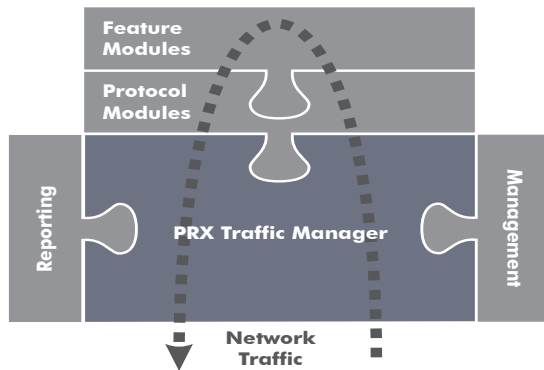


# Protocol Modules

*PRX Traffic Manager comes as a base unit plus a number of protocol and feature modules. Protocol modules extend the detection capabilities.*



## PRX Protocol Modules

Legacy filtering approaches based on port numbers often used by firewall systems are error prone. They produce many mismatches and are easily circumvented. PRX Protocol Modules use a combination of deep packet inspection (DPI) and behavioral analysis to detect and classify network applications and protocols. This approach guarantees a reliable detection with an extremely low false negative rate and virtually no false positives. Even proprietary and encrypted protocols are supported.

### Peer-to-Peer (P2P), Instant Messaging (IM) and Voice over IP (VoIP) Protocols

This module includes all the major P2P, IM and VoIP protocols, including BitTorrent, eDonkey, Skype, Yahoo, MSN and many more.

File sharing in peer-to-peer networks (P2P) is the single most bandwidth-consuming application in many parts of today's Internet. It not only incurs rising communication costs, but also adversely affects the performance of important network applications such as Internet telephony, Web, e-mail and file transfer. The high volume and the often questionable nature of the exchanged content make P2P a good target for traffic shaping. Assigning P2P a lower priority and defining data rate limits increase the performance of mission-critical applications particularly during periods of high utilization. Expensive network upgrades can be postponed. The rate limitation is invisible to P2P users. File sharing applications continue to work, only with a lower data rate. This approach minimizes the motivation of users to try to circumvent the P2P filter device. However, it is also possible to completely block P2P protocols.

Voice over IP (VoIP) has become one of the most-widely used Internet applications. The VoIP detection allows companies to gain insight in and control over their employees' VoIP usage. It enables Internet service providers to offer differentiated services and to control the VoIP bandwidth consumption in their networks. VoIP applications are most severely affected by overloaded networks. This effect can be alleviated by prioritization and bandwidth guarantees using the PRX detection and traffic management features. Even non-standard protocols such as Skype are supported.

Instant messengers (IM) are popular with many network users. Their uncontrolled use poses severe security threats and degrades staff productivity. The dangerous botnets are based on hijacked IM programs

used to distribute worms and viruses and to mount large-scale DDoS attacks. Particularly in corporate environments it is usually favorable to block such IM activities and only allow sanctioned IM clients. This can be achieved with simple IM filtering rules.

### Streaming Protocols

This module supports media streaming protocols and applications. Media streaming refers to streaming of audio and video content and is used by Internet radio and TV stations, but also by media content embedded in Web pages. Prominent examples are Joost and YouTube. Joost uses a protocol similar to Skype to distribute TV-like programs using P2P technology. YouTube facilitates Adobe Flash to offer video streaming embedded in its Web site. Flash is also used by many online advertisements. All these services have become very popular and are responsible for a significant data volume in the network.

### Standard Protocols

This module comprises the most popular legacy protocols for Web, e-mail and file transfer. In addition it includes support for direct download links (DDL). The term DDL refers to a service offered by so-called one-click file hosters such as RapidShare.com and MegaUpload.com. They allow to upload arbitrary files to a Web server without having to create a user account first. After a file has been uploaded, the hosting service provides a URL that directly links to this file. This link can then be published in forums, on Web pages or via e-mail. Simply clicking on this link will start the download of the file. The traffic generated by DDL services is rapidly rising and begins to rival the data volume generated by P2P-based file sharing.

### Tunnel Protocols

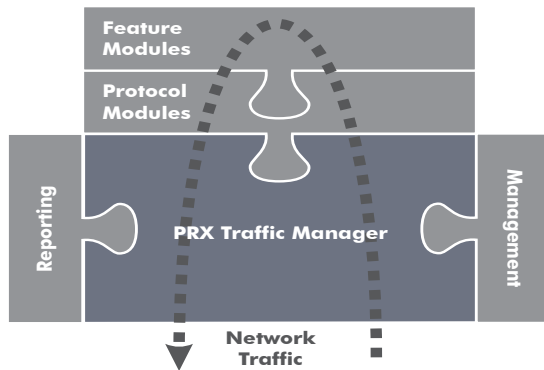
This module supports the most important tunnel protocols and applications such as OpenVPN and IPSec. Tunnel protocols are widely used to securely transfer data over the public Internet. Depending on the tunneled application, a tunnel may potentially consume a large amount of bandwidth. While it is virtually impossible to break encryption and analyze the traffic inside the tunnel, the tunnel itself can be detected and managed. Various different scenarios are possible. For example, tunnel traffic can be restricted to dedicated tunnel endpoints within a company to control the transfer of confidential data, or a certain amount of bandwidth may be guaranteed for business-critical VPN traffic.

### Gaming Protocols

This module supports the most popular gaming protocols and applications. While gaming protocols generally don't consume much bandwidth, latency is important to guarantee a smooth gaming experience when playing ego shooters like Half-life 2 or action strategy games like the famous World of Warcraft. The ipoque PRX Traffic Manager helps to keep latency low by allocating a certain amount of bandwidth for gaming. This is especially interesting for special gaming tariffs where users pay for a better gaming experience. The PRX Traffic Manager can also be used to block online gaming in schools or universities, for example.

# Feature Modules

*PRX Traffic Manager comes as a base unit plus a number of protocol and feature modules. Feature modules provide additional management and monitoring capabilities.*



## PRX Feature Modules

### Advanced Reporting

The Advanced Reporting module offers additional accounting and statistics capabilities to provide network operators with detailed data on the usage patterns in their network. It allows the definition of traffic classes. These classes can comprise user groups based on IP addresses and subnets, but they can also be based on VLAN tags or the differentiated services codepoint (DSCP) field in the IP header. Subscriber awareness in environments with dynamic IP addresses, for instance based on DHCP, is also supported. All statistics are then available for these classes and the individual users represented by them. These statistical data can be either directly displayed in the Web console or automatically exported to an FTP server for further processing.

### IP Control

The IP Control module provides user- and subscriber-aware traffic management. Similar to the Advanced Reporting module, it allows the definition of classes based on IP addresses, subnets, VLANs or the differentiated services codepoint (DSCP) field in the IP header. For each defined class, individual rules (e.g. application data rates, volume limits) can be assigned either to the overall class or to each user or subscriber in this class. Subscriber-aware traffic management with dynamic IP addresses is also supported.