, 2020
Brian Shannon—VP of Product

News regarding security breaches is broadcast almost every day. Unfortunately, it is now likely an unauthorized entity will gain access to an organization's data. The Federal Information Processing Standards Publication 140-2 (FIPS 140-2) is a US Government Standard with a goal addressing such a security vulnerability and rendering proprietary data unusable should an unauthorized individual or entity get physical access to an organization's computing hardware.

FIPS Overview

The FIPS 140-2 standard entitled "Security Requirements for Cryptographic Modules" specifies the security requirements for a cryptographic module utilized within a security system for protecting sensitive information. FIPS was initially developed for the US government and private entities engaged in dealings with the government, companies have now embraced FIPS 140-2 and are beginning to embrace FIPS 140-3 as information security standards.

A cryptographic module is any combination of computer hardware, firmware or software that encrypts or decrypts data, applies a digital signature, applies a variety of authentication techniques, and/or uses random number generation. In simplest terms, it prevents unauthorized parties from being able to use sensitive data even if they get access to it.

The FIPS 140-2 standard has 4 levels, each level being a superset of a lower level and providing increasing security for proprietary data:

- Level 1 is the lowest FIPS 140-2 security level requiring at least one approved algorithm or security function to be used, such as data encryption, when sensitive data resides on a computer. Production grade closure with removable cover is acceptable.
- Level 2 augments data encryption by adding the requirement of physical tamper-evidence capabilities such as coatings, seals, and lock for the networking system. Requires additional of tamper evident seals on chassis and tamper evident coating on cryptographic module intelligence.
- Level 3 supplements Level 2 capabilities by preventing a malicious source from gaining access to critical security parameters (CSPs) e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs by zeroing CSPs in the case of unauthorized physical access to the computing device. Hardware must be significantly hardened to prevent and detect malicious entry.
- Level 4 is the highest level of FIPs 140-2 security and provides a comprehensive detection 'envelope' for all cryptographic modules with the goal of preventing, discovering, and countering all unsanctioned efforts at physical access.

FIPS 140-2 Level 3: Enabling Secure Management of Encryption Keys

Government agencies and enterprises that deal with storage and sharing of sensitive data require FIPS 140-2 compliant network and

security solutions. And agencies and businesses that want to assure the security of their sensitive data should be particularly focused on safeguarding their cryptographic keys, so they remain secure; such entities need FIPS 140-2 level 3.

Beyond the tamper-evident physical security features called for in FIPS 140-2 level 2, level 3 prevents malicious entities from gaining access to critical security parameters (CSP)s stored in the cryptographic module. Level 3 physical security features are meant to have a high likelihood of discovering and countering attempts at unauthorized physical access, use or modification of the cryptographic module. The physical security features may comprise the use of robust enclosures and tamper discovery and response features which reset all plaintext CSPs to zeros if the covers or doors of the cryptographic module are unsealed.

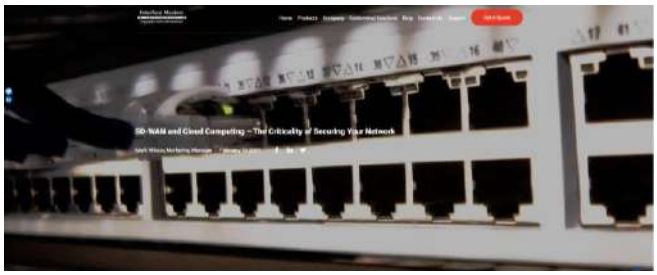
FIPS 140-2 level 3 requires identity-based authentication mechanisms involving authentication of the identity of an operator and verifying that the identified operator is authorized to assume a specific role and perform a corresponding set of services. For example, using identity-based authentication, the cryptographic device will allow authorized operators to open the seals and access the keys, but only after successfully authenticating.

Hardware Security Module (HSM) for FIPS 140-2 Level 3 Compliance

A hardware security module, or HSM, is a dedicated, FIPS 140-2 standards-compliant cryptographic device designed to protect sensitive data in transit, in use, and at rest using physical security measures, logical security controls, and strong encryption.

Interface Masters Technologies: Embedded Appliances Enabling Inherent Threat Defense

Interface Masters embedded appliances support both FIPS 140-2 Level 2 and FIPS 140-2 Level 3 designs. Interface Masters' HSM-enabled embedded appliances protect key storage utilizing tamper-evident capabilities and other physical security capabilities while meeting ever-greater encryption/decryption performance requirements, simplifying certificate management, and reducing compliance costs.



SD-WAN and Cloud Computing—The Criticality of Securing Your Network

February 17, 2021
Mark Wilson—Marketing Manager

Designing and building a secure network requires smart, informed decisions and knowing the network's risks. For some, securing a network drives them to paralysis by analysis. Too much analysis, overthinking and input to the point where nothing has been clearly secured. The decisions that go into securing a network today are complex with additional infrastructure, software or vendor requirements needed than were just a couple of years ago. In fact, just a few years ago most network data was secured behind a firewall – today more than 48% of business data is stored in the cloud (statista.com 2019). Threats have reached critical mass – it is now more important than ever to secure your critical network data.

Despite the growing amount of business data being stored, or the type of Cloud looking to be used (private cloud, hybrid or public) your network's security needs may be best secured with a simplified, infrastructure. A secure infrastructure permits an enterprise to take advantage of the benefits that a Software-Defined WAN provides. An enterprise employing a SD-WAN will see a network 100 times faster than a WAN at a cost savings of three times on a network built for scalability, flexibility and easier manageability. Combine it with the Cloud and you have a network you do not want to leave open to risk.

How is Your Network at Risk?

Adversarial nation states continue to aggressively and broadly use implanted hardware data-tracking devices, cyber tactics, and malware to obtain sensitive intellectual property from the United States and Europe – targeting confidential government, private enterprise and educational institution research data.

As one example, on October 24, 2018, Bloomberg uncovered a state-sponsored network hack enabled through 'off-the-shelf' Asian built network appliances. The hack exposed confidential data from more than thirty leading US based technology companies. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

SD-WAN infrastructure designers and appliance buyers should be mindful of the equipment being used.

U.S. designed and manufactured networking appliances along with robust software (and operating systems such as a standardized Linux O/S) assist in control and accountability over the infrastructure rollout or add-ons. Often employed at the edge of an SD-WAN Cloud network, the hardware that speeds this data for storage is made up of off-the-shelf solutions to optimize and ensure cost-effective results. This hardware is ready to run the customer's secure image. Financial branch offices, corporate campuses, or remote data centers reflect some of the local locations where this infrastructure is put in place and where network appliances

are playing an active part in the growing Cloud solution.

Additional protection for a network is afforded by employing standards like the Federal Information Processing Standards' FIPS 140-2, level 2 and level 3 which are increasingly becoming the choice for securing a device, even for those not mandated by the federal government. FIPS 140-2 compliancy is mandatory for use in federal government departments that collect, store, transfer, share and disseminate sensitive information. This includes contractors, service providers, networking and providers associated with cloud services outside of the government. Hardware Security Module-enabled embedded appliances (with encryption) protect critical storage utilizing tamper-evident capabilities and other physical security capabilities. These devices meet ever-greater encryption/decryption performance requirements and provide simplified certificate management. Devices designed and manufactured in the U.S. enable the additional FIPS 140-2 standard to be added to a device assuring the secure criticality of a network system from infrastructure through the Cloud.

Secure Foundation

Because adversarial nation states compromise networking hardware, resulting in risk to your SD-WAN Cloud computing, it is critical to emphasize the importance of securing key hardware and software for your networking needs. Interface Masters Technologies' embedded network appliances provide scalable network security platforms that readily meet the design, hardware and software foundation required of security-assured network appliances. Providing a secure start with your software eliminates many problems. Design, manufacturing and software create the security needed. Finally, Interface Masters currently offers a full range of US designed and US manufactured appliances based on a wide range of CPU and switch fabric technologies supporting high-performance threat protection.

Network Appliance: Why Custom?

August 26, 2020
Mark Wilson—Marketing Manager

OEMs, Fortune 100 and startups know that network appliances running security applications are the vigilant watchmen of a network. Designed and built to reside on a network with other hardware, software and services, these appliances can be centralized for a cost-effective security-focused network management solution. Customize the design and build and that appliance is custom-made and ready for unified threat management (UTM), intrusion detection systems (IDS), intrusion prevention system(IPS), data loss prevention (DLP), and more.

Why choose a custom appliance for security as an OEM, Fortune 100 or startup? Here are a few reasons to consider custom for your new solution.

1. Current appliance is not secure. A custom appliance designed and manufactured in the U.S.A will ensure the integrity of the hardware vs a State-sponsored, network hacking, enabled through ‘off-the-shelf’ nefarious state-built network appliances.
2. Changing needs. With new demands being placed on the network, issues like increased remote workers or seeing employees double after a company merger/transition? Custom features help meet changing needs, such as more storage, faster connections, designing in precision time protocol (PTP) or integrating a trusted platform module (TPM) and other functionality for increased security.
3. Increased productivity. Fast hardware acts and reacts quickly to secure the network. Slow hardware adversely affects a system’s overall productivity and can increase the need for support. Fast or slow, a custom setup will provide flexibility to enable made-to-order productivity.

Custom solutions are a scalable approach toward meeting a variety of unique network needs for different size companies. For a network appliance, this scalable approach provides a cost-effective means of getting precisely what is needed regardless of whether it is in a unified threat management (UTM), intrusion detection systems (IDS), intrusion prevention system (IPS), data loss prevention (DLP), or having the hardware to choose the security application. The right solution will have hardware integrity, have an active lifespan, meet changing needs, and be productive.

Providing Customization / About Us

For over 25 years, Interface Masters Technologies has been providing customization services to OEMs, Fortune 100, and startup companies along with off-the-shelf innovative networking solutions. We are headquartered in San Jose, California in the heart of Silicon Valley where we proudly design and manufacture all products. Based on MIPS, ARM, PowerPC and x86 processors, and switch fabrics up to 12.8T, Interface Masters appliance models enable OEMs to significantly reduce time-to-market with reliable, pre-tested, pre-integrated, long-life appliance solutions that

can meet the most challenging networking requirements. Learn more about us at www.interfacemasters.com

Looking for the benefits of custom, but want off-the-shelf? Here are a couple of solutions to consider:

Tahoe 2624 a semi-modular 1U switch appliance based on Barefoot Tofino® high-speed switch fabric and managed by an Intel x86 control plane.

Tahoe 8724 a highly-flexible 1U networking appliance designed for enterprise installations. Tahoe 8724 is based on Cavium 64-bit MIPS technology

About Interface Masters Technologies

For 25 years Interface Masters Technologies has been providing off-the-shelf innovative networking solutions with customization services to OEMs, Fortune 100, and startup companies. Our headquarters is in San Jose, California in the heart of Silicon Valley where we are proud to design and manufacture all our products. Based on MIPS, ARM, PowerPC and x86 processors, Interface Masters appliance models enable OEMs to significantly reduce time-to-market with reliable, pre-tested and pre-integrated appliance solutions that can meet the most challenging networking requirements.

What We Do
Interface Masters Technologies develops and manufactures highly innovative, low OPEX and power efficient products for SDN, IoT and embedded markets. Customer service and attention to detail is a hallmark of Interface Masters Technologies.

Off-The-Shelf Products
Interface Masters offers a wide variety of off-the-shelf ARM, MIPS and X86 appliances, smart NICs, and high port density NICs. Our standard products are available under the Sierra and Tahoe brand names.

The many configuration options of our product lines offer the opportunity to create a unique product solution for every customer. Interface Masters' long history of providing high reliability systems is embedded in the design. We update our existing products or design from ground up to meet your product requirements.

As a supplier to Tier 1 OEMs and start-up companies, we specialize in private labeling and full design, customization and manufacturing services. We work closely with our customers to take their "back of the napkin" concept through the design, prototyping and certification stages, culminating in turn-key manufacturing and logistics. Interface Masters provides documentation, operating system and software support and complete diagnostics allowing our customers to bring their ideas to market in a cost-effective and timely manner.

Our Team
Interface Masters Technologies has a team of intelligent, highly skilled, capable, and dedicated individuals who work together seamlessly. From our engineering team to our operations, to our sales and marketing, we all share one goal – to make our customers happy. This mantra has been the core of our success for over twenty-five years.