



**Intrusion Detection. Application Management.
Forensic Collection. Security Auditing.
Real-Time Analysis. Access Management...**

... Enterprises are deploying thousands of new security and network management tools every day. But, are they being used effectively?

How are organizations making sure these critical devices get all the data they need in the most cost-effective, efficient, and secure way possible?

How do they intend to access and manage the increasing number of network tools and the massive amounts of data each collects?

The Modern Network

Today, almost every network is mission critical and needs to be available 24x7. Demand for higher performance and greater bandwidth is constantly increasing. Downtime, security breaches, and non-compliance with important standards and regulations are simply unacceptable.

To meet these stringent demands, redundant links are deployed throughout the network to provide fault tolerance, switches are combining links into virtual channels of traffic to increase bandwidth, routers and servers are breaking up data streams, so they can be transmitted in the most efficient way, even if it means the same data conversation has to be reassembled from several different physical paths. In other words, the “virtualization” of the enterprise network is becoming nearly impossible to monitor effectively with traditional out-of-the-box monitoring tools and network access devices.

Network, security, and compliance teams need to be able to view entire data conversations; they need to know where the data is coming from and where it’s going. Thus, traditional network tools are becoming less effective every day.

The enormous number of network segments, access points, and switches used in the enterprise network further compounds the problem. It is too costly to deploy all the tools needed on every critical segment where data needs to be monitored, collected, and analyzed. With limited resources, limited space, and limited budgets, internal teams are at best, fighting over access to the tools they need, or at worst, leaving themselves exposed to security threats or not getting the vital data necessary to support their organization effectively.

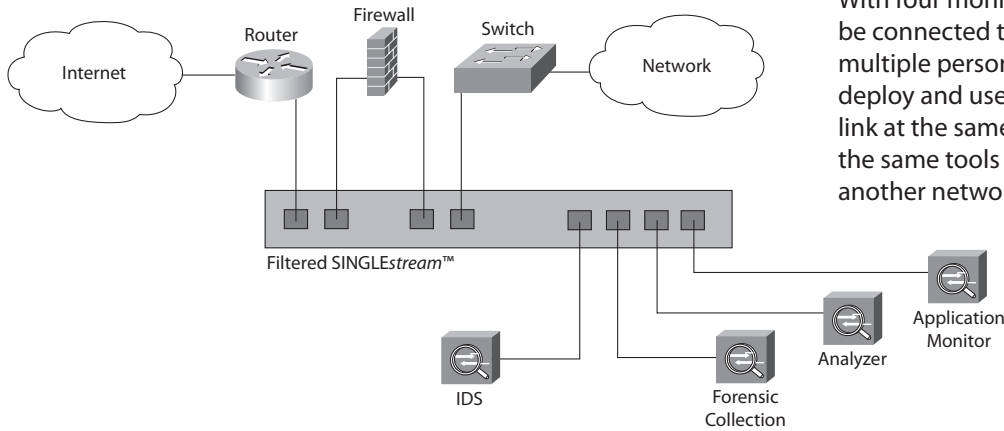
The Filtered SINGLEstream™ to the Rescue

As the premiere provider of network access solutions, Datacom Systems understands the critical nature of network operations and every organization’s need to “do more with less.” That is why we have created the revolutionary new Filtered SINGLEstream™ to

- Reduce the number of tools on your network
- Increase the number of tools that can be connected to your access ports
- Aggregate and reassemble full duplex conversations from multi-trunked links, redundant networks, EtherChannel, load balanced servers, and asymmetrically routed traffic
- Simultaneously monitor data at multiple points on the network with the same set of devices for a complete end-to-end view of your traffic
- Apply port level packet filtering to reduce traffic to your tools and eliminate “data overload” by making sure you get only the data you want

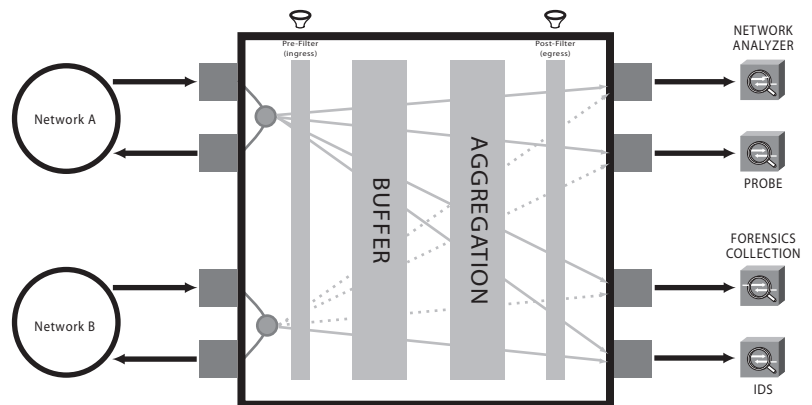
A C C E S S Y O U R N E T W O R K ™

Link Aggregation and Access Port Regeneration



With four monitor ports, four monitoring devices can be connected to the same in-line segment, allowing multiple personnel from multiple departments to deploy and use the devices they need on the same link at the same time. Additional network ports, give the same tools the ability to simultaneously monitor another network segment.

With the Filtered SINGLEstream's flexible "any to any" architecture, you can designate the port assignments to meet your specific needs. Any of the connected monitoring devices can see any of the connected network links. You can also quickly and easily change and customize port assignments on the fly with the built-in software, so there is no need to disconnect and reconnect any of the physical links if you want to assign a different tool to view a different network segment.



Additionally, the Filtered SINGLEstream™ supports link aggregation to combine the full duplex stream of data from the incoming network ports into one single output of data and sends copies to all the connected devices. The "many to any" aggregation functionality allows your connected devices to receive the entire data conversations from both network links, making this a perfect solution for monitoring redundant/failover links, EtherChannel over two physical paths, and asymmetric traffic.

A C C E S S Y O U R N E T W O R K ™

Packet Filtering - The Filtered SINGLEstream™ Advantage

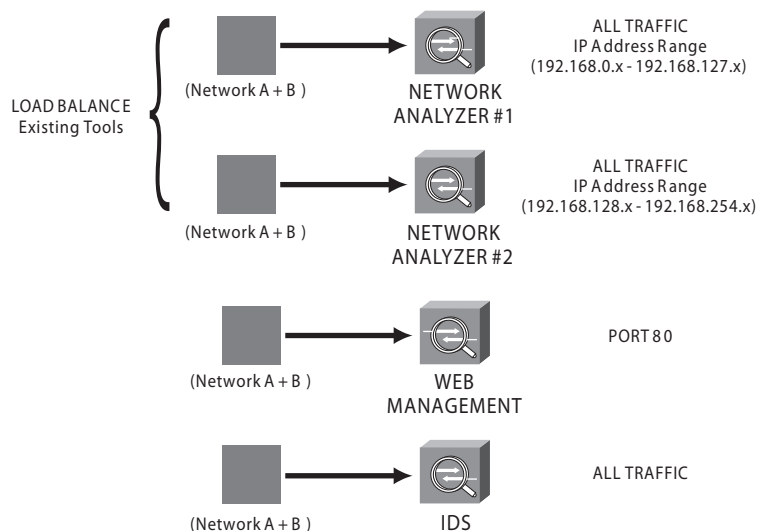
In addition to the flexibility and functionality of custom port assignments, link aggregation, and port regeneration, the Filtered SINGLEstream™ can take your tools to the next level with powerful data filtering.

Apply bit mask filters on the network (ingress) ports, and you have the ability to collect (pre-aggregation) only the data you need to see. By removing the irrelevant data before aggregation, you significantly reduce the chance of port over-subscription. Additionally, you can also apply filters on the tool (egress) ports (post-aggregation) giving you increased control over the level of filtering you require, and allowing you to create a unique set of filters for each connected monitoring tool. All filtering is hardware based and can be applied to any field of the 64-byte header. The Filtered SINGLEstream™ comes with numerous pre-built filters but can be easily customized, allowing you to drill down to specific IP, Subnet, MAC, VLAN, application port, or customized packet on the network.

The Filtered SINGLEstream™ is a far superior solution than any port regenerator, aggregator, and matrix switch.

Traditional regeneration taps, in addition to not being able to filter traffic, don't aggregate data, so they cannot provide full duplex data to monitoring tools that need it. The same problem exists for matrix switches. Finally, without the ability to filter, multi-port aggregators ("many to one") put into high-traffic areas can easily suffer from port over-subscription caused when the inflow of data exceeds the capacity of the output port.

The Filtered SINGLEstream™ suffers none of these limitations and opens the door to a whole new way of managing the diverse and ever-growing set of tools you need to deploy on your network.



Additional Features & Benefits

- Flexible network connectivity - Small form pluggables (SFP) allow you to connect up to four (4) SX, LX, or 10/100/1000 monitoring tools. Network ports are available in both fiber and copper.
- Easy to use client management interface – simply access and manage the Filtered SINGLEstream™ from anywhere in your network.
- Built-in 512MB buffer manages utilization overflow and significantly reduces chances of port over-subscription.
- Passive tap ports allow network traffic to flow uninterrupted if power is lost to the unit.
- Dual redundant power supplies insure seamless monitoring even if the main power source is unavailable.
- Easy to install – 1U space-saving design fits conventional 19" rack.

A C C E S S Y O U R N E T W O R K ™

The Filtered *SINGLEstream*™ Value Proposition

The Filtered *SINGLEstream*™ combines several network access technologies into one intelligent platform designed to help save your organization valuable resources.

Link Aggregation reduces the number of tools you deploy on your network, saving you money on deployment, recurring licensing fees, and valuable human resources. Providing you the ability to combine and reassemble entire data conversations reduces the time required to manually gather data from multiple sources. The easy-to-use, built-in aggregation of the Filtered *SINGLEstream*™ is easy to deploy, requires virtually no management, and eliminates the expense and compounded complexity of managed “do-it-yourself” switching solutions.

Port Regeneration helps eliminate contention for access to critical links and allows you to deploy more tools to analyze a single link. Easy access to your links, more efficient deployment of tools, and increased teamwork speed problem resolution and decrease downtime.

Filtering reduces traffic by eliminating what you don’t need to see, optimizing bandwidth, and making port over-subscription and dropped packets a thing of the past. With virtual port assignments, network downtime is not needed to disconnect and reconnect multiple tools. Central management allows for more efficient use of tools and saves man hours by not having to deploy remote personnel.

Intelligent media architecture allows you to use your existing tools without having to worry about variances in media type.

Simply put, the Filtered *SINGLEstream*™ was designed with not only today’s enterprise network in mind but tomorrow’s as well.

A C C E S S Y O U R N E T W O R K ™