Pervasive Embedded Application Intelligence and Security
Cisco Catalyst 6500 Supervisor Engine 32 PISA

At-A-Glance

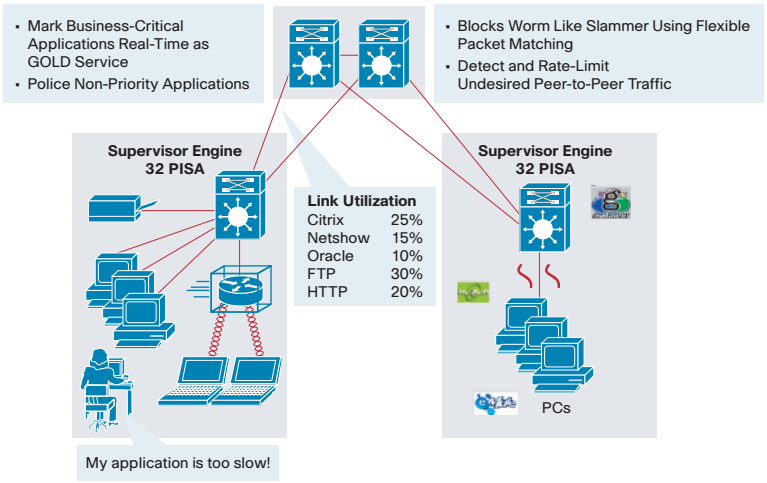
Why Should I Care About Application Intelligence and Security?

The application landscape of campus networks are changing. The convergence voice, video and data over IP networks, application webification; and the increase in applications for communications, collaboration and peer-to-peer file sharing; have dramatically increased the amount of traffic between hosts in the campus network. To deliver a high quality user experience, this traffic must be managed in the campus wiring closets and distribution layers.

In addition, the campus LAN access has become more open and less controlled due the employee mobility, diversified user devices such as wired and wireless PCs, IP phones, PDA etc, increased partner and contractor access. The risk of security threats such as worms and viruses has dramatically increased. Worms such as Slammer and Mydoom demonstrated that such threats could rapidly compromise campus networks. It is important for enterprise to apply tight access control and security pervasively at the campus wiring closets to stop threats before they enter into the campus network.

What Problems Need to Be Solved?

- Gain better visibility of network usage
- Mission critical communications including voice, video and corporate instant messaging must be prioritized
- Recreational application traffic needs to be managed so it does not impact critical applications
- Differentiated Web application controls using application specific attributes
- Organizations need to minimize their exposure to risk and liability. For example, block file sharing activities of copy right protected materials
- Notable worms and viruses need to be addressed at the access layer and WAN edge before they impact the campus network

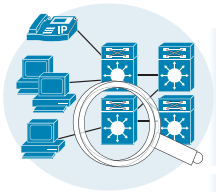


Catalyst 6500 Supervisor Engine 32 Programmable Intelligent Service Accelerator

The embedded hardware-accelerated deep packet inspection technology in Cisco Catalyst 6500's Programmable Intelligent Service Accelerator (PISA) provides stateful application intelligence and integrated security that can be pervasively applied right at your campus or WAN edge.

The embedded service model of PISA allows pervasive deployment of intelligent services in campus networks without adding expensive management and operational cost. The programmable hardware architecture provide future proof for quick new service adoption without sacrificing the performance.

Supervisor Engine 32 PISA
8x1GE Uplinks + 1x 10/100/1000
Supervisor Engine 32 PISA
2x10GE Uplinks + 1x 10/100/1000



NBAR
Application awareness and intelligent classification
Multigigabit Performance

Flexible Packet Matching
Rapid Security Protection
Multigigabit Performance

Programmable Architecture
Seamless new service adoption

Full Integration with
IPv4 and IPv6 in hardware
Advanced multicast and MPLS
Enhanced Manageability
HA with NSF/SSO and more

"We've always been able to be on the cutting edge of productivity because we have invested wisely in our networking infrastructure … The Catalyst Series 6500-E is the flagship switching platform for Cisco where a lot of the innovations begin, and when advancements like the Supervisor Engine 32-PISA are introduced, we can upgrade easily and cost-effectively."

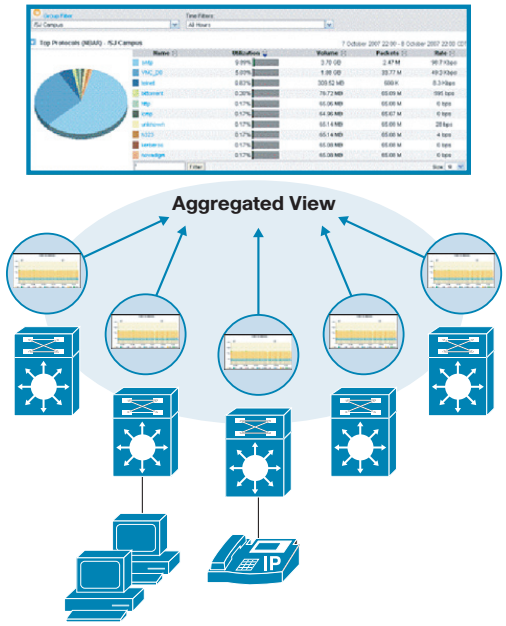
— Network Architect, a Biopharma company testing Sup32-PISA

Pervasive Embedded Application Intelligence and Security
Cisco Catalyst 6500 Supervisor Engine 32 PISA

At-A-Glance

Benefits of PISA Application Intelligence

- Increased visibility into network usage enables better network planning
- More than 100 applications (enterprise applications, P2P, instant messaging, multimedia, networking protocols, healthcare, financial protocols etc) are already recognizable by PISA. Granular sub-port application classification for multimedia and Web applications.
- The ability to take action on traffic at the access point ensure the user experience
- Multi-gigabit performance scales in wiring closet and WAN edge deployments
- Cisco Quality-of-Service Policy Manager centrally manages all PISA deployments
- Applications can be added while the switch is in service, delivering non-stop communications. Allows customized application definition



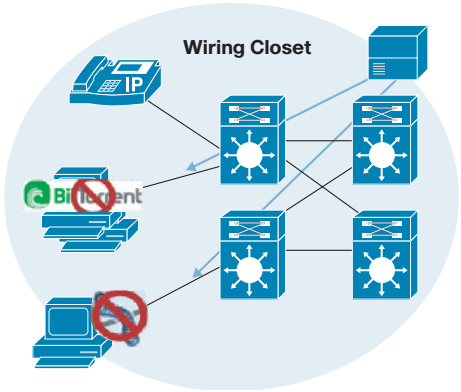
The comprehensive application intelligence SNMP MIBs provided by PISA allows easy integration with Cisco or third-party network monitoring solutions such as Cisco QoS Policy Manager, NetQoS NetVoyant, MRTG, InfoVista etc. These management solutions gather information from PISAs to provide real-time application visibility with both localized and aggregated network usage views.

The PISA application intelligence will also to be integrated with NetFlow to allow NetFlow export of application information using standard NetFlow v9 format.

Benefits of PISA Deep Packet Inspection Security

- Protection against notable worms, viruses and day zero attacks
- Identify and control undesired applications, such as recreational P2Ps, for security compliance
- URL filtering solution to help enterprise to enforce corporate Internet usage policy
- Integration with the Cisco Catalyst 6500 Firewall Service Module to provide central application-aware access control policy (IM and P2P control) enforcement leveraging distributed application intelligence provided by PISA
- Filters can be added while the switch is in service, delivering non-stop communications

The multi-gigabit deep packet inspection capability provided by PISA Flexible Packet Matching provide network administrator an embedded, pervasive infrastructure security tool to quickly respond to network events, such as worm outbreaks, right at campus LAN or WAN edge.



The PISA Flexible Packet Matching can be provisioned using Cisco Security Manager, which provides central security management for Cisco Security products. The Flexible Packet Matching policy events can be monitoring using Cisco CS-MARS.

For More Information

For more information, go to the following link: http://www.cisco.com/go/6500

Copyright © 2006 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

C45-468471-00 04/08