Möglichkeiten der Überwachung im 10GbE-Datenverkehr

Lars Weiler ‹pylon@ccc.de›

SIGINT 2009

22. Mai 2009

Inhalt

Über den Referenten

- MAGELLAN Netzwerke GmbH in Köln
- Installation, Konfiguration, Betrieb, Monitoring, Analyse 10GbE-Netzwerke
- Mobilfunkprovider, Internetprovider, Finanzunternehmen, europaweit

MAGELLAN
Netzwerke GmbH

Inhalt

Einsatz von 10GbE-Leitungen

- Backbone
  - Standortvernetzung
  - Punkt-zu-Punkt-Verbindung
  - Ringbetrieb
- Mobilfunk
  - SGSN zu GGSN
  - Serving GPRS Support Node
  - Gateway GPRS Support Node

Norm und Vorgaben

- IEEE 802.3ae seit Juni 2002
- Voll-Duplex-Betrieb
- Nur Punkt-zu-Punkt-Verbindungen
- Kollisionsfrei

10GbE-Filtern in Zahlen

Bis zu 14.880.952 Frames pro Sekunde

- bei 64 Byte pro Frame
- 12 Byte Inter-Frame Gap

10GbE-Filtern in Zahlen

Bis zu 14.880.952 Frames pro Sekunde

- bei 64 Byte pro Frame
- 12 Byte Inter-Frame Gap

Vergleich: Heuhaufen

- Etwa 1.000.000 Grashalme

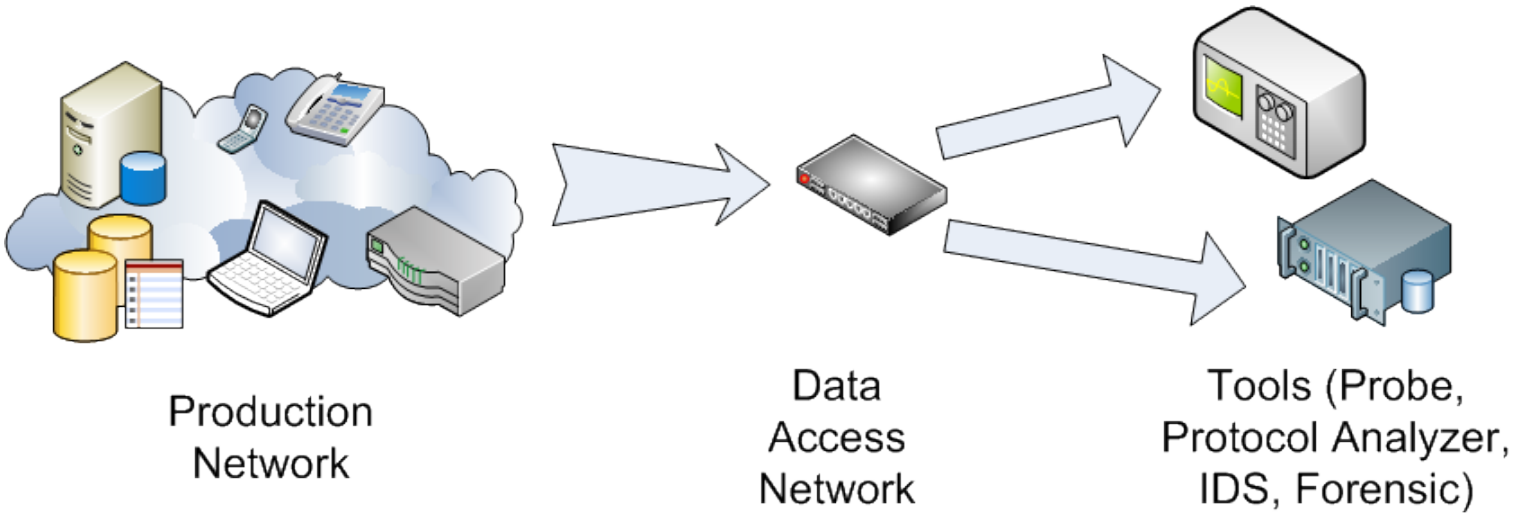
Das Filtern von einem Paket bedeutet mehr als 14 Heuhaufen pro Sekunde zu durchsuchen!

Inhalt

Verwendung von 10GbE-Überwachung

- Durchsatz an verschiedenen Messstellen
- Ausfall von Leitungen
- „Netzblockaden“
- z.B. MPLS oder 3G Networks

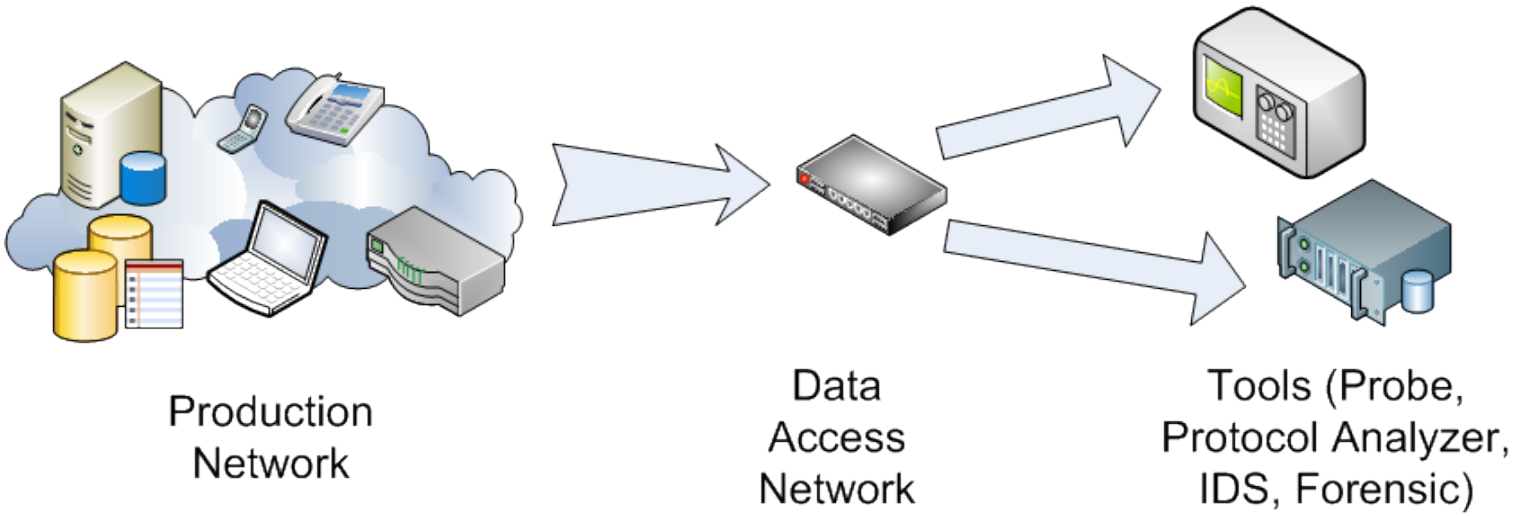
Aufbau einer Monitoring-Umgebung



Production Network

(Passive) TAPs

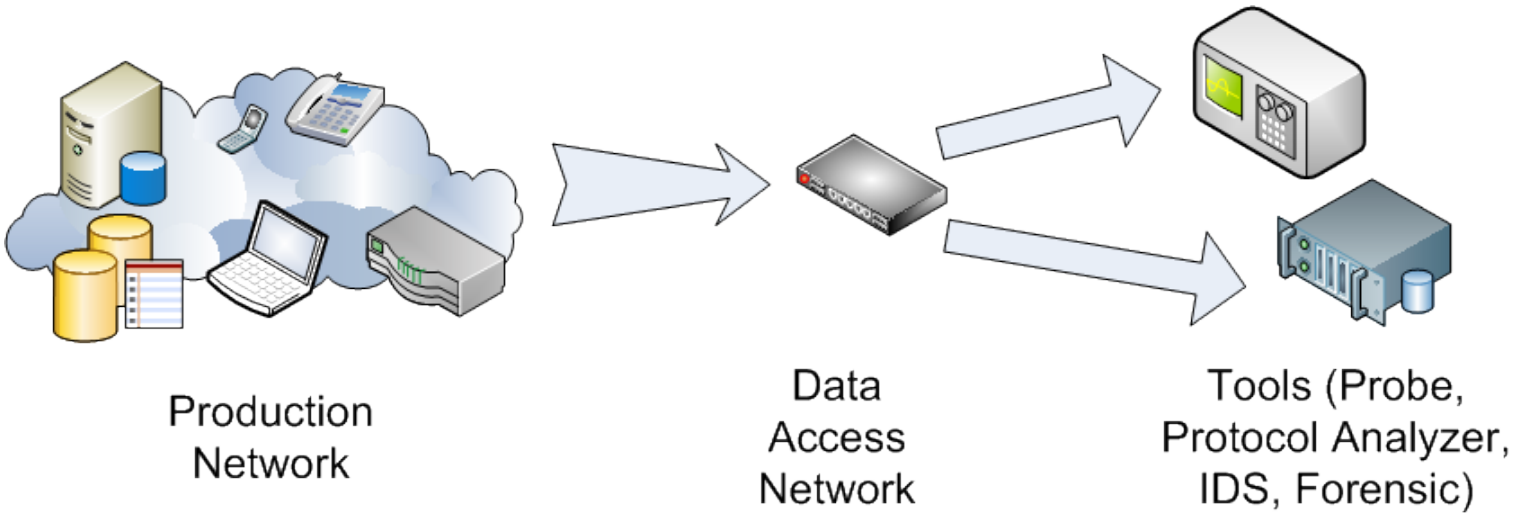
Aufbau einer Monitoring-Umgebung



Data Access

Aggregation, Replication, Filtering

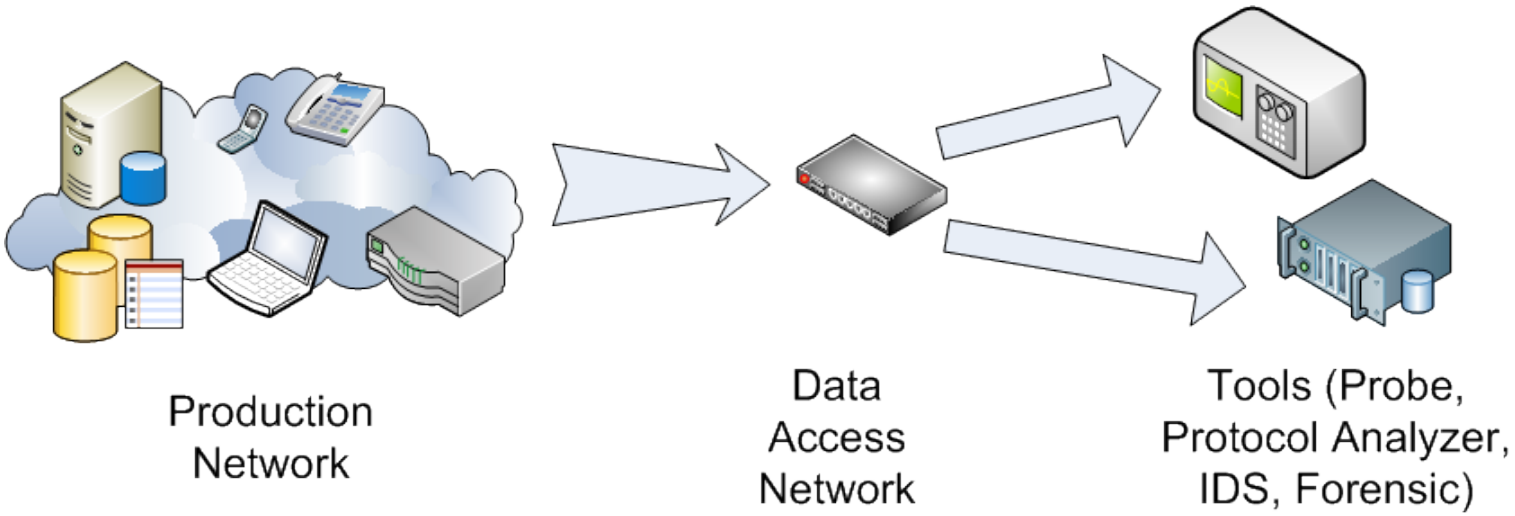
Aufbau einer Monitoring-Umgebung



Monitor/Tool

Capture, Analyse

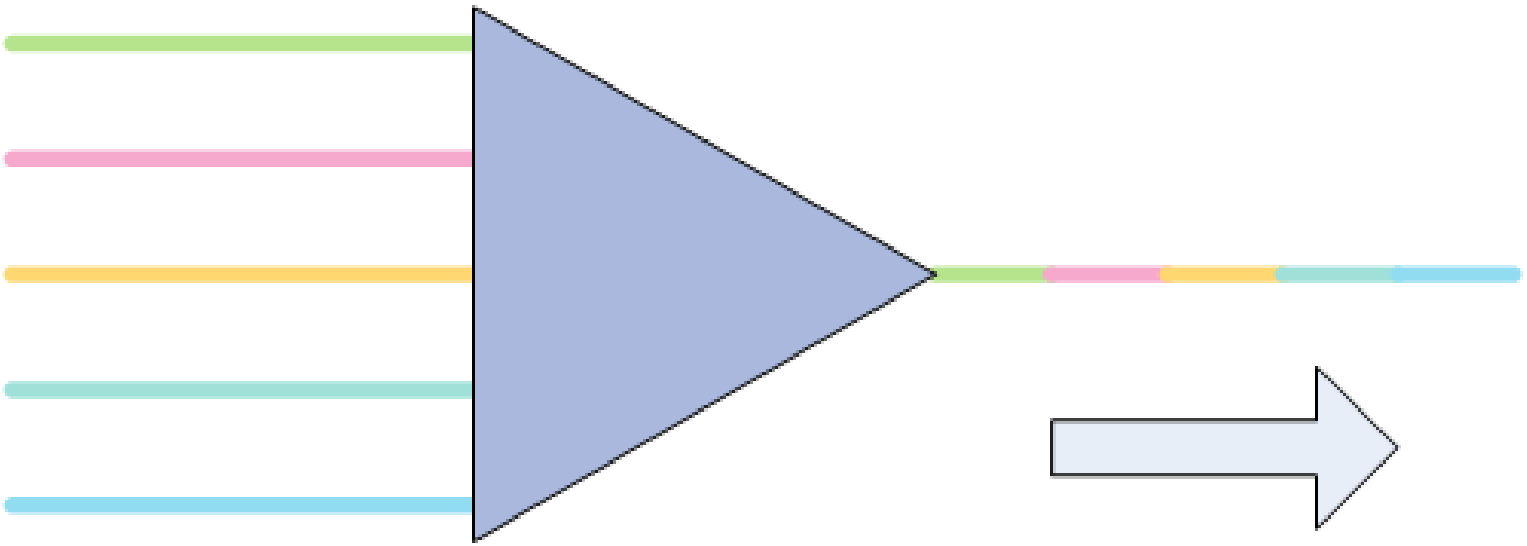
Aufbau einer Monitoring-Umgebung



Data Access

Aggregation, Replication, Filtering

Mehrere Leitungen bündeln



Daten werden zusammengeführt und verdichtet

Überbuchung

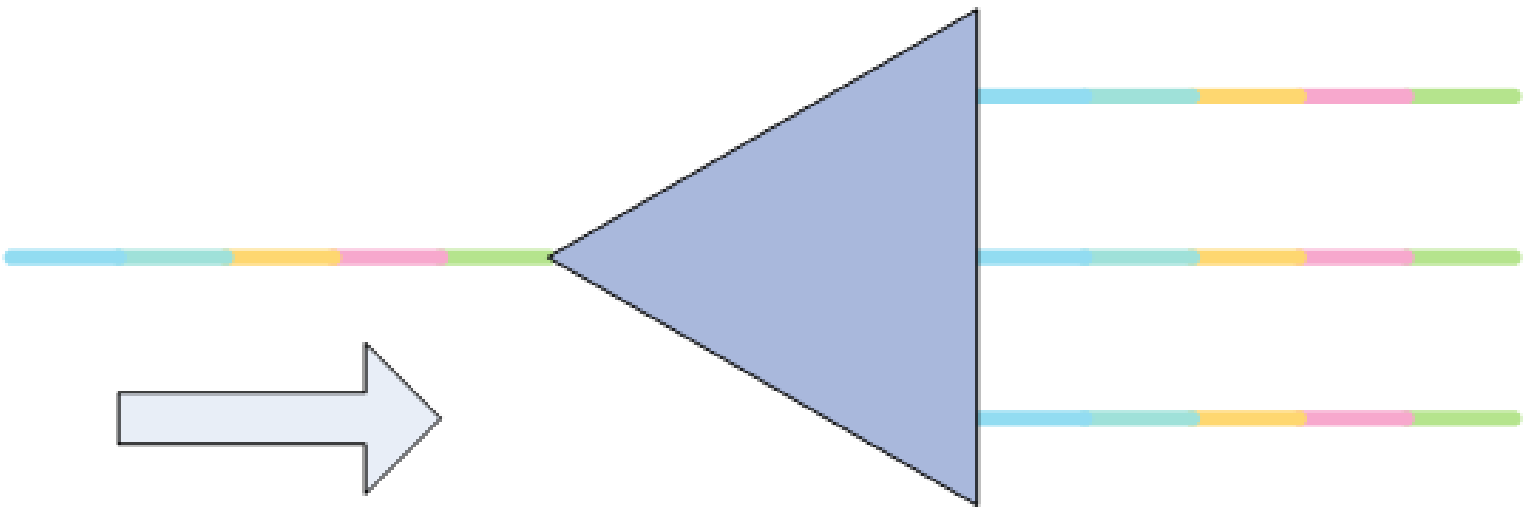
Problem

Überbuchung besteht, wenn mehr Daten aggregiert werden als die Zielleitung aufnehmen kann.

Lösungsansatz

1. „Unnötige“ Daten herausfiltern
2. Auf mehrere Ausgangsleitungen verteilen; Trunking

Eine Leitung auf mehrere verteilen



Daten werden parallel an mehrere Ausgangsleitungen geschickt

Latenz durch Kopie

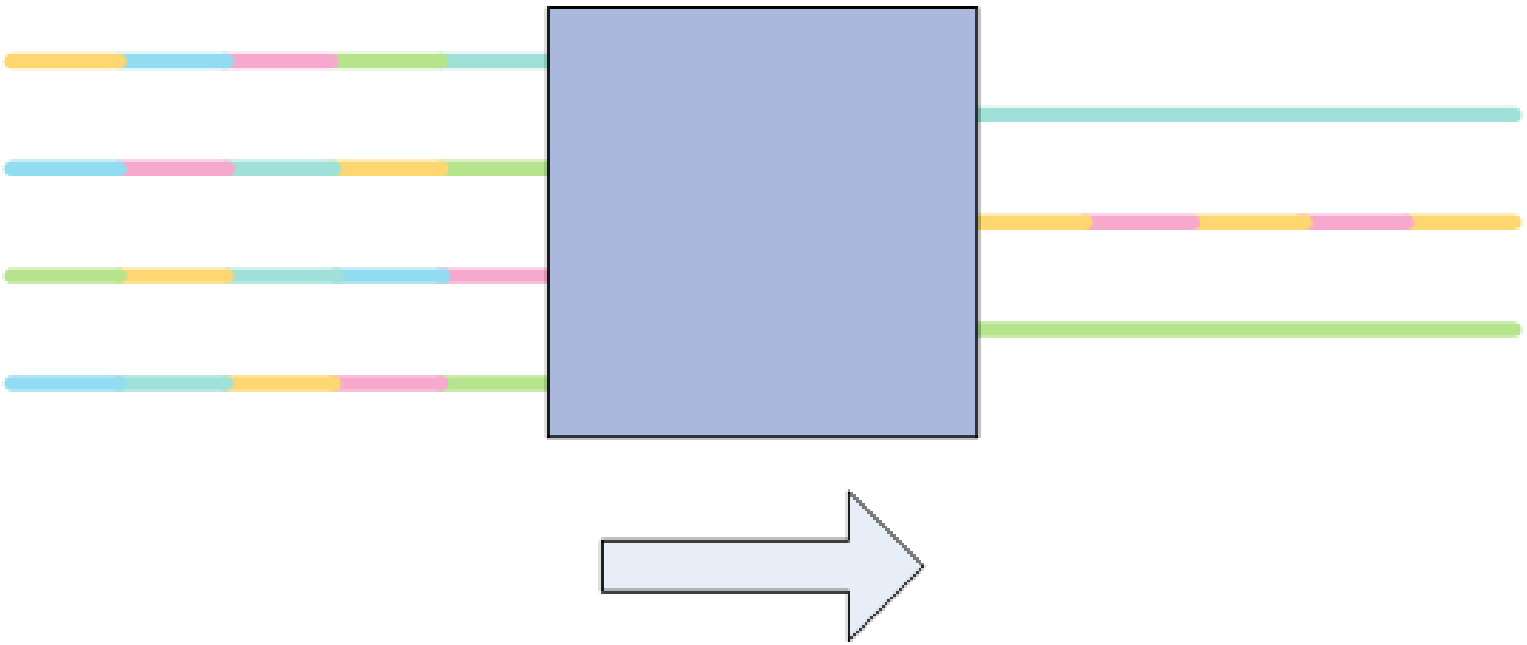
Problem

Eine Kopie verzögert die Datenausgabe. Werden weitere Daten auf demselben Gerät verarbeitet darf der Kopiedatenstrom nicht unterbrochen werden.

Lösungsansatz

1. Pufferspeicher
2. Ausreichend große Backplane; „Zwischenswitches“
3. Priorisierung der Datenströme

Datenstrom verkleinern



Allow-Filter Nur bestimmte Daten verarbeiten

Deny-Filter Bestimmte Daten ignorieren

Latenz durch Rechengeschwindigkeit

Problem

Filter müssen berechnet und jedes einzelne Paket betrachtet werden. Selbst schnelle CPUs stoßen dabei an ihre Grenzen.

Lösungsansatz

1. Filter optimieren
2. Einsatz von FPGA (*Field Programmable Gate Array*) oder CPLD (*Complex Programmable Logic Device*)

Inhalt

Erinnerung: TCP/IP-Referenzmodell

Application Layer
Transport Layer
Internet Layer
Link Layer

Möglichkeiten

- Filter auf allen Schichten möglich
- Reduzierung des Datenstroms?
- $\rightarrow$ Inhaltliche Überwachung des Datenstroms!

Filter im Link Layer

Application Layer
Transport Layer
Internet Layer
Link Layer

MAC-Adressen

- Source-MAC-Address/-Range
- Destination-MAC-Address/-Range

Filter im Internet Layer

Application Layer
Transport Layer
Internet Layer
Link Layer

IPv4

- Source-Address/-Range
- Destination-Address/-Range
- IP-Fragments

Filter im Internet Layer

Application Layer
Transport Layer
Internet Layer
Link Layer

IPv6

- Source-Address/-Range
- Destination-Address/-Range
- Flow Label Field

Filter im Internet Layer

Application Layer
Transport Layer
Internet Layer
Link Layer

Weitere Filter

- Ethertype
- VLAN ID/Range
- DiffServ (DSCP-Byte)

Filter im Transport Layer

Application Layer
Transport Layer
Internet Layer
Link Layer

Filtermöglichkeiten

- Protocol (Next Header)
- Source-Port-Number/-Range (TCP/UDP)
- Destination-Port-Number/-Range (TCP/UDP)
- TCP Control Bit (URG, SYN, FIN, ACK, . . .)
- Type of Service (TOS)
- Time to Live (TTL)

Filter im Transport Layer

Application Layer
Transport Layer
Internet Layer
Link Layer

Stand: Mai 2009

- E-Mail-Adresse (Komplett oder Domain)
- SIP-Nummer (Komplett oder Range)

Pattern-Match-Filter

- Frei wählbares Bitmuster
- Bis zu 16 Byte
- Zusätzlich Offset von bis zu 16 Byte möglich
- Ressourcenhungrig!

Inhalt

Produkte für 10GbE Data Access Network Appliances

Marktführer und Innovativ

- Gigamon GigaVUE-series
- VSS Monitoring

Weitere Produkte

- Net Optics Director
- Anue Systems Tool Aggregator
- Apcon IntellaPatch

Firma

- 2003 gegründet
- Firmengründer kommen allesamt aus dem Analysebereich
- Firmensitz in San Jose, Bay Area, CA

Hardware

- 1G und 10G Lösungen (“1G Legacy Support”)
- Max. 24 $\times$ 10G Ports
- Network- und Tool-Ports frei wählbar
- Full-Line-Speed
- Filter mit Hilfe eines Altera Max II (CPLD)
- Filter werden auf allen Layern unterstützt
- Pattern-Match-Filter
- Eigenes CLI- und WebGUI-basiertes OS
- Stacking möglich

Produktbilder

GigaVUE 420

GigaVUE 2404

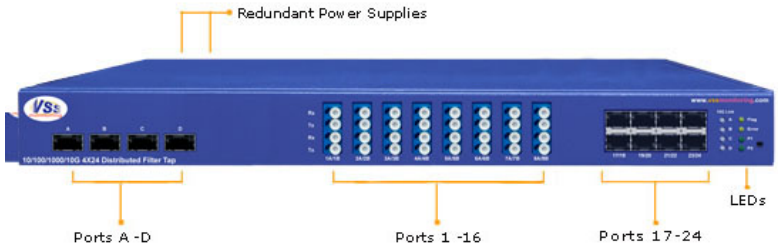
Firma

- 2003 gegründet
- Firmensitz in Burlingame, Bay Area, CA
- VSS steht für „Visibility, Stealth & Security“
- Produktbandbreite von passiven TAPs bis 10G-Filterlösungen

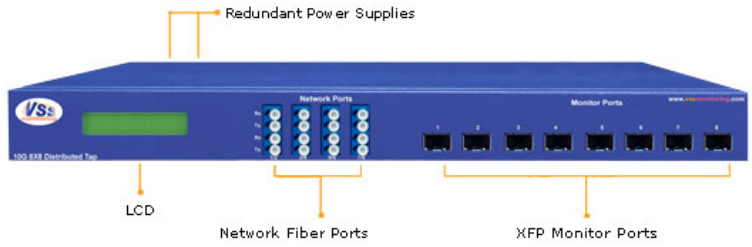
Hardware

- 10M bis 10G Lösungen
- Network- und Monitor-Ports beschränkt frei wählbar
- Benutzerwünsche auf Anfrage realisierbar
- Full-Line-Speed
- Filter mit Hilfe eines FPGA (Aussage Techniker)
- Filter von Link bis Transport Layer
- Pattern-Match-Filter
- Seit 2009 läuft ein Embedded Linux (GPL?)

Produktbilder



VSS 4x24 Distributed Filter TAP (10/100/1000/10G)



VSS 8x8 Distributed Filter TAP (10G)

Inhalt

Kostensenkung und Testsetups

- Aggregieren von Daten, um Probes zu sparen
- Replikation für das Anschließen von Testsystemen oder zur Ausfallsicherheit
- 10G auf 1G Ports verteilen

Im 3G-Sektor

- Monitoren einer Leitung
- Datendurchsatz („Abfallprodukt“)
- Analyse von (Kunden-)Daten nach Reklamation
- Bestimmte Daten separat auswerten

Staat

- Alle Youtube-Videos
- Kompletter Netzwerkverkehr

Inhalt

40G, 100G, Ports und SAN

- Unterstützung für IEEE P802.3ba (40GbE, 100GbE)
- Mehr Ports
- Ausgefeiltere Application-Layer-Filter
- SAN-Unterstützung: Index und Filter auf Dateien

Zusammenfassung

- Aufbau von Data Access Networks
- Filtermöglichkeiten
- Hersteller
- Implementationen
- Ausblick

Vielen Dank für die Aufmerksamkeit