# nGenius 6002 Packet Flow Switch

## Hardware-accelerated Performance, All-Inclusive Features

### HIGHLIGHTS

- 3 Rackmount Unit chassis with highly available, hot-swappable architecture
- 1.2Tbps throughput and non-blocking switching fabric
- Up to 2 hot-swappable blades
- Up to 120 non-blocking ports of 10GE per chassis
- Up to 30 non-blocking ports of 40GE per chassis
- Up to 12 non-blocking ports of 100GE per chassis
- Line rate performance on all features, including rate conversion, aggregation, replication, filtering, load balancing, port tagging, time stamping, de-duplication, protocol stripping and / or de-encapsulation, and conditional masking and slicing
- IP Tunnel termination (e.g. ERSPAN, NVGRE)
- Active inline traffic forwarding for active security or WAN optimization with customizable health checks
- Flexible policy defined triggers for event handling and high availability scenarios
- Intelligent fully meshed stacking / interconnect (pfsMesh)
- Management via command line, NETCONF, and graphical user interfaces for local and remote access
- Designed for NEBS III Compliance

### Product Description

The nGenius® 6000 Series Packet Flow Switch (PFS) is a large-scale, high-performance, high-density blade and chassis system that bridges the gap between 1G, 10G, 40G, and 100G Ethernet networks and tools.

The nGenius 6002 Packet Flow Switch model is designed for NEBS level III compliance and consists of a 3RU chassis that supports up to two line cards with each line card supporting up to 600 Gbps throughout – for a chassis total throughput of 1.2Tbps and up to 120 ports. All ports on each line card are enabled by default with each port configurable as an input port, intermediate (service) port, or output port.

With the NETSCOUT® pfsMesh, a self-organizing architecture, traffic capture devices can be deployed in a redundant, low-latency meshed architecture for dynamic and fault-tolerant visibility that can scale to over 4000[1] ports across LAN and WAN environments.

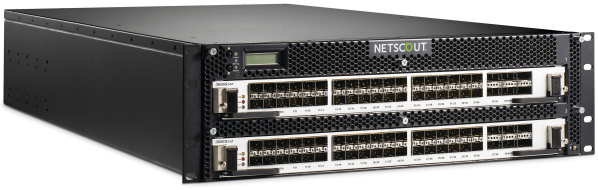
### Delivery Optimization

Beyond scalable aggregation and speed conversion, nGenius 6002 Packet Flow Switch supports line rate hardware-based packet filtering and session-based load balancing of packets to tools.

Hardware-based, user-independent filtering allows traffic to be distinguished according to source and/or destination MAC address, VLAN inner/outer ID, IP address, SCTP/TCP/UDP port, as well as by specific protocols, such as HTTP, VoIP (SIP, RTP), and others. A custom filter enables more granular specification, specifically within the payload of a packet. Filters can be ingress, egress, and overlapping.

Flow-aware load balancing provides control of traffic distribution to monitoring tools, increasing output capacity while maintaining session integrity. For example, a 100G network can be captured and automatically balanced across multiple 10G monitoring tool ports based on user-defined session criteria. Flow-aware load balancing can operate in tandem with hardware-based filtering or independently.

[1] Total number of ports in a single pfsMesh is dependent on quantity and complexity of filtering.




| | |
|---|---|
| **36S6Qstd Line Card** | 36 x 1Gb/10Gb SFP+ Ports & 6 x 40Gb QSFP+ Ports |
| **15Qstd Line Card** | 15 x 40Gb QSFP+ Ports |
| **6Cstd Line Card** | 6 x 100Gb CFP2 Ports |
| **6Q28std Line Card** | 6 x 100Gb QSFP28 Ports |
| **40Sadv Line Card** | 40 x 1Gb/10Gb SFP+ Advanced Ports and Advanced feature packages |

### Security Optimization

To take action as offenders and bad actors are detected active inline security tools need to see and handle all the traffic that needs to be inspected.

nGenius packet flow switches with inline tool chaining allow aggregation, filtering, and load-balancing of actual network traffic toward multiple inline security applications whilst adding only a single device to each network link while providing application-specific health checks (not just ICMP heartbeats) to ensure the active security tools are connected and functioning properly. The deployment of policy-based triggering facilitates automatic failure scenarios including high availability. The deployment of policy-based triggering facilitates automatic failure scenarios including high availability. External bypass TAPs can be used to ensure that the security policies are adhered to during power failure.

### Management

nGenius 6002 Packet Flow Switch can be locally managed via a serial console and remotely managed via a Web GUI, CLI, and NETCONF XML API using HTTP, HTTPS, or SSH. The system can be monitored via Syslog and SNMP. Each device ships with an intuitive and easy to use graphical element management system (EMS) out of the box. Simply point a web browser at the nGenius 6002 Packet Flow Switch to manage and let the web-based user interface (WebUI) power the packet flow system.

The devices support field software updates for maintenance and feature or performance enhancements. nGenius 6002 Packet Flow Switch can be centrally managed and configured.

### Virtual Access

For accessing traffic that is completely virtualized and never makes it onto a physical network, traffic can be mirrored and forwarded from the virtual network to the physical network using tunneling protocols such as NVGRE (L2GRE) or ERSPAN which encapsulate the traffic of interest. The nGenius 6002 Packet Flow Switch can be the destination of these tunnels and terminate the tunnel, and the traffic can then be forwarded on to monitoring applications either as is or de-encapsulated.

### Power and Compliance

Designed for NEBS III compliance, nGenius 6002 Packet Flow Switch supports hot-swappable power supplies, fans, air filters, and line cards. Redundant power allows seamless transitions between power systems to ensure uptime.

## Features and Benefits

| Features | Benefits |
|---|---|
| **Up to 120 line-rate ports in 3RU**<br>• 72 x 1G/10G<br>• 120 x 10G<br>• 30 x 40G<br>• 12 x 100G<br>• Mix of 1G/10G/40G/100G<br><br>Compatible with SFP, SFP+, QSFP+, QSFP28, and CFP2 MSA compliant transceivers | **High density system:**<br>• Reduces per-port cost and increases flexibility<br>• Condenses the nGenius PFS footprint (rack space)<br>• Reduces power consumption<br>• Simplifies management |
| **I/O configurable**<br>• Full flexibility in selecting ports for network access, intermediate service, interconnect, or monitor output<br>• Dual network access & monitor output port class<br>• IP tunnel (e.g. ERSPAN, GRE, NVGRE/L2GRE) termination | • Enables agile response to monitoring infrastructure changes<br>• Facilitates effectively doubled capacity for input and output<br>• Allows virtualized traffic to be forwarded over an IP network to PFS ingress ports, and then forwarded onto monitoring devices as is, or de-encapsulated[2] |
| **Selective Aggregation**<br>• Fully flexible any-to-any port mapping | • Enables large scale aggregation to maximize tool visibility<br>• Addresses asymmetrical routing issues |
| **Hardware-based Filtering**<br>• User-independent<br>• OSI Layers 2 - 7<br>• Custom offset (user-defined)<br>• Ingress<br>• Egress<br>• Overlapping | • Allows only "traffic of interest" to be forwarded to each tool, which increases tool efficiency and reduces the number of required tool interfaces |
| **Session-based/flow-aware load balancing**<br>• Distributes traffic load across multiple instances of a tool or tool port<br>• Maintains session stickiness for full conversations<br>• Up to 64 ports per group | • Prevents oversubscription of monitoring tools and security systems – eliminating blind spots without sacrificing session integrity<br>• 40G and 100G copied traffic can be easily distributed across multiple lower speed tool ports, allowing users to preserve existing tool investments |
| **Monitor traffic port tagging**<br>• Provides identification of traffic based on source network/link using VLAN tagging or Port stamping | • Users can quickly and precisely pinpoint where an issue, such as latency or security event, is occurring in the network.<br>• Provides options for different tools to access port identification |
| **Microburst mitigation**<br>• High Data Burst Buffering | • Prevents packet loss resulting from aggregation or speed conversion of bursty traffic (microbursts) |
| **Intelligent Stacking (pStack)**<br>• Enables pMesh architecture for local and remote of up to 256[3] PFS devices as a single redundant system<br>• Works over LAN and WAN connections | • Ensures highly available monitoring<br>• Scales visibility with network infrastructure and new tools<br>• Ensures delivery of traffic across LAN or WAN to tools |

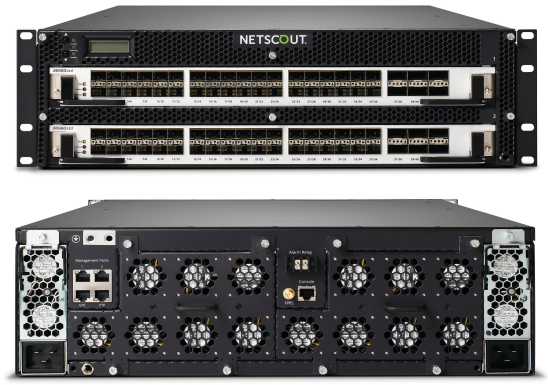
[2] Requires Advanced line card.

| Features | Benefits |
|---|---|
| **Hardware-based Advanced Packet Optimization**<br>• Accurate time stamping (from 4ns) for latency analysis; supports GPS, PTP, 1PPS, and NTP for accurate timing synchronization<br>• Protocol header removal (stripping and de-encapsulation) for broader tool support; supports removal of ERSPAN, Fabric Path, GRE, GTP, MAC-in-MAC, MPLS, NVGRE, TRILL, VLAN, VN-tag, & VXLAN protocol headers, as well as almost any other protocol used for tunneling in networks<br>• Conditional packet masking for selective payload obfuscation; supports masking from anywhere up to 9000 bytes into the packet<br>• Conditional packet masking for selective payload obfuscation; supports data masking from anywhere up to 4000 bytes into the packet<br>• Adaptive load-balancing on inner L2-L4 headers of tagged/encapsulated traffic; supports ERSPAN, Fabric Path, GRE, GTP, MAC-in-MAC, MPLS, NVGRE, TRILL, VLAN, VN-tag, & VXLAN protocol headers, as well as almost any other protocol used for tunneling in networks<br>• Deduplication at line-rate for removing duplicate packets; supports numerous packet comparison criteria and user-defined duplicate detection window up to 4 seconds | • Provides time-of-capture data<br>• Allows any and all tools to monitor the same network traffic<br>• Enables tools to perform faster, more effective analysis<br>• Facilitates regulatory data privacy compliance<br>• Ensures correct balancing and forwarding of all traffic types<br>• Reduces traffic volume to be backhauled to tools |
| **Policy-based event triggering and actions**<br>• Dynamic traffic redirection based on occurrence of events<br>• Send alerts when specific events occur | • Reduces management overhead and enables faster response times to incidents |
| **Active inline access and forwarding**<br>• Aggregation of multiple network segments<br>• Filtering and load balancing towards applications/tools<br>• Easy to configure simple and complex inline tool chaining<br>• Customizable health check packets for "positive" (return) and "negative" (no return) checks | • Removes multiple points of failure<br>• Gains visibility for a single inline security tool (e.g. security proxy, IPS) and/or WAN optimization<br>• Easy deployment of layered security<br>• Removes multiple points of failure by fully exercising tools |
| **Local and remote management**<br>• XML API<br>• CLI (SSH)<br>• GUI (HTTP/HTTPS)<br>• SNMP<br>• Syslog (transport over UDP, TCP, or TLS) | • Easy to use via graphical interfaces or via CLI for users already familiar with Cisco<br>• Easy integration with applications using CLI or NETCONF XML API<br>• Alerts can be received by any Syslog server or SNMP manager, with option for sending securely |
| **Role-based Access**<br>• Multiple user and user role support<br>• Flexible user/role defined privileges, unique screen views, and access control | • Conforms to security policy needs of IT organizations |
| **AAA security with Remote (RADIUS and/or TACACS+)** | • Meets authentication policy needs of IT organizations and Local authentication |
| **Hot swappable line cards and fan trays** | • Maintains high availability for 99.999% uptime (five-9s) or better<br>• Scales to meet changing needs |
| **Redundant, universal power feed units**<br>• AC and DC hot-swappable options | • Maintains high availability for 99.999% uptime (five-9s) or better |
| **Traffic Statistics**<br>• Port-level packet and throughput metrics, including overflow drops, bad packets, etc.<br>• Flow level packet and throughput metrics | • Visibility into network and tool port activity<br>• Visibility into traffic type activity |

[3] Total number of packet flow switches in a single pMesh is dependent on device sizes, number of ports, and complexity of filtering.

# nGenius 6002 Packet Flow Switch

## Chassis and Blades




### Base Chassis

Base 2-slot nGenius 6002 Packet Flow Switch chassis, including

- 2 x Management port
- 1 x Serial console port
- 1 x GPS port
- 1 x PTP port
- 1 x 1PPS port
- 2 x Power supply/entry units (redundant)
- 2 x Fan tray

### 36S6Qstd Line Card

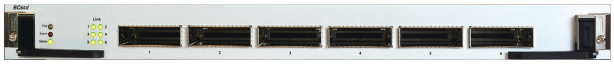
36 x 10G/1G SFP+ and 6 x 40G QSFP+ standard edition line card for nGenius PFS 6000

- Allows up to 72x 10G/1G and 60 x 40G ports, or 600 x 10G (using breakouts for 40G) ports with base feature set

### 15Qstd

15 x 40G QSFP+ standard edition line card for nGenius PFS 6000

- Allows up to 30 x 40G ports with base feature set



### 6Cstd Line Card

6 x 100G CFP2 standard edition line card for nGenius PFS 6000

- Allows up to 12x 100G ports with base feature set

### 6Q28std Line Card

- 6 x 100G QSFP28 standard edition line card for nGenius PFS 6000
- Allows up to 12 x 100G ports with base feature set

### 40Sadv-R Line Card

40 x 10G/1G SFP+ Advanced edition line card for nGenius PFS 6000

- Allows up to 80 x 10G/1G ports with advanced and base feature sets

### DC Power Entry Unit

DC Power entry unit (included in base chassis)

### AC Power Supply Unit

AC Power supply unit (included in base chassis)

## PRODUCT SPECIFICATIONS

### Physical Characteristics

| Component | Height | Width | Depth | Weight |
|---|---|---|---|---|
| **Base Chassis** | 3RU<br>5.2 in (133 mm) | 17.5 in (446 mm) | 29.9 in (760 mm) | 49 lb ( 22.2kg)<br>70 lb (31.8 kg)<br>fully populated |
| **36S6Qstd Line Card** | 16.5 in (419 mm) | 1.5 in (38.2 mm) | 17.5 in (445 mm) | 9.3 lb (4.2 kg) |
| **15Qstd Line Card** | 16.5 in (419 mm) | 1.5 in (38.2 mm) | 17.5 in (445 mm) | 9.2 lb (4.2 kg) |
| **6Cstd Line Card** | 16.5 in (419 mm) | 1.5 in (38.2 mm) | 17.5 in (445 mm) | 9.1 lb (4.1 kg) |
| **6Q28std Line Card** | 16.5 in (419 mm) | 1.5 in (38.2 mm) | 17.5 in (445 mm) | 9.1 lb (4.1 kg) |
| **40Sadv-R Line Card** | 16.5 in (419 mm) | 1.5 in (38.2 mm) | 17.5 in (445 mm) | 10.4 lb (4.7 kg) |
| **AC Power Supply Unit** | 4.6 in (116 mm) | 1.6 in (41 mm) | 11.8 in (300 mm) | 5 lb (2.3 kg) |
| **DC Power Entry Unit** | 4.6 in (116 mm) | 1.6 in (41 mm) | 11.8 in (300 mm) | 4 lb (1.8 kg) |

### Power Specification

| Component | Specifications |
|---|---|
| **Base Chassis** | Empty chassis: 300 W (1,024 BTU)<br>Fully loaded: 1,600 W (5,459 BTU) |
| **36S6Qstd Line Card** | 200 W typical, 300W max (1,024 BTU) |
| **15Qstd Line Card** | 220W typical, 320 W max (1,092 BTU) |
| **6Cstd Line Card** | 240 W typical, 340 W max (1,160 BTU) |
| **6Q28std Line Card** | 230 W typical, 330 W max (1,126 BTU) |
| **40Sadv-R Line Card** | 330 W typical, 430 W max (1,467 BTU) |
| **AC Power Supply Unit** | 100 to199 V AC, 14 A max. 200 to 240 V AC, 10.5 A max. 90% efficiency |
| **DC Power Entry Unit** | -40V to -60 V DC, 40 A max. |

## Environmental Specification

| | |
|---|---|
| **Operating Temperature** | 32° to 113°F (0° to 45°C) |
| **Storage Temperature** | -4° to 212°F (-20° to 100°C) |
| **Operating Humidity** | 20% - 80% (non-condensing) |
| **Storage Humidity** | 5% – 95%, (non-condensing) |

## Electrical and Optical Characteristics

| Aspect | |
|---|---|
| **Data Rates** | 1Gbps, 10Gbps, 40Gbps, 100Gbps |
| **Interface Types** | Ethernet: 1000 Base-T, 1000 Base-SX, 1000 Base-LX, 1000 Base-ZX, 10G Base-T, 10G Base-LR, 10G Base-ER, 10G Base-ZR, 10G Base-SR, 40G Base-SR4, 40G Base-LR4, 40G Base-ER4, Cisco 40G Base-SR2 BiDi, 100Gbase-SR4, 100Gbase-LR4, 100Gbase-SR10, 100Gbase-ER4 |
| **Propagation Delay** | < 1.6µs across each 20-port group,<br>< 3.2µs across 20-port groups and across cards |

## Standards and Compliance

| Standard | Specification(s) |
|---|---|
| **Ethernet** | IEEE 802.3, IEEE 802.3ba, IEEE 802.3ab, IEEE 802.3ae, IEEE 802.3z |
| **VLAN** | IEEE 802.1Q, IEEE 802.1ad |
| **ARP** | IETF RFC 826 |
| **IP** | IETF RFC 791, 2460 |
| **UDP** | IETF RFC 768 |
| **TCP** | IETF RFC 793 |
| **FTP** | IETF RFC 959, 2228 |
| **SSH** | IETF RFC 4251, 4252, 4253 |
| **HTTP** | IETF RFC 2616, 2817 |
| **TLS (SSL)** | IETF RFC 4492, 5246 |
| **SNMP** | IETF RFC 1157, 3411-3418 |
| **Syslog** | IETF RFC 5424 |
| **RADIUS** | IETF RFC 2865, 2866 |
| **TACACS+** | IETF RFC 1492 |

| Standard | Specification(s) |
|---|---|
| **NTP** | IETF RFC 5905 |
| **PTP** | IEEE 1588-2008 |
| **EMC** | FCC Part 15 Class A, ICES 003, KN 32, KN 35, VCCI Class A, CNS 13438 Class A, EN55032 Class A, EN55024 Class A, EN61000-3-2, EN61000-3-3, EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN61000-4-11 |
| **Safety** | UL 60950-1, CSA C22.2 EN 60950-1, IEC-60950-1 |
| **NEBS Level 3** | GR-63, GR-1089 |
| **RoHS** | RoHS 6, EU directive 2002/95/EC |
| **REACH** | EC 1907/2006, 121/2006 |

## Ordering Information

| Part Numbers | Description |
|---|---|
| **6002NA000000** | nGenius 6000 Series Packet Flow Switch - 6002 chassis (2-slot), AC power |
| **6002ND000000** | nGenius 6000 Series Packet Flow Switch - 6002 chassis (2-slot), DC power |
| **6000NBAFA100** | 6000 Series - 36S6Qstd Line Card with 36 x 1Gb/10Gb Ports & 6 x 40Gb Ports |
| **6000NBFK4100** | 6000 Series - 15Qstd Line Card with 15 x 40Gb Ports |
| **6000NBBGB100** | 6000 Series - 6Cstd Line Card with 6 x 100Gb CFP2 Ports |
| **6000NBBGE100** | 6000 Series - 6Q28std Line Card with 6 x 100Gb QSFP28 Ports |
| **6000NBCJ2L0A** | 6000 Series - 40Sadv Line Card with 40 x 1Gb/10Gb Ports and 3x Advanced feature packages |

For transceivers, please refer to the list of transceivers offered by NETSCOUT Systems.

## MORE INFORMATION OR QUESTIONS

For more information or any questions, about NETSCOUT Systems or its products, please contact your local representative, call +1 800-309-4804 or +1 978-614-4000, or go to www.netscout.com.

NETSCOUT

**Corporate Headquarters**
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

**Sales Information**
Toll Free US: 800-309-4804
(International numbers below)

**Product Support**
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us



PFSPDS_011_EN-1901 11/2019