

ИСПОЛЬЗОВАНИЕ СРЕДСТВ ПРОГРАММНОГО МОНИТОРИНГА ИНТЕРНЕТ-ТРАФИКА В ВЫСОКОНАГРУЖЕННЫХ КОРПОРАТИВНЫХ СЕТЯХ

Современные корпоративные сети представляют собой сложные инфраструктуры, обеспечивающие передачу больших объёмов данных между множеством узлов. В условиях высокой нагрузки критически важен эффективный мониторинг интернет-трафика.

Корпоративные сети строятся по иерархической модели, включающей уровни: Access Layer (доступ) – обеспечивает подключение конечных устройств; Distribution Layer (распределение) – агрегирует трафик с уровня доступа и применяет политики безопасности (VLAN, ACL); Core Layer (ядро) – высокоскоростная магистраль для передачи данных между распределительными узлами.

В крупных организациях используются: сегментация сети для повышения безопасности и управляемости, балансировка нагрузки для распределения трафика между серверами, избыточность каналов, централизованное управление.

Для анализа сетевой активности используются следующие технологии мониторинга трафика: Flow-анализ для сбора метаданных о трафике, глубокий анализ пакетов (DPI), реал-тайм инструменты.

Используемые механизмы QoS управления приоритетами: Voice (DSCP 46), Interactive (DSCP 32-38), Business Critical (DSCP 24-30).

Разработано веб-приложение «Base» (с открытым кодом, MIT li-cense) для использования системными администраторами внутри корпоративных сетей. На рисунке представлен интерфейс главной страницы приложения:

| Инвентарный номер | Раздел | IP адрес | Мак адрес |
|-------------------|------------|--------------|-------------------|
| 00018 | Девайсы | --- | --- |
| 00026 | Девайсы | --- | --- |
| 079 | Системники | 192.168.1.86 | 00:25:90:a8:cd:bc |
| 080 | Системники | 192.168.0.11 | 10:fe:ed:02:c2:79 |
| 082 | Системники | 192.168.0.60 | 00:25:90:79:8a:50 |
| 085 | Системники | 172.25.8.21 | 2c:4d:54:cf:77:7b |
| 086 | Системники | 172.24.0.22 | 50:e5:49:9d:e9:c8 |

Приложение интегрировано в компании ООО «Эффективные программы».