

Cost-Effective Traffic Monitoring with Cisco Nexus Dashboard Data Broker



Providing visibility into networks

Today networks across industries, whether in data centers, enterprises, or service providers, are becoming increasingly large and complex. Users scattered across the globe, an ever-increasing plethora of applications, and the wide range of devices accessing these applications all add to this complexity. In such a scenario, the task of maintaining and providing a network that is not only always available, but also secure, compliant, and efficient is becoming all the more important.

How do you stay on top of this complexity, navigate using a variety of different tools, and stay ahead of potential problems to

guarantee the best continuous delivery of service? How do you correlate the underlying network and application performance to act fast and stay ahead of problems? The solution lies in “observability” – and key to this is visibility into application traffic. Pervasive visibility into this traffic is critical to maintain security, support troubleshooting, help ensure compliance, perform network/application performance monitoring, and perform resource planning, to achieve business agility and SLAs.

The Cisco Nexus® Dashboard Data Broker provides this visibility.

Cisco Nexus Dashboard Data Broker: Simple and scalable

The Cisco Nexus Dashboard Data Broker is a simple, scalable, and cost-effective solution for data center, enterprise, and service provider customers who need to monitor high-volume and business-critical traffic. It replaces traditional purpose-built matrix switches with one or more Cisco Nexus 3000,

9300 or 9500 series switches that you can interconnect to build a highly scalable TAP-Aggregation network that can help copy or mirror the production traffic using Optical TAPs (test access points) and Cisco® Switched Port Analyzer (SPAN). The data broker lets you:

- Build a TAP SPAN infrastructure with a wide range of port density and bandwidth ranging from 1 Gbps to 400 Gbps. Bandwidth supported include 1, 10, 25, 40, 100, and 400 Gbps.
- Support line-rate filtering, replication, and traffic forwarding.
- Deploy advanced functionalities such as time stamping, source port tagging, MPLS label stripping, VXLAN header stripping, GRE header stripping, ERSPAN header stripping, packet slicing, and more.
- Generate sFlow and NetFlow records.
- Copy and redirect traffic from remote or local sources to remote or local tools.
- Integrate with Cisco Application Centric Infrastructure (Cisco ACI®) to configure access SPAN sessions using the Cisco Application Policy Infrastructure Controller (APIC) REST API.
- Integrate with Cisco DNA Center (DNAC) to configure SPAN on selected access switches in enterprise networks.
- Onboard a Cisco Nexus 3550 Series Switch as a TAP device.
- Remove duplicates from copy traffic and send unique traffic flows to analytical/service tools for further analysis.

Benefits

- Offers a simple, scalable, cost-effective solution for monitoring high-volume and business-critical traffic.
- Replaces traditional purpose-built matrix switches with Cisco Nexus 3000, 9300 or 9500 series switches.
- Support port capacities from 1 to 400 Gbps within the network Test Access Point (TAP) and Cisco Switched Port Analyzer (SPAN) infrastructure.
- Provide line-rate traffic filtering, replication, and forwarding functions.
- Support inline traffic redirection to multiple security tools at the perimeter of the data center network.
- Deduplication helps in preserving sanctity of data sent to service nodes/ tools thereby augmenting the quality and effectiveness of the analytical results.

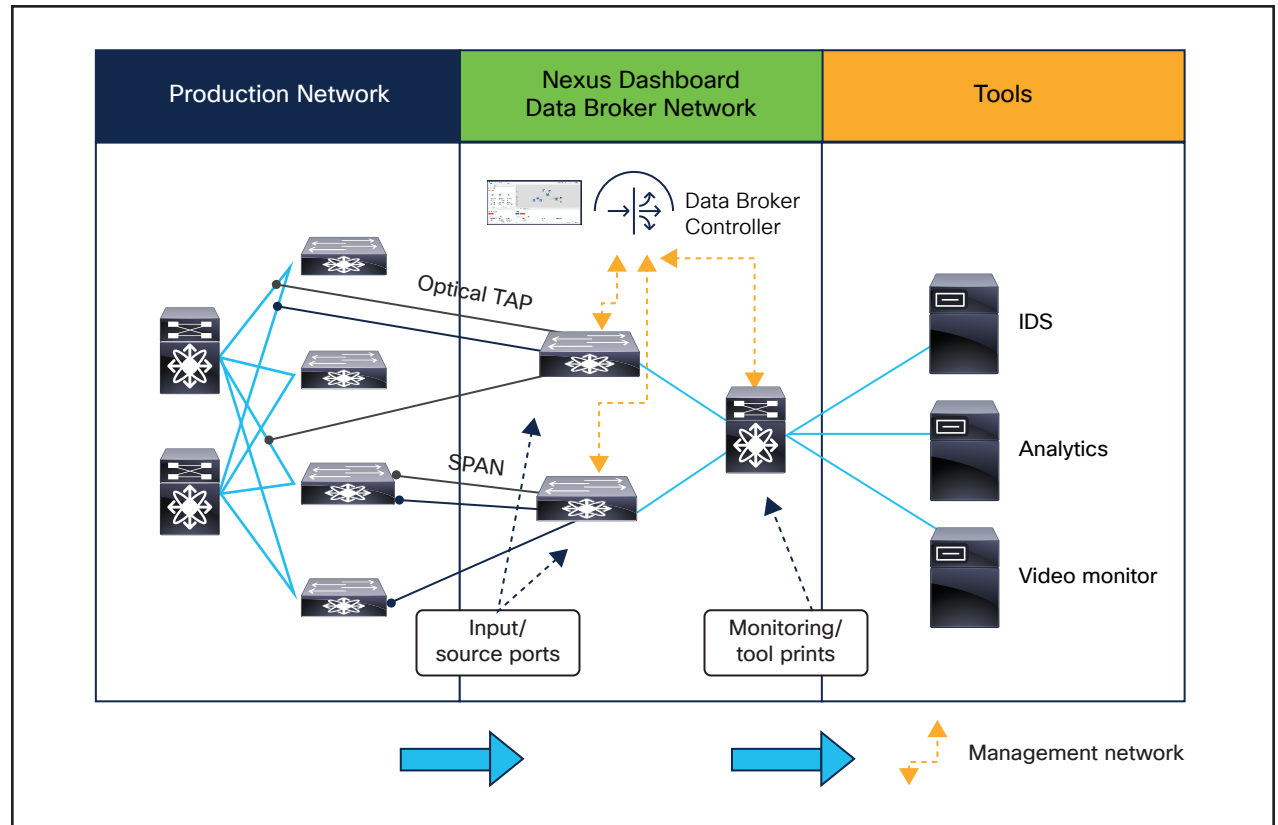


Figure 1. Cisco Nexus Dashboard Data Broker supporting TAP and SPAN aggregation

Inline traffic monitoring

Today's security landscape requires proactive, inline tools to create a strong, layered security environment. Common tools include Intrusion Prevention Systems (IPSs) and web filtering tools at the perimeter of the network. With the Cisco Nexus Dashboard Data Broker inline option (Figure 2), you can add one or more Cisco Nexus 3000 or 9000 Series platform switches to your production infrastructure to connect to these security tools (service nodes). The data broker lets you configure redirection policies that match specific traffic, redirecting it through multiple security tools before it enters or exits your data center. In failure scenarios, the data broker automatically bypasses the service nodes, and it can completely bypass all security tools for emergency troubleshooting.

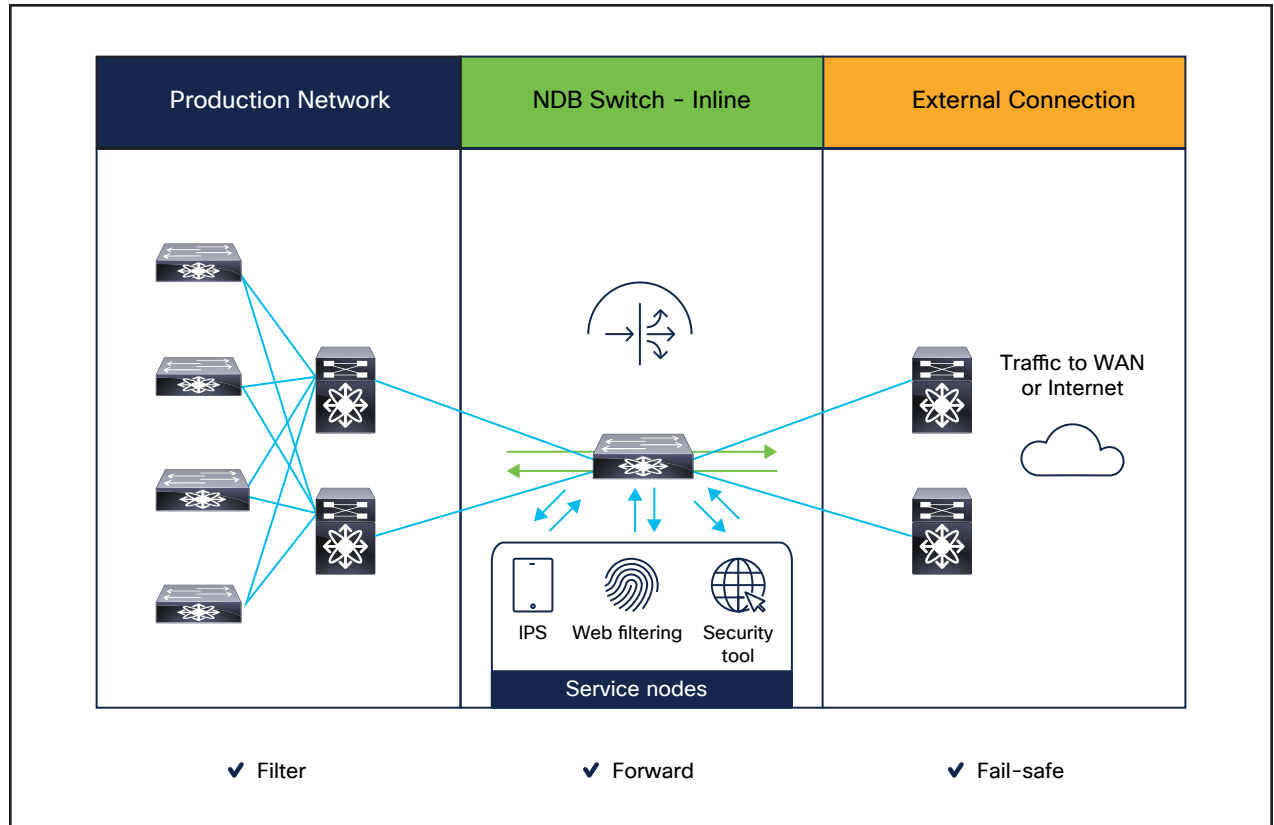


Figure 2. Cisco Nexus Dashboard Data Broker supporting inline traffic monitoring

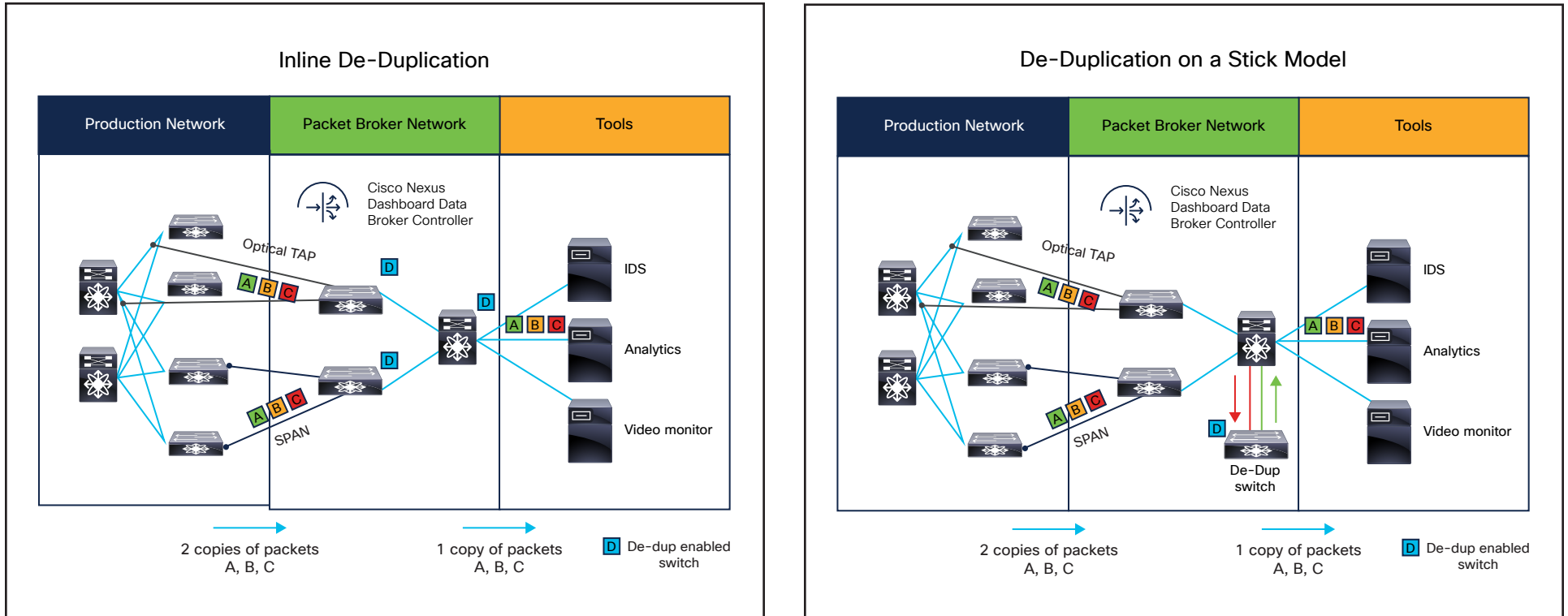


Figure 3. Cisco Nexus Dashboard Data Broker Deduplication deployment models

Next steps

For more information about Cisco Nexus Dashboard Data Broker, please visit <https://www.cisco.com/go/nexusdatabroker>.