

Protocol and Application Classification Engine (PACE)

ipoque's Protocol and Application Classification Engine (PACE) helps network equipment and software vendors to enhance their products with a powerful and proven layer-7 protocol detection. PACE uses a combination of deep packet inspection (DPI) and behavioral analysis to reliably detect protocols even if they use advanced obfuscation and encryption techniques. PACE has been optimized for performance and classification reliability. It is highly flexible and can be integrated in any existing system such as firewalls, UTM appliances, and WAN optimization controllers.

Many different network devices require information about the protocol and application type of passing network traffic. Such devices include firewalls, WAN optimization controllers (WOCs), unified threat and security management appliances (UTM, USM), billing and accounting systems, and lawful interception (LI) solutions.

Legacy applications, such as Web, e-mail and FTP, once could be easily and rather reliably detected by their IANA-assigned port numbers being used in TCP and UDP headers. This is no longer true. Many new applications, including peer-to-peer file sharing (P2P), instant messaging (IM), and Internet telephony (VoIP), do not adhere to these standards anymore. Some even explicitly try to prevent their detection.

ipoque has developed its Protocol and Application Classification Engine (PACE) to reliably detect all types of protocols and applications, even those using advanced obfuscation and encryption techniques to hide from detection. PACE uses a unique combination of deep packet inspection (DPI) and behavioral analysis to scan for various types of patterns that allow an extremely reliable protocol classification with very low false negatives and virtually no false positives. See the latest supported protocols list available on our Web site for more details.

PACE statefully tracks all network flows and, upon classification of a flow, returns a verdict stating the protocol used by this flow. This verdict can then be freely used for subsequent processing in the host system. The following list provides some technical details about PACE:

- Callback function interface to the host system
- Integrated connection/session tracking engine; existing implementations can also be used
- Runs on big and little endian machines
- Can be used as a dynamic or static library in user space or as a kernel module in kernel space
- Runs on 32- and 64-bit architectures
- 100% proprietary code provides clean licensing without GPL compliance issues
- Optional GPL-compliant netfilter wrapper for user space processing
- Less than 1,000 CPU cycles on average per complete protocol detection
- Less than 500 CPU cycles on average for the built-in session tracking code

PACE has been used for several years in ipoque's PRX Traffic Managers, which are deployed in networks with over a million attached subscribers. Every protocol signature undergoes a rigorous quality assurance process before being released. In addition, the large installed base of PRX Traffic Managers provides a valuable source of real-world feedback on signature quality used for further improvements.

ipoque's engineering team is highly experienced in the integration of PACE into many different platforms. PACE has been successfully integrated in firewalls, WAN optimization controllers, lawful interception systems, and multimedia delivery, accounting and billing systems for wireless network operators. Backed by these past experiences, ipoque can provide consulting and integration support to reduce the time to market to a few weeks.



- Layer-7 protocol and application detection
- Combines DPI and behavioral analysis for maximum reliability
- Proven application signatures for P2P, VoIP, IM, Skype, media streaming, and many more
- Support for obfuscated and encrypted protocols
- Regular signature updates
- >90% detection rate
- No false classifications
- Flexible integration and portability to any architecture
- Streamlined integration process
- Improve firewall performance and detection capabilities

"Implementing traffic management for P2P and IM protocols for our netfence gateway product line was a straightforward and efficient process with ipoque's PACE solution. Outstanding performance, ease of implementation, and responsive support confirmed ipoque was the best solution to fit our needs."



Dr. Klaus Gheri, CTO & Co-Founder phion AG