Bivio 2000
Disruptive Technology to Secure the DoD Network Environment

A Strategic Shift in Sensor Capabilities

Uncompromising performance. Unmatched flexibility.
Executive Overview

Bivio Networks has created a new disruptive technology platform that will change the way DoD and other Federal agency IA personnel think of high-performance, defense-in-depth, networking strategies.

Founded in 2000, Bivio Networks has evolved into the leading supplier of next generation packet handling platforms and sells its multi-gigabit network appliances to network infrastructure providers, as an OEM business model, and to the Federal Government. Bivio’s products are unique in their ability to combine fully-programmable, deep-packet processing with deterministic, multi-gigabit network throughput for any network service, and, thus, represent an optimal appliance hardware platform for a new generation of software-based network applications that Bivio’s partners are bringing to market. Bivio’s list of OEM partners includes such notable security vendors such as: SourceFire, NFR Security, Demarc, SECUi, and Arbor Networks, with more and more security vendors evaluating the platform.

Some of the highlights of key product capabilities:

• A single operational platform that allows for maximum flexibility in matching the needs of the overall IA/CND mission, even as the specific mission goals change.
• The ability to share the same data stream in an inline (or passive or both) manner with multiple IO/IA applications; can be a mix of COTS and GOTS applications on the same 2U Platform
• The ability to more efficiently leverage multiple sensors through a single data stream provides greater informational awareness and greatly contributes to the INFOSEC capabilities and Information Superiority goals of DoD, while reducing overall operational costs
• The ability to securely operate both GOTS and COTS applications on the same operational platform, without memory or resource contentions, increases productivity while saving power & rack space at each location

The Challenge

For the warfighter, correlating data and information from multiple sources for a common operational picture of the battlefield is often a difficult task. The Department of Defense’s resolution to this problem is Net-Centricity, which will ease the flow of information between sensors, computational nodes, and even different communication grids. When this information is consolidated and fused in real-time, the result may be a tighter sensor-to-shooter gap and much faster deployment of key assets—space satellites, battleships, attack aircraft, submarines, ground vehicles, and teams of special forces soldiers—by all branches of the armed services.

The Defense Information Systems Agency (DISA) is transforming to better support DoD’s strategic goal of Net-Centricity. One of DISA’s best-known initiatives supporting Net-Centricity, the Global Information Grid-Bandwidth Expansion (GIG-BE) program, will vastly improve the current network infrastructure. There are other significant initiatives specifically in the area of Information Assurance (IA) that will contribute to a secure Net-Centric environment. As Net-Centricity evolves, access to the network and the information it supports will become more ubiquitous than ever.

Along with that comes:

• The inherent threat imposed by a larger user population
• A greater appetite for mission-critical information
• The necessity to understand how the bandwidth is being used and who is using it
• The ability to re-program network IA sensors for different IA missions without having to keep upgrading, purchasing more, or re-racking the servers

Likewise, on the Federal Civilian side, the issues that agencies such as DHS is dealing with from an Information Assurance perspective, are very similar to what the DoD organizations are dealing with on a daily basis:
• Both need to protect their networks
• Both need as close to real-time information as possible (Situational Awareness) to: Identify, assess and mitigate any asymmetric threat thrown at the targeted network(s)
• Both are susceptible to the same threats by virtue of the fact that they are both citizens of the Internet
• Both have limited resources and space/power requirements

In some ways, DHS has a more difficult time than DoD because of a couple of different factors:
• They don’t have the Global Information Grid (GiG) infrastructure that allows the DoD to better control the data flows and access point to the internet
• The DHS has to deal with many access points to the web with many different agencies and sub-agencies having their own access -- too many holes from a security standpoint
• It is very challenging to penetrate the varying cultures and political realities involved in working with different organizations

DHS is leveraging some of the DoD developed IA tools to help protect their networks and it looks like they are also beginning to evaluate their IA needs from a more security-centric perspective. They have to not only deal with FISMA scores, HSPD-12 compliance, but they have the additional difficult task of providing oversight for the level of network protection that will not get compromised by the next hacker or application-based worm, all with the same number of resources.

The most innovative and fastest growing network applications in the areas of Information Assurance, security, VoIP (voice over IP), multimedia, wireless, and IPv6 are increasingly being implemented as software applications running on traditional “intel-based” hardware, indicating a fundamental change in the way network services are implemented. But, these emerging software-based, packet-handling applications also demand new requirements from the networking platforms used to implement them. Chief among these new challenges is the demand for multi-dimensional scaling capabilities; led by increasing deep-packet inspection, network bandwidth, and application agility requirements – a software-driven, programmable network.

A programmable network is distinguished from any other networking environment by the fact that it can be programmed from a minimal set of APIs from which one can ideally compose an infinite spectrum of higher-level services. The need for programmable networks stems from the demand to rapidly create, deploy, and manage these new services and applications in a dynamic way and, most likely, run multiple security applications on the same programmable platform.

Existing hardware has traditionally focused on scaling in a single dimension. For example, networking technology has focused on bandwidth scaling, while server technology has focused on computational scaling. The result has been an increasing gap between the demands of packet handling applications and the capabilities of the existing platforms to satisfy them. In essence, the existing “hardware” platforms have become a network bottleneck in high-speed networks having to “share” memory resources, thus increasing overhead and greatly decreasing performance. In addition, it is next to impossible to create the necessary programmable network environment necessary in today’s Net-Centric environment with existing Intel or ASIC-based platforms.

As 1GE and 10GE establish themselves as the new connectivity standard in the networking infrastructure, these bottlenecks will only increase unless a new architectural approach emerges which is capable of reconciling what traditionally have constituted mutually exclusive requirements in networking: performance and flexibility.
The Solution

The Bivio 2000 is a programmable network appliance featuring a groundbreaking architecture specifically optimized for wire-speed execution of emerging network services that increasingly demand deep packet processing, combined with high network throughput.

The uniqueness of the low profile (2U form factor) with 6 RISC-based Linux servers, dedicated network processor, 10Gb full-duplex switch and load balancer, is purpose-built for high-performance security, deep packet processing, analysis (lawful intercept) and network applications. This innovative architectural approach delivers a new level of network capabilities and scalability for all DoD and other Federal organizations not currently available from any other vendor.

Bivio’s innovative architectural approach to building a network appliance delivers on the requirement for multi-dimensional scaling in future networking infrastructure, making highly adaptable, program- mable high performance networks a reality. The system delivers any networking service with unmatched flexibility and scalability, vastly outperforming other architectural alternatives.

Any Linux network application can be easily ported onto the Bivio architecture and accelerated to run at multi-gigabit speeds. The programmable nature of the entire networking and application plane results in the system’s ability to adapt to the ever-changing nature of the network infrastructure – new applications, changing protocols, as well as the platform’s ability to deliver on the long- standing promise of service convergence.

BIVIO’S UNIQUE CAPABILITIES

The uniqueness of the low profile (2U form factor) with 6 RISC-based Linux servers, purpose-built for high-performance, deep packet processing, inspection and analysis (lawful intercept) and network applications, provides a new level of network capabilities for the Department of Defense that cannot be sourced by any other vendor or manufacturer.

In addition, no other vendor can offer:

- 6 RISC-based Linux servers in this form factor that can run multiple classes of network security or other open source GOTS/COTS applications for multiple organizations
- Stackable/Scalable CPU and network architecture
- Separation of the Network Processor and Load balancer in the same appliance with no shared memory resources, which eliminates network traffic bottlenecks and increases security
- Up to 64,000 queues in the network processor to defend against DDOS and other asymmetric network attacks
- Full IPv6 support today
- Bivio Networks is 100% made in USA (both hardware and software development).

The Bivio 2000 can support a wide range of mission critical network infrastructure and deep packet inspection applications and architectures including:

- Security
- Traffic management
- Compression
- Acceleration (SSL, TCP, XML)
- Layer 4-7 server load balancing
- Lawful Intercept
- Performance monitoring and correlation
- IPv6
• Routing
• Secure VoIP infrastructure
• Wireless infrastructure
• Airborne/Naval Operations

**BIVIO 2000 FEATURES**

- Powerful computation platform that enables true wire-speed for any service at any packet size
- Cluster of up to 6 RISC-based Linux servers in 2U form factor (can be stacked for more network/processing performance)
- Deep packet inspection and Wire-speed programmable forwarding operations
- Multi-dimensional scaling and hardware acceleration
- Dedicated network processor and Network Processing API with Dynamic data path reprogramming capabilities
- Dedicated network load balancer purpose built in the B2000 appliance
- Flow "cut-through", blocking, pre & post processing
- Low power consumption

![](image)

**BIVIO 2000 BENEFITS**

**True Wire-Speed, Multi-Gigabit Performance:** The unique capabilities of the Bivio 2000 system architecture ensures all deep packet handling services on all interfaces are processed and forwarded at line rate, achieving optimal performance across the spectrum of packet sizes.

**Advanced Traffic Management:** The Bivio 2000 enables hierarchical traffic and user class prioritization and bandwidth shaping on a per flow, per customer, and per traffic type basis. All QoS features are completely programmable and implemented via sophisticated nested, standard queuing algorithms and include the following capabilities:
- 4 Gb/s aggregate throughput
- Wire-speed programmable forwarding operations
- Packet inspection & classification
- Modification & transformation (NAT)
- Traffic Management (QoS)

**Scalable Application Processing:** The Bivio 2000 provides unmatched application processing power in a compact 2U form factor, and unlimited processing performance through stacking technology.

**Service Agility:** Any Linux-based networking application can be quickly ported to take full advantage of the Bivio 2000 system performance by using the BivioAPI, thus achieving instant performance differentiation. Due to its fully programmable packet forwarding and application processing subsystems, the Bivio 2000’s application flexibility is unmatched by any Intel-based product.

**High Availability:** The Bivio 2000 supports active/active or active/standby system configurations that eliminate any single points of failure to deliver non-stop services, resulting in the ability to support even the most mission critical applications for the Department of Defense.
Summary
Bivio Networks, Inc. provides the next-generation network hardware appliance platform specifically tailored to the requirements of packet handling in high-performance networks. The platform delivers a standard Linux-based execution environment augmented by a comprehensive set of common networking and management function that allows for both COTS and GOTS applications to reside and operate at wire-speed in the same appliance, depending on the operational mission.

Bivio delivers the scalable processing power to support DoD and Civilian Federal Government Information Assurance/Computer Network Defense requirements and also provides greater overall price-performance than any other COTS solution on the market today.

From “Mission Critical” to “Mission Capable!”
About Bivio Networks

Bivio Networks has developed an award-winning, deep-packet inspection and processing platform that combines unparalleled scaling of network performance, processing power, and application agility. Bivio’s network appliance platform features a groundbreaking architecture specifically optimized for wire-speed execution of emerging network services that increasingly demand deep packet processing combined with high network throughput. Based on open industry standards, Bivio Networks fuses unmatched flexibility with uncompromising performance to enable its customers to overcome existing bottlenecks and deliver the foundation of the next generation network infrastructure.