СПАЙДЕР–NGN

Система мониторинга сетей NGN/VoIP

Ваши сети под контролем

Развертывание сетей следующего поколения (NGN) ставит перед операторами задачи сохранения высоких показателей качества и надежности, привычных для абонентов традиционной телефонии, при внедрении услуг связи на основе современных технологий.

Постепенность процесса перехода к NGN требует наличия в составе OSS/BSS особых средств контроля и диагностики, способных предоставить всю информцию о состоянии сети и качестве услуг, анализируя интерфейсы как внутри NGN, так и в направлении сетей ТФОП, СПС и Интернет.

В этих условиях организация единого центра эксплуатации и управления, доступ к которому имеют различные подразделения компании, значительно повышает экономическую эффективность бизнес-процессов оператора связи.

Использование системы мониторинга СПАЙДЕР-NGN в качестве основы центра управления NGN-сети обеспечивает контроль оборудования разных производителей, предоставляет унифицированную отчетность по параметрам состояния сети и качества услуг вне зависимости от технологии связи, применяемой на отдельном участке, и обеспечивает возможность расчета интегральных показателей.

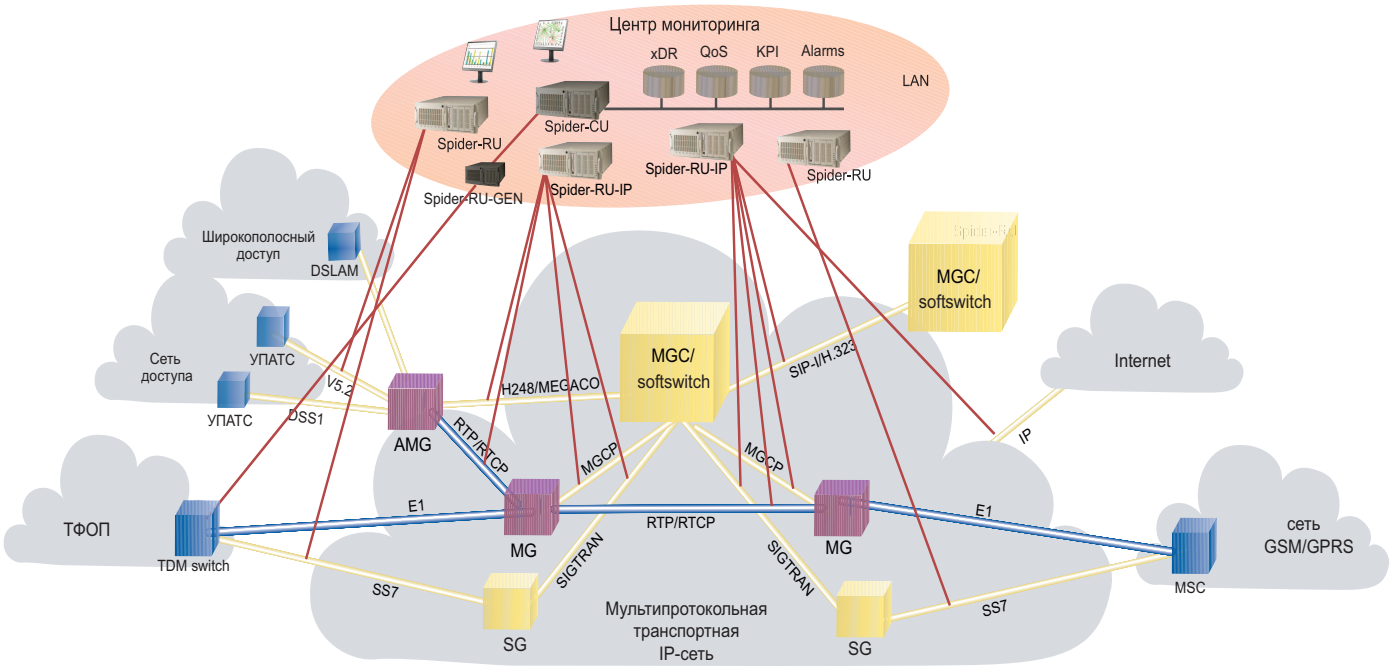
Возможности системы

- Контроль сигнального трафика разных технологических доменов: ОКС-7, H323, H248, SIP, SIGTRAN.
- Наблюдение за состоянием оборудования и историей аварийных сообщений (SNMP)
- Анализ производительности сети связи и доступности ресурсов
- Анализ качества связи
- Мультирпротокольная трассировка вызовов (ISUP, SIP, H.323)
- Он-лайн декодирование
- Формирование детализированных записей о вызовах (xDR)
- Настраиваемые KPI (ASR, NER, BMI, PDD, ...)
- Генерация трафика
- Измерения качества передачи речи (MOS, PESQ, G.107)
- Выявление мошенничества

ST
seventest
ТЕСТИРОВАНИЕ И КОНТРОЛЬ

СПАЙДЕР-NGN представляет собой распределенную систему сбора и централизованного анализа информации. Гибкая иерархическая архитектура позволяет внедрять систему на сетях любого масштаба

Архитектура и подключение



Система сетевого мониторинга СПАЙДЕР обеспечивает распределенный сбор и централизованную обработку информации на сетях связи любого масштаба, построенных на основе различных телекоммуникационных технологий.

Система СПАЙДЕР построена по иерархическому принципу. Подключение к сети и сбор данных в системе СПАЙДЕР осуществляют удаленные модули Spider-RU и малогабаритные пробники, обеспечивающие пассивное подключение к сигнальным звеньям сети, или специальные сервера Spider-RU-IP, собирающие данные непосредственно из IP-сети через порт зеркалирования маршрутизатора. Для решения задач тестирования и измерения качества передачи речи могут использоваться портативные временно подключаемые удаленные модули-генераторы трафика Spider-RU-GEN. Такой модуль подключается в качестве эмулятора и производит одновременно генерацию сигнального или разговорного трафика и его мониторинг, при этом другие модули системы отслеживают дальнейшее прохождение вызова.

Данные, полученные из сети, предварительно обрабатываются удаленными модулями. Центральный модуль Spider-CU производит управление всей системой мониторинга, просмотр информации о состоянии сети ОКС-7 и формирует целостную картину работы сети связи. Базы данных, содержащие статистику, CDR, журнал событий, а также функции обнаружения мошенничества могут быть реализованы на Spider-CU или на отдельных модулях Spider-DR/QOS/FMS.

Все модули системы взаимодействуют по выделенной технологической сети TCP/IP. Рабочие места пользователей организуются на любых персональных компьютерах, имеющих доступ в данную технологическую сеть. При принятии соответствующих мер безопасности возможна организация удаленного доступа пользователей через сеть Интернет.

Аппаратный состав системы

Spider-RU
Удаленный модуль, предназначенный для сбора информации из каналов сигнализации. Подключение осуществляется посредством интерфейсных модулей Agent-E1 и Agent-SDH.

Spider-RU-IP
Удаленный модуль, предназначенный для сбора данных по интерфейсам IP-сети. Данные собираются через порт зеркалирования маршрутизатора.

Spider-RU-Gen
Портативный модуль, предназначенный для генерации сигнальной и разговорной нагрузки.

Spider-CU
Центральный управляющий модуль.

Spider-FMS
Модуль обнаружения несанкционированного доступа.

Spider-DR/QoS
Модуль сбора подробной информации о вызовах и расчета показателей QoS.

Модульный принцип построения программного обеспечения системы СПАЙДЕР позволяет конфигурировать необходимые приложения в зависимости от потребностей заказчика

Возможности системы

Основные показатели

Общие параметры

calls	число вызовов
BH	час наибольшей нагрузки
...	...

Параметры качества передачи речи

MOS	средняя экспертная оценка
R	R-фактор
DEG	доля вызовов со снижением качества передачи речи
...	...

Параметры прохождения вызовов

ASR	доля отвеченных вызовов
NER	коэффициент эффективности сети
RNA	доля неотвеченных вызовов с нормальной причиной разъединения
SSB	доля вызовов, встретивших занятость
CLR	доля потерянных вызовов с аномальными причинами разъединения
...	...

Временные характеристики вызовов

CT	среднее время разговора
PDD	среднее время соединения
WTA	среднее время ожидания (отвеченные)
WTU	среднее время ожидания (неотвеченные)
BMI	число тарифицируемых минут
...	...

Характеристики передачи пакетов

BTx/Rx	число переданных/полученных байт
PTx/Rx	число переданных/полученных пакетов
PLR	доля потерянных пакетов
RDT	задержка “в оба конца”
...	...

Характеристки тракта ИКМ

BER	коэффициент битовых ошибок
ESR	коэффициент секунд с ошибками
...	...

Система СПАЙДЕР-NGN обладает широкими возможностями для контроля сети связи и мониторинга услуг.

Информация о состоянии и нагрузке сети выводится на карту в режиме реального времени, собранная статистика доступна в виде табличных и графических отчетов.

Приложение “Трассировка вызовов” производит отслеживание всего сигнального обмена, связанного с обслуживанием вызова, или предоставлением другой услуги. Трассировка производится в режиме реального времени или по историческим данным.

На основе сигнальной информации формируются детализированные записи о предоставленных услугах (CDR, TDR, IPDR), которые служат исходными данными для приложений подсистем оценки качества обслуживания и обнаружения несанкционированного доступа. Для просмотра CDR пользователями используются специальные приложения, в которых реализована возможность задания критериев отбора и получения суммирующих отчетов (например, общее число вызовов, соответствующих заданному критерию).

Подсистема оценки качества обслуживания, используя CDR, сформированные системой СПАЙДЕР, производит расчет показателей QoS и ключевых индикаторов производительности KPI для голосовых вызовов и других услуг. Учитывается качество обслуживания вызовов, процент завершенных и незавершенных вызовов и другие KPI. Формируются отчеты по статистике использования различных услуг, в том числе услуг доступа к информационным ресурсам, и доступности услуг. Производятся измерения качества передачи речи (G.107, MOS, PESQ), возможна также генерация трафика специальными удаленными модулями и одновременные измерения показателей, а также мониторинг сигнального обмена.

Контроль соблюдения согласованных уровней качества предоставления услуг (SLA) автоматизирован, рассчитываемые системой KPI автоматически сравниваются с заданными пороговыми значениями, при отклонении формируется запись в журнале событий и аварийное сообщение.

Подсистема Spider FMS обеспечивает автоматический поиск и обнаружение различных типов мошенничества, пресечение новых попыток нелегального доступа, предоставление полной информации по источникам, типам и числу попыток совершения мошенничества в сети оператора. Выявляет карточный фрод, спам и вирусные атаки.

Система производит регистрацию в журнал событий изменений состояний объектов тестирования и выводит уведомления о выходе за заданные границы параметров нагрузки, показателей QoS и SLA.

Поддерживаемые протоколы

NGN		
H.323	RAS	ITU-T H.225.0
	H.225	ITU-T H.225-0
	H.245	ITU-T H.245
	H.248/ MEGACO	ITU-T H.248
MGCP		IETF RFC 3435
SIP		RFC 2543
SIP-I		ITU-T Q.1912.5
SIP-T		RFC 3372
SIGTRAN	SCTP	IETF RFC 2960
	M2UA	IETF 3331
	M2PA	ETF RFC 4165
	M3UA	IETF RFC 3332
	SUA	IETF RFC 3868
	IUA	IETF RFC 3057
	V5UA	IETF RFC 3807
RTP		IETF RFC 3550
RTCP		IETF RFC 3550
BICC		ITU-T Q.1902
BCTP		ITU-T Q.1990
TRIP		IETF RFC 3219

Internet content	
HTTP	IETF RFC 2616
ICQ	ICQ Ver 7
POP3	IETF RFC 1081
SMTP	IETF RFC 788, 1981
FTP	IETF RFC 959

LAN/WAN	
MAC	IEEE 802.3
LLC	IEEE 802.2
ARP	IETF RFC 826
RARP	IETF RFC 923
PPP	IETF RFC 1134
LAPF	ITU-T Q.922
IP	IETF RFC 791
TCP	IETF RFC 793
UDP	IETF RFC 768
ICMP	IETF RFC 792
IGMP	IETF RFC 2236, RFC 3376
DHCP	IETF RFC 2131
DNS	IETF RFC 2929
IDRP	ISO/IEC 10747
OSPF	IETF RFC 2328
NetBIOS	IETF RFC 1002
RSVP	RFC 2205
RADIUS accounting	IETF RFC 2865, RFC 2866
DIAMETR accounting	IETF RFC 3588
RIP	IETF RFC 1058, 1988
SNMPv3	IETF RFC 3416
VRRP	IETF RFC 3768, 2004
BGP	IETF RFC 4271
EGP	IETF RFC 904
LDAPv3	IETF RFC 4511

ОКС-7	
MTP	ITU-T Q.701-Q.704, Q.707-Q.709 ANSI T1.111
SCCP	ITU-T Q.711-Q.714 ANSI T1.112
ISUP	ITU-T Q.761-Q.Q764, Q.767 ETSI ETS 300 121 MoU
TCAP	ITU-T Q.771-Q.774 ANSI T1.114
MAP	3GPP TS 29.002, ETSI GSM 09.02 ANSI TIA/EIA-41.5-D
INAP	ITU-T Q.1218 ETSI ETS 300 374
CAP	ETSI GSM 09.78 3GPP GSM TS 29.078
BSSAP	ETSI GSM 08.08
DTAP	ETSI GSM 04.08 3GPP TS 24.008 Rel-6
BSSAP+	3GPP TS 29.018
SMS	ETSI GSM 04.11 3GPP TS 23.040
Сеть доступа	
DSS1 L1	ITU-T I.431, ETSI ETS 300 011
LAPD	ITU-T Q.921 ETSI ETS 300 125
DSS1 L3	ITU-T Q.931 ETSI EN 300 403
QSIG L3	ETSI ETS 300 172,
LAPV5	ETSI ETS 300 324-1, ETS 300 347-1
V5 L3	ITU-T Q.931 ETSI ETS 300 324-1; ETS 300 347-1

Использование информации, предоставляемой системой СПАЙДЕР в различных подразделениях Оператора повышает коммерческую эффективность ее внедрения и сокращает период окупаемости проекта

Области применения

КАЧЕСТВО ОБСЛУЖИВАНИЯ

Проактивный мониторинг сети на уровне услуг, анализ качества обслуживания и статистики использования различных услуг обеспечивают эффективное планирование ресурсов и рост доходов. Повышение оперативности при рассмотрении жалоб абонентов повышает их лояльность.

Возможности системы

- Унифицированные отчеты и графики показателей QoS для услуг разных типов с разбивкой по: присоединенным операторам, кодам направлений (страна/регион/город/оператор), типам услуг
- Тревожные сообщения QoS при снижении показателя ниже настраиваемого пользователем граничного значения с выводом в журнал событий и также отображением на карте
- Несколько десятков заданных KPI, удобный инструмент для создания пользовательских индикаторов
- Возможность как раздельного анализа качества услуг NGN и ТФОП, так и сведения статистики по ним в единый отчет
- Табличный и графический формат отчетов
- Формирование подробных записей о каждом вызове xDR (CDR, IPDR, TDR)

Преимущества:

- Проактивное выявление проблем сети для предотвращения потерь
- Снижение числа претензий абонентов и присоединенных операторов
- Минимализация финансовых убытков от потерянных вызовов

ЭФФЕКТИВНАЯ ЭКСПЛУАТАЦИЯ

Мультипротокольный мониторинг обеспечивает стабильность работы при взаимодействии оборудования разных технологий (PSTN/TDM, NGN/IP). Исследование причин и источников каждого отказа, трассировка любого проблемного вызова, а также анализ общей статистики по причинам и источникам отказов позволяет выявлять проблемные точки сети.

Возможности системы

- Отображение структуры, состояния, нагрузки сети в режиме реального времени
- Статистика по отказам и перегрузкам
- Мультипротокольная трассировка вызовов в реальном времени и по историческим данным
- Декодирование сигнальных сообщений разных технологий связи
- Анализ эффективности маршрутизации
- Длительное хранение и архивация данных

Преимущества:

- Снижение эксплуатационных затрат и трудоемкости при построении, развитии и управлении сетью
- Ускорение внедрения новых услуг
- Обеспечение надежности функционирования сети
- Минимизация времени простоя оборудования и недоступности услуг

ФРОД И БЕЗОПАСНОСТЬ

Контроль в реальном времени за содержанием сигнальных сообщений и поведением заданных групп абонентов (“черные”, “белые”, “серые” списки и др. критерии) позволит ОТДЕЛУ БЕЗОПАСНОСТИ повысить оперативность и эффективность реагирования на преднамеренные угрозы информационной безопасности, операторские ошибки, сбои систем сбора биллинговой информации и выставления счетов.

Возможности системы

- Обнаружение и регистрация фактов мошенничества и угроз информационной безопасности с минимальными затратами ручного труда
- Предоставление информации соответствующим службам
- Прослушивание и запись информации в разговорных каналах
- Формирование CDR в режиме реального времени

Преимущества:

- Повышение оперативности и эффективности реагирования на преднамеренные угрозы информационной безопасности, операторские ошибки, сбои систем сбора информации и выставления счетов

Сертификат соответствия: № ОС-1-СУ-0037

тел/факс: +7 (812) 333 36 37
e-mail: sales@seventest.ru
http://www.seventest.ru