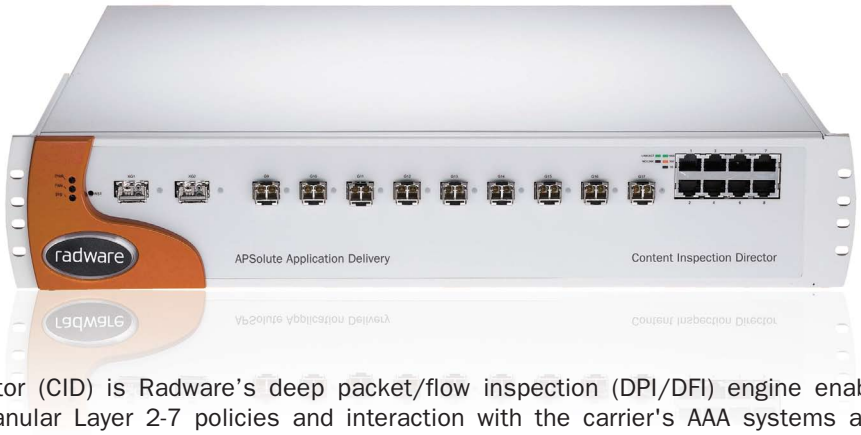
radware
availability | performance | security

Content Inspection Director Data Sheet

Extending the Value of Carrier Networks through Smart DPI/DFI



Content Inspection Director (CID) is Radware's deep packet/flow inspection (DPI/DFI) engine enabling value-added service deployment based on granular Layer 2-7 policies and interaction with the carrier's AAA systems as well as with operators management systems to enable dynamic activation of new granular policies. As wire-line and mobile operators face increasing competition and are searching for new revenue generators, CID drives carriers' profitability by enabling dynamic service selection for creation of new premium services and the building of new business models for a variety of network edge services derived by the deployment of next-generation network architectures.

CID for Mobile Operators

As mobile operators move from controlled, closed internet access to fully open internet access business models, the amount of traffic in their networks increases dramatically. In addition, as the internet gains greater weight as a content source – influenced in large part by user generated content (e.g., Web 2.0) and the introduction of advanced mobile devices (e.g., smart phones and Pocket PCs) utilizing open operating systems (such as Symbian and Windows Mobile) that provide a platform for a wide range of data traffic generating applications – network congestion grows even further.

Faced by these challenges, mobile operators are looking for ways to optimize mobile internet delivery over the Radio Access Network (RAN) as well as the ability to manage and charge for advanced content services. CID ensures high availability of the operator's mobile data services, guaranteeing service continuity. Its wire speed identification capabilities, together with the proxy modifications capabilities for various services, support both client-initiated traffic (POP3, HTTP, RTSP, etc) and server-initiated protocols (AOL IM, SMTP, etc).

Typical mobile operator implementations of CID include:

- Differentiated charging schemes support for premium content.
- Mobile internet optimization and acceleration (such as image reduction, compression and WTCP adaptation) over the Radio Access Network (RAN) empowered by AppXcel (Radware's accelerator engine), which reduces CapEx.
- Offloading major operator's congested platforms such as WAP gateways and content adaptation servers.
- Introduction of managed content services provided by third-party vendors to generate additional ARPU.

CID for Wire-Line Operators

Session Border Controllers (SBCs) are becoming a main point of congestion in pre-IMS implementations as the volume of VoIP calls and services increases. Therefore, carriers are looking for ways to offload the SBCs in order to allow even greater volumes of VoIP minutes. In addition, carriers have been plagued over the past several years with the ever-increasing peer-to-peer (P2P) traffic that frequently disrupts their internet business models.

Typical wire-line operator implementations of CID include:

- SBC offloading by identifying the call/session parameters and redirecting trans-coding and TLS functions to be performed by external (non-SBC) transcoders and TLS description servers, for more cost effective resource utilization. Offloading these functions out of the SBC path results in significant scalability and CapEx savings.
- In the peer-to-peer space, alleviation of P2P traffic burden on the network by redirecting P2P to caching and facilitating rate limiting.
- Saving interconnect bandwidth to the ISP in certain implementations when traffic to the service provider's Walled Garden can be redirected internally without going out to the Internet.
- Flexible introduction of managed content inspection services, enabled by redirection of subscriber's traffic by CID to any third-party content inspection tools.

CID transparently intercepts traffic and performs deep packet and flow inspection (DPI/DFI) in order to enable wire speed policy-based redirection of the traffic to the required service engines. This redirection is based on a wide range of Layer 2-7 parameters that leverages the network's awareness to user, service and content attributes. CID offers a multi-gigabit per second capacity, built-in redundancy and automatic service failure detection and failure bypassing. With these capabilities, CID enables carriers to offer a wide array of services based on an open platform for federation of multiple service domains with the required carrier grade avilability, performance and subscriber scalability mandatory for high volume networking environments.

Managed Services Delivery

With CID, carriers can effectively support the delivery of high performance, customized content inspection services. These services include typical store and forward inspection tools such as: URL filtering, anti-virus, anti-spam, Web Application Firewalls (WAF) and parental control as well as acceleration services such as caching, compression and SSL for business and residential customers.

CID enables the seamless deployment of high-availability, optimized, best-of-breed (third party) content inspection tools across carrier networks by redirecting the classified flows into the content inspection tools. This creates a unique competitive differentiator for service providers in their local market and high margin new revenue generating services.

The ability to provide managed content and security services to subscribed users is based on the user, service and content information. The traffic is directed to the relevant services for each. For example, only paying users' relevant traffic is redirected to the anti-virus server, while traffic such as video and voice streaming as well as non-paying users' traffic is redirected to bypass the anti-virus tools.

By sequentially redirecting the same session traffic across multiple content security tools and filtering operations, CID lets carriers customize a large number of content inspection flows for a large number of managed accounts and granular policy-based content inspection service customization.

Traffic Acceleration and Mobile Data Optimization

Combining load balancing, header modifications and advanced traffic management, CID's tight integration with AppXcel (Radware's acceleration engine) helps accelerate IP traffic delivery, guaranteeing service levels for the best end user experience. This is critical for mobile operators struggling to provide quality IP traffic delivery over the Radio Access Network (RAN).

Employing subscriber user agent, application and content classification (through HTTP parsing) and service and network attributes (through Radius sniffing), CID makes it possible to intelligently route traffic to relevant compression, acceleration or caching proxies. CID enables differentiated traffic handling and 'best-fit' mobile Internet data service acceleration and optimization over the Radio Access Network (RAN) through wireless TCP support and content compression improving significantly the TCP throughput over-the-air.

By extending caching services from within the Gi Network, CID dramatically reduces delivery times across subsequent user requests for the same content. This eliminates the need to fetch content from the Internet or recompress, for enhanced user response time while reducing overall bandwidth consumption and reducing unnecessary network congestion.

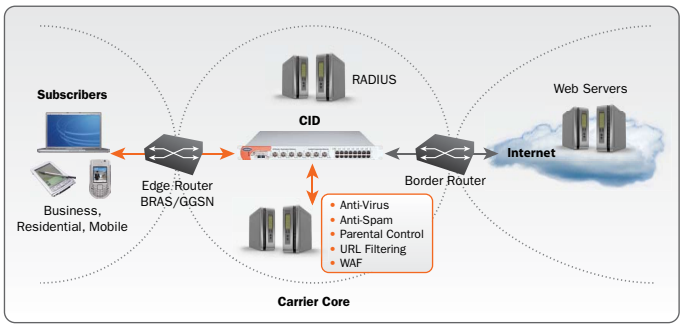


Figure 1 – Managed Content Services

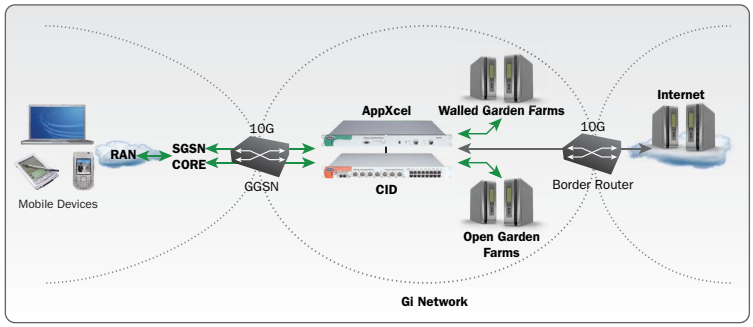


Figure 2 – Mobile Internet Optimization

Differentiated Service Delivery

CID's granular traffic classification and flow management enable the simple introduction of value-added services, allowing carriers to configure, tailor and deploy service packages according to customer preferences.

CID drives mobile carrier profitability by enabling dynamic service selection and premium value-added service delivery, based on any Layer 2-7 service criteria.

CID enables premium Walled Garden content services by 'capturing' subscribed users from the network edge and selectively routing them to dedicated mobile content services including third party trans-coding servers, MMS, Presence, on-line gaming, music and any other dedicated content service. With CID, mobile carriers can distinguish between paying and non-paying customers and direct users to dedicated premium services, letting operators participate in the content service value chain.

Leveraging CID's capabilities, carriers can easily provide a wide set of value- added content security services to their residential and business customers, as well as acceleration services to boost response time for end users. In both cases, only traffic from subscribed users is directed to the service, and application and content based policies ensure that the traffic is not damaged on the way by bypassing traffic type that can be affected by specific services.

Feature	APSolute Advantage	Business Benefit	Operations Benefit
Traffic interception and redirection	• Granular traffic classification per any Layer 2-7 parameter including subscriber, service and content information • User-defined traffic management (redirection) policies	• Quick-to-market introduction of tailored, differentiated service packages	• Fast and easy deployment of new services • Flexibility in service package definition
Load balancing traffic between multiple resources	• User-defined priorities for load balanced servers based on real-time measurements of: – Application response time – Inbound/outbound bandwidth – Number of packets/sec (Tx+Rx) – Number of concurrent users (Sessions/Connections) – Relative weight of servers – User-defined SNMP (MIB) data values – Cyclic (round-robin) and Hashing traffic dispatch	• Scalability of new carrier services to millions of subscribers • Cost effective, grow-as-you-need investment for new services • Minimize the cost of new service deployment	• Optimize server utilization • Prevent server overload • Maximize usage of best performing server • Seamless service capacity scaling • Maximize servers infrastructure investment
RADIUS-based traffic management	• Monitors the Radius authentication process to learn user information and redirects the traffic according to the user's service packages.	• Self-provisioning on-the-fly service • Reduce operational efforts	• Simple configuration and maintenance • Supports fixed and dynamic user access
Bandwidth management and traffic shaping	• Class based traffic shaping using CB-WFQ • Predefined Classes include over 40 common applications, ToS or Diffserv bits • User-defined classification per any Layer 2-7 parameter. • Limit/guarantee bandwidth per user-defined class • RED/wRED support • Marking sessions by Diffserv/ToS	• Ensure best user experience by guaranteeing service levels • Enable end-to-end QOS enforcement beyond simple Layer 2/3 information according to application and content type	• Bandwidth management is an integral part of a solution for acceleration (caching and compression), redirection and security
Application health monitoring for real-time failure detection and failure bypassing	• Server/application availability based on user-defined path • Five levels of application health monitoring: – Physical Port Status – ARP, ICMP, Ping – Application level Monitoring: Citrix App Browsing, Citrix ICA, DNS, FTP, FIX, HTTP, HTTPS (SSL/TLS), IMAP4, LDAP, LDAPS, NNTP, POP3, RADIUS, RTSP, SIP (TCP & UDP), SNMP – Content Level Monitoring: HTTP/HTTPS (SSL/TLS) Content check, HTTP/HTTPS Content Check with HTTP Authentication, HTTP/HTTPS response code verification, LDAP search, file verification on FTP servers, Citrix Server check, and more – User defined custom content health checks (binary/text content is supported) • Bind multiple checks with logical AND/OR conditions for complex, and flexible dependency	• Guarantee carrier service availability • Eliminate business losses due to IT failures • Provide highest SLA to users and customers • Savings on infrastructure costs	• Quickly identify and bypass failures • Automatically redirect traffic to the best available servers • Simplify and reduce costs of clustering and fault tolerant architectures • Use cost-effective components without suffering reliability penalty
Device redundancy	• VRRP • State synchronization between redundant switches for zero transaction downtime	• Guarantee uptime • Reduce service interruptions at all cases • Lower solution TCO	• Prevent the introduction of a single point of failure in a high-availability architecture
Highly reliable platform	• Purpose built appliance • High MTBF: 120,000-150,000 hours • Redundant power supply		
DoS shield and behavioral DoS protection	• Protection against zero-day attacks with patented behavior-based technology (18 seconds from detection to elimination) • Content, anomaly and behavioral based techniques • Bandwidth management mechanism can stop malicious traffic to ensure availability for critical applications • 1500 attack signatures out-of-box for wide range of applications	• Ensure service up-time even while under attack • Protect reputation with business partners and customers	• Prevent known and zero-day DoS attacks from bringing down services and servers
Integrated Intrusion Prevention			• Protect wide range of services/applications from malicious exploits and worms' infiltration
Advanced Security Reporting	• Security update service for up-to-date protection		• Real-time visibility into network-wide security threats • Logging and reporting of security events for forensics and compliance

Technical Specifications

				
Feature	**CID 200/202**	**CID 1000**	**CID 3020**	**CID 6000**
Nominal Throughput	Up to 200Mbps	Up to 1Gbps	Up to 3Gbps	Up to 5Gbps
Non-Blocking Backplane	9.6 Gbps	19.2 Gbps	44 Gbps	88 Gbps
Layer 2 Switching	Wire-Speed	Wire-Speed	Wire-Speed	Wire-Speed
RISC Processor	Motorola PPC 750 266 MHz	Motorola PPC 7410 500 MHz	Motorola PPC 7457 1.3 GHz	Motorola PPC 7457 1.7 GHz
RAM	Up to 256MB	Up to 512MB	Up to 1GB on Master and 2GB on Accelerators	Up to 2GB on Master and 4GB on Accelerators
Copper Ethernet Ports	8 x 10/100	16 x 10/100	12 x 10/100/1000	8 x 10/100/1000
Gigabit Ethernet GBIC/SFP Ports	0/2	5	8	9
10 Gigabit Ethernet Port	0	0	0	2
RS-232C Console	DB-9 serial connection female DCE interface for out-of-band management	DB-9 serial connection female DCE interface for out-of-band management	DB-9 serial connection female DCE interface for out-of-band management	DB-9 serial connection female DCE interface for out-of-band management
Dimensions	432mm x 475mm (17x18.7”) 19" EIA rack or standalone Height: 44mm (1U) Weight: 3.85 kg (8.5 lbs)	432mm x 475mm (17x18.7”) 19" EIA rack or standalone Height: 44mm (1U) Weight: 5.3 kg (11.7 lbs)	432mm x 485mm (17x19.1”) 19" EIA rack or standalone Height: 88mm (2U) Weight: 7.0 kg (15.4 lbs)	440mm x 486mm (17.3x19.1”) 19" EIA rack or standalone Height: 88mm (2U) Weight: 7.0 kg (15.4 lbs)
Environmental	Operating Temperature: 0-40º C Humidity (non-condensing): 5-95%	Operating Temperature: 0-40º C Humidity (non-condensing): 5-95%	Operating Temperature: 0-40ºC Humidity (non-condensing): 5-95%	Operating Temperature: 0-40ºC Humidity (non-condensing): 5-95%
Power	Auto-range supply: 100-250V or 38-72v DC 50-60Hz Power Consumption: 35 Watt Heat Dissipation: 119.5 BTU/h	Auto-range supply: 100-250V or 38-72v DC 50-60Hz Power Consumption: 44 Watt Heat Dissipation: 150.3 BTU/h	Auto-range supply: single or dual 100-250V or 38-72v DC 50-60Hz Power Consumption: 78 Watt Heat Dissipation: 266.3 BTU/h	Auto-range supply: single or dual 100-250V or 38-72v DC 50-60Hz Power Consumption: 110.8 Watt Heat Dissipation: 378.3 BTU/h
Certifications	Safety: EN 60950; UL 1950, CSA 22.2 No 950 EMI: EN 55022 Class A, EN 50024 FCC, Part 15B Class A CE, CUL, VCCI RoHS	Safety: EN 60950; UL 1950, CSA 22.2 No 950 EMI: EN 55022 Class B, EN 50024 FCC, Part 15B Class B CE, CUL, VCCI RoHS, NEBS	Safety: EN 60950; UL 1950, CSA 22.2 No 950 EMI: EN 55022 Class A, EN 50024 FCC, Part 15B Class A CE, CUL, VCCI RoHS	Safety: EN 60950; UL 1950, CSA 22.2 No 950 EMI: EN 55022 Class A, EN 50024 FCC, Part 15B Class A CE, CUL, VCCI RoHS

Radware APSolute™ Product Suite

Radware, the global leader in integrated application delivery solutions, assures the complete availability, performance and security of business-critical applications for more than 5,000 enterprises and carriers worldwide. With Radware’s comprehensive APSolute suite of application front end, access, and security products, companies can drive business productivity, improve profitability, and reduce IT operating and infrastructure costs by making their networks “business-smart.”

Certainty Support

Radware offers technical support for all of its products through the Certainty Support Program. Each level of the Certainty Support Program consists of four elements - phone support, software updates, hardware maintenance, and on-site support. Radware also has dedicated engineering staff that can assist customers on a professional services basis for advanced project deployments.

Learn More

To learn more about how Radware’s integrated application delivery solutions can enable you to get the most of your business and IT investments, email us at info@radware.com or go to www.radware.com.