Spider

SURVEILLANCE SYSTEM FOR TELECOM NETWORKS

SUMMARY

Today, network service providers are looking for opportunities to increase growth with new, advanced services, while at the same time, facing significant challenges, such as increasing competition, expanding networks, converging technologies and rapidly changing equipment platforms.

Spider is advanced network and service assurance solution for network service providers. It is designed to support a range of business and technical operations throughout the organization of any network operator.

Spider is a Surveillance System used for telecom networks using Signalling System 7 and IP networks.

Spider provides solutions for:

- Network performance monitoring
- Network planning
- Trouble shooting
- Traffic analysis
- Multi-protocol call tracing
- Collection of CDR/TDR/…
- QoS, SLA
- Billing verification
- Fraud detection
- Monitoring, analysis, and QoS for VoIP networks

The philosophy of Spider is to extract the information needed directly from the network, thereby creating a vendor independent network quality assurance solution based on the data delivered by each transaction in the network.

SPIDER ARCHITECTURE

The architecture of Spider is distributed, where the non-intrusive monitoring probes (Agents and RUs) are located at the sites where the monitored links terminate and the surveillance center server (CU and some special units like CDR-server, FMS-server, QoS-server) is located at the network surveillance center.
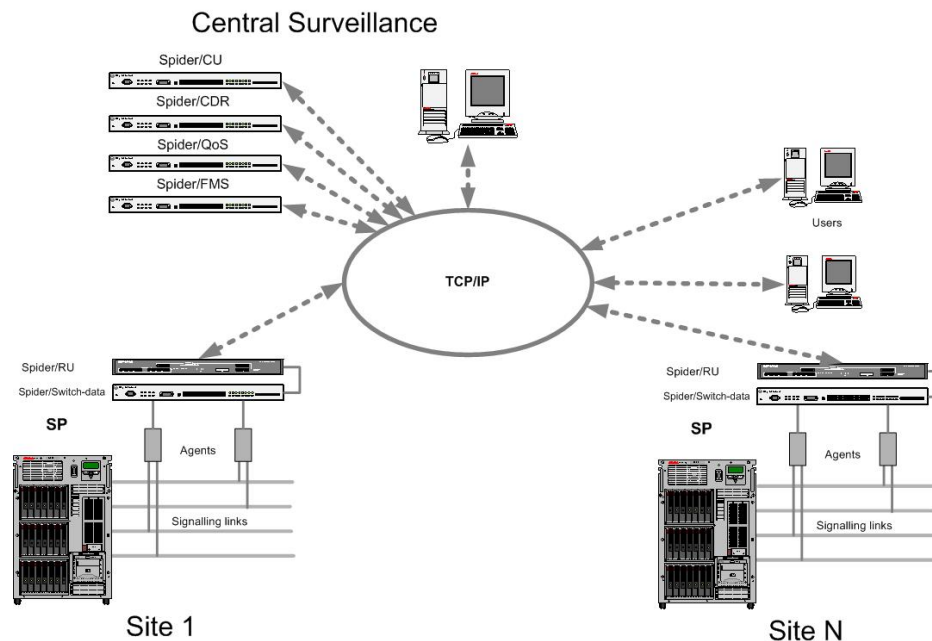
The components of the system communicate through a standard LAN/WAN structure. To handle this, standard routers are used, and they will therefore typically already be part of the network operators existing network infrastructure.

From RUs the measurement information is sent to CU, which then correlates the information and presents it to the operator.

The architecture enables a field-based operator to access the data of the system, from anywhere in the network. It is also possible to distribute the center functionality into central and regional surveillance centers.
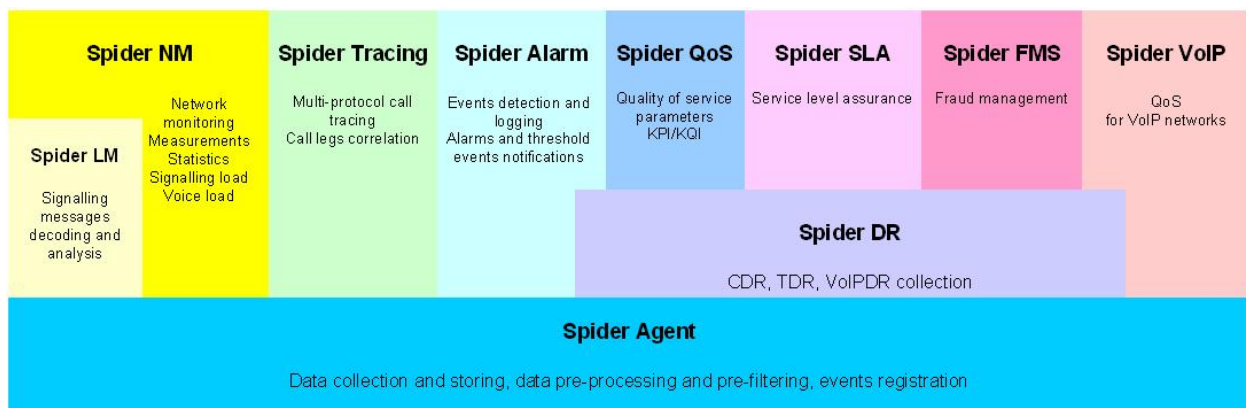
With a distributed architecture the system easily becomes horizontally scalable

- when adding new sites
- when adding more probes to existing sites
- when adding surveillance centers
- when adding servers in surveillance centers.

The monitoring probes have large storage capacity, providing the system with distributed storage capacity. This enables storage of the collected information as far out in the system as possible. The measurements are forwarded to the central servers when requested by an application. The amount of data stored on the probes provides the possibility of gathering historical information for post-analysis of a faulty situation.

SPIDER APPLICATIONS

The Spider solution is a combination of state-of-the-art non-intrusive probes and advanced software applications:

Spider NM	Spider Tracing	Spider Alarm	Spider QoS	Spider SLA	Spider FMS	Spider VoIP
Network monitoring Measurements Statistics Signalling load Voice load	Multi-protocol call tracing Call legs correlation	Events detection and logging Alarms and threshold events notifications	Quality of service parameters KPI/KQI	Service level assurance	Fraud management	QoS for VoIP networks

Spider LM — Signalling messages decoding and analysis

Spider DR — CDR, TDR, VoIPDR collection

Spider Agent — Data collection and storing, data pre-processing and pre-filtering, events registration

Spider Agent

- Data collection and storing
- Data pre-processing
- Pre-filtering
- Events registration

Spider NM

- Real time network elements status monitoring
- Graphic view of network structure and status
- Signalling load measurements
- Voice trunks load measurements
- Signalling traffic statistics
- Graphical and tabular traffic statistics reports

Spider LM

- Signalling information real time decoding
- Detailed protocol analysis
- Checking of signalling units correctness
- 2-3 weeks MSU Mass Storage for detailed protocol analysis in the past

Spider ALARM

- Alarm threshold manager
- Alarm notifications
- Real time event and threshold alarms
- Event log

Spider QoS

- CDR based Quality of Service reporting
- Release cause statistics
- Manual and scheduled report generation
- Notifications of QoS degrading based on pre-set parameters
- KPI/KQI evaluation
- PESQ procedure
- Packet delay, packet loss, jitter
- Real time graphical and tabular reports

Spider FMS

- Fraud detection based on CDR analysis
- Real time fraud detection
- DTMF analysis
- Prepaid services data vs actual subscriber activity comparing
- Black lists
- Fraud rule editor

Spider SLA

- Automatic control of SLA

Spider Tracing

- Fast real time network wide Call Traces (also in the past and in the future)
- Multi-protocol Call tracing (call leg correlation)
- 10 simultaneous Call Traces (per user)
- View of signalling messages in full decoded form

Spider DR

- CDR, TDR, IPDR collection
- Flexible criteria
- Records storage for given intervals
- User access for data analysis
- Manual and scheduled report generation

SPIDER HARDWARE

The Spider solution is based on standard components. The use of standard components provides a security of availability to the operator, in terms of scalability and replacement of components.

Spider/Agent

Agent-E1 - interface module for non-intrusive connections to E1s	1. One Agent-E1 per 2 E1s
	2. Up to 24 Agents can be connected to RU via Spider/Switch-Data
Agent-STM1 - interface module for connection to STM1 via passive optical splitter	1. One Agent-STM1 per 1 STM1, 10 E1s, 32 simultaneously processed SLs.
	2. If necessary from one STM1 derive more than 10 E1s, then Agents-STM1 can be connected in cascade.

Spider/ Switch-Data

24-ports LAN SWITCH with power supply	3COM 4400 PWR
	Connects Agents to Spider/RU

Spider/RU, Spider/CU, Spider/CDR, Spider/FMS, Spider/QoS

Rack mounted IPC	HW platform - SuperServer Supermicro
	Rack mounted server 19'', 1U, dual P4 Xeon, 1GB RAM, 3x73GB SCASI HDD RAID, 2xLAN 100

PROBE

Probe consists of:

- interface modules – Spider/Agent (up to 24 Agents per RU, 48-96 SLs per RU)

- processing module Spider/ RU

- LAN switch - Spider/Switch-Data

The intention behind Agents is to collect signalling information in real time without disturbing the signalling (non-intrusive).

The probe will decode the signalling in real time and signalling messages will be collected and saved for later use or for immediate display.

The presentation of the signalling results is carried out through applications that basically reside on a server and partly on the probes.

E1 connections (Agent-E1)

Agent collects data from signalling links, converts them into Ethernet packets, and sends the information to processing unit (RU). Power: 12VDC or 40-72VDC.

The probes provide interfaces toward the network links to be monitored. The probe will usually be connected to an isolated test point on the MDF where the switches are connected to the cables. This is done with cables going directly between the MDF and the Agents.
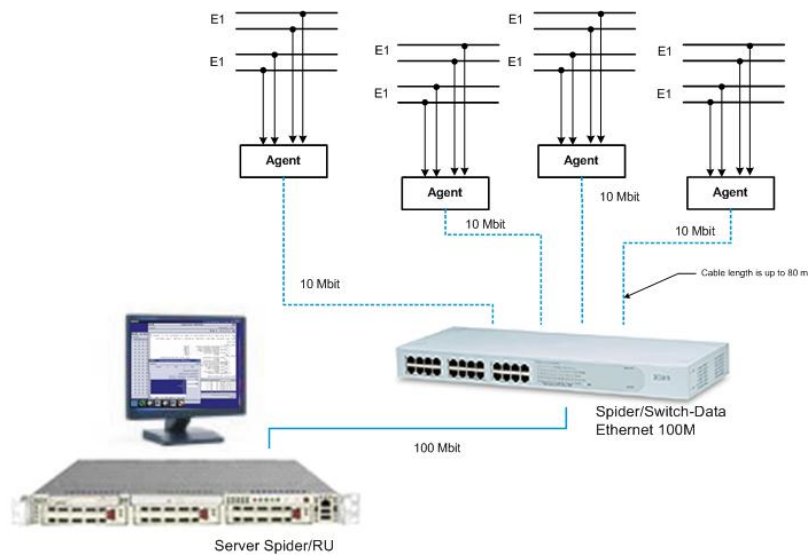
Probe perform transmission-alarm detection, framing analysis, CRC checking, time stamping of events, statistics counting and FISU filtering.

STM1 connections (Agent-STM1)

The probes provide interfaces toward the network links to be monitored. The probe will be connected to an STM1 via passive optical splitter.

	STM1	number of E1s	number of SLs
One Agent-STM1			
- can be cjnnected to:	1		
- derives from STM1:		10	
- simultaneously processes:			32
Note: if necessary from one STM1 derive more than 10 E1s, then Agents-STM1 can be connected in cascade.			