Netzwerkanalyse - Troubleshooting
Die suche nach der Nadel im Heu ???

Patrick Petersson

CEO I CIO
HEXCOM UG

10 Jahre
Berufserfahrung

Entwickler von Messtechnik für IT Netzwerke mit Fokus auf;
Netzwerkanalyse, Netzwerktest und der Netzwerkforensik

AGENDA

- Open Systems Interconnection Reference Modell
- Internet Control Message Protocol
- Die goldene 5 x 3 Regel

Theorie

Der Hilferuf !!! Unser Job an der Front ….

- Netzwerkmesspunkte (SPAN Port vs. Netzwerk TAPs)
- Was mache ich mit TB großen Daten?
- Live Vorführung CommView und NetResident

Praxis

ISO/OSI Model

Open Systems Interconnection Reference Modell

OSI-7-Layer-Model *(Open Systems Interconnection Reference Model)*

Begriffe: Englisch - Deutsch

1 Application Layer	-	Anwendungsschicht
2 Presentation Layer	-	Darstellungsschicht
3 Session Layer	-	Sitzungs- bzw. Kommunikationsschicht
4 Transport Layer	-	Transportschicht
5 Network Layer	-	Netzwerk- bzw. Vermittlungsschicht
6 Data Link Layer	-	Sicherungsschicht
7 Physical Layer	-	Bitübertragungsschicht

PC im Netzwerk A

W http://www.wikipedia.org

Der Benutzer empfängt lediglich die Antwort des Servers ("wikipedia.org"-Startseite). Im Allgemeinen bekommt er von der Schachtelung seines Seitenaufrufs durch die Ebenen seines PCs (abwärts) und vom Parsen der Antwort des Servers zurück durch die Ebenen seines PCs (aufwärts) nichts mit !

Server schickt die entsprechenden Daten über die selbe Methode zurück. (s.u.)

Server im Netzwerk A

Zusammenbau des Pakets:
(Package Assembling/Formatting)

Datenpaket z.B. Serverrequest

	OSI-Layers
Funktionsaufruf durch den Anwender — AH + Daten	7 Application
Umwandlung der Daten ein eigenes Format — PH + AH + Daten	6 Presentation
Verbindungen zwischen den Endsystemen — SH + PH + AH + Daten	5 Session
TH + SH + PH + AH + Daten Datenpaket wird einer Anwendung zugeordnet	4 Transport
NH + TH + SH + PH + AH + Daten Erstmalige logische Adressierung der Endgeräte	3 Network
DH + NH + TH + SH + PH + AH + Daten Physikalische Adressierung mit Fehlererkennung, Fehlerbehebung und Datenflusskontrolle	2 Data Link
PhH + DH + NH + TH + SH + PH + AH + Bits Definition der elektrischen, mechanischen und funktionalen Schnittstelle zum Übertragungsmedium	1 Physical

Zusammensetzung der Abkürzungen oben :
Anfangsbuchstabe der Schicht und "H" für Header.
z.B. Application Header = AH

Header "Addition"

Schichten werden ineinander eingebettet.

Das Datenpaket wird nach unten hin größer.

Einordnung der Orientierung	Standard	TCP/IP Schicht	Einordnung der Verbindung	Protokoll
Anwendungs-orientiert	FTAM	Anwendung	Ende zu Ende (Multihop)	HTTP FTP HTTPS NCP
	ASN.1			
	ISO 8326			
Transport-orientiert	ISO 8073	Transport		TCP UDP SPX
	CLNP	Internet	Punkt zu Punkt	ICMP IGMP IP IPX
	HDLC	Netzzugang		Ethernet Token Ring FDDI ARCNET
	Token Bus			

Request Antwort

Das verschachtelte Datenpaket wird entpackt.

Somit wird es wieder kleiner.

Header "Subtraktion"

7 6 5 4 3 2 1

Parsen/Zerlegen der Daten durch die Ebenen

physikalische oder logische Verbindung

Tatsächlicher Datendurchsatz / Übertragungspfad

ICMP im Detail

Eckdaten

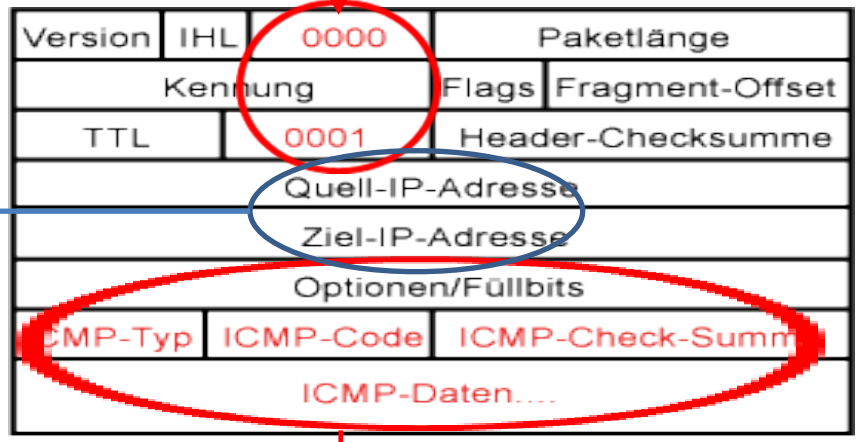
Bestandteil des Internet Protocols (IP)

ICMP hat keine eigene Header-Struktur,
stattdessen wird der Standard-IP-Header genutzt

Aufbau einer Internet Protocol Adresse

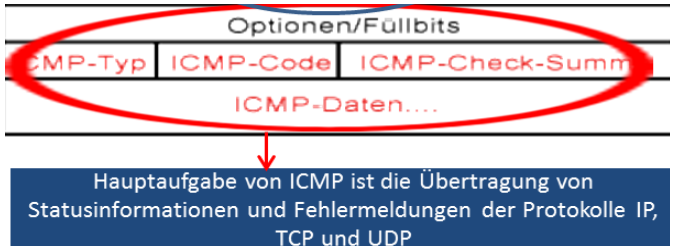
	Binär	Dezimal
IP-Adresse	10001101 01011001 01000000 00000001	141. 89. 64. 1
Netzmaske	11111111 11111111 00000000 00000000	255.255. 0 . 0
	Netzanteil / Hostanteil	Netz / Host
IP-Adresse	00111010 00010001 10000011 00101100	58. 17.131. 43
Netzmaske	11111111 11111111 11111111 00000000	255.255.255. 0
	Netzanteil / Hostanteil	Netz / Host
IP-Adresse	01111011 00000101 01100100 00000010	123. 5 .100. 2
Netzmaske	11111111 11111111 11110000 00000000	255.255.240. 0
	Netzanteil / Hostanteil	Netz / Host

IP Header-Feld Type-of-Service wird auf Wert "0000„ geseztz.
IP-Header-Feld Protokoll wird auf Wert "0001„ gesetzt = ICMP



ACHTUNG:
ICMP wird jedoch als
eigenständiges Protokoll behandelt

Hauptaufgabe von ICMP ist die Übertragung von Statusinformationen und Fehlermeldungen der Protokolle IP, TCP und UDP

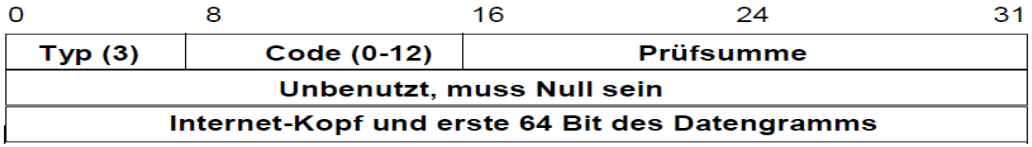


Beispielmeldungen aus der täglichen Praxis

Meldungen über nicht erreichbare Destinationen

Wenn ein IP-Paket nicht weitergeleitet werden kann, wird eine entsprechende Fehlermeldung erzeugt.

0	Netz nicht erreichbar	7	Zielrechner unbekannt
1	Rechner nicht erreichbar	8	Zielrechner isoliert
2	Protokoll nicht erreichbar	9	Netzkommunikation unerwünscht
3	Port nicht erreichbar	10	Rechnerkommunikation unerwünscht
4	Fragmentierung benötigt	11	Netz für diesen Dienst unerreichbar
5	Falsche Quell-Route	12	Rechner für diesen Dienst unerreichba
6	Zielnetz unbekannt		



Die Goldene 5x3 Regel

5 Goldregeln

>> Bevor ich überhaupt an die Netzwerkanalyse im Live Betrieb denke <<

I. Capture Engine auf "Clear Buffer" stellen *(nicht "Wrap Buffer")*

II. Alle Pakete aufzeichnen *(keine Paket-Filter, keine Protokoll-Filter)*

III. Alle Pakete in voller Länger aufzeichnen ***(kein "Packet Slice")***

und die 3 größten dont´s !!!

IV. Messpunkt genauestens dokumentieren (SPAN-Port / TAP etc.)

V. Ort der Messung muss dem vermuteten Fehler angemessen sein

Welche Messpunkte?

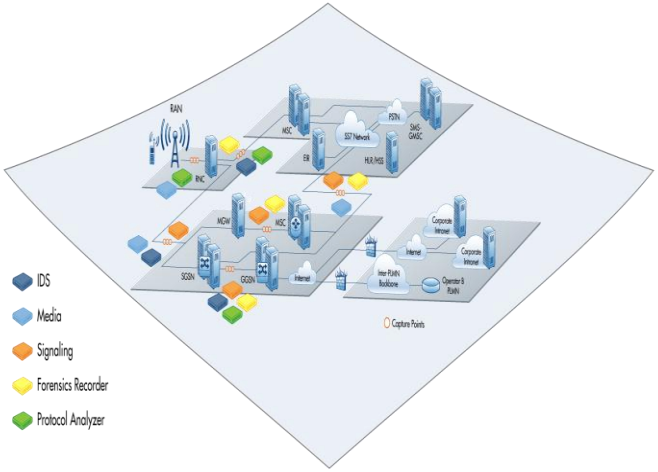
Welche Topologien?

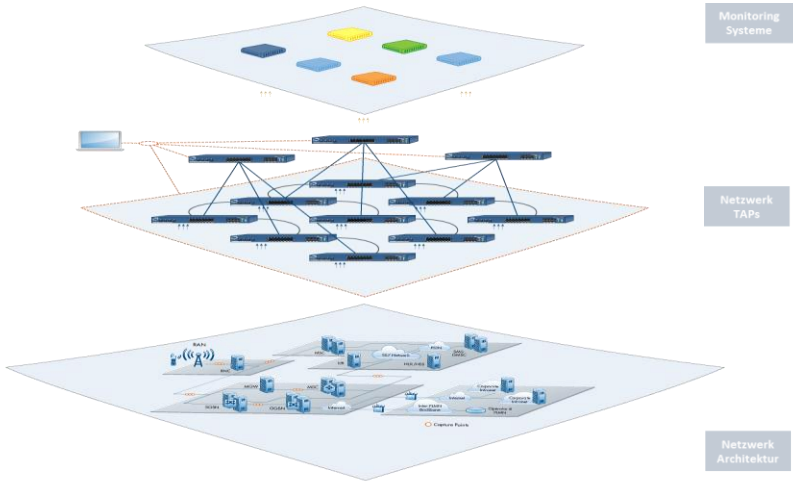
Der Hilferuf
unser Job an der Front

Zugangspunkte für die Netzwerkanalyse

„ Netzwerkmonitoring 1.0 “
Span Port, Mirror Port, Server, On the Desk etc…

„ Netzwerkmonitoring 2.0 “
Netzwerk TAPs, Monitoring TAPs, Distributed Analysis etc…



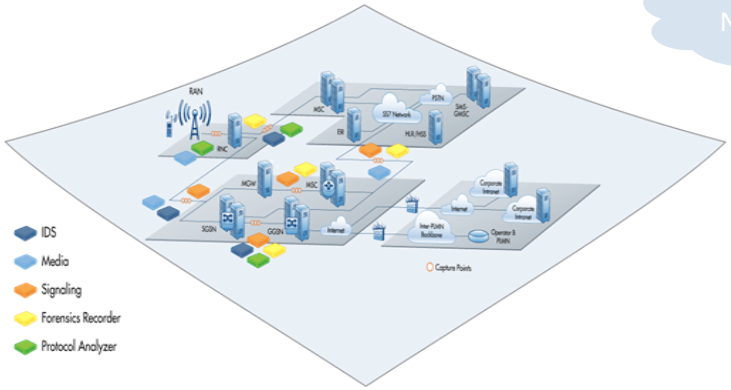


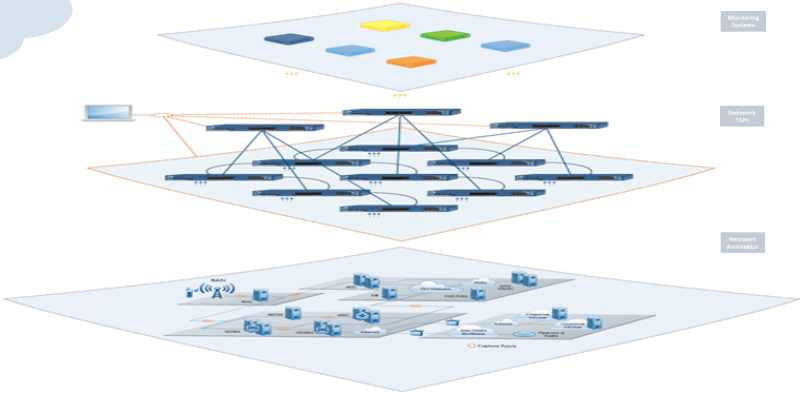
Für und Gegenargumente (Dauer 1 Tag) - Folgende Leitsätze daher:

Wenn erkennbar ist, dass es sich um "logische" Probleme handelt, startet man mit einem SPAN/Mirror Port.
Wenn es im Laufe der Untersuchung Hinweise auf "harte" Netzwerkprobleme gibt, wechselt man auf einen TAP.
Wenn von Anfang an klar ist, dass ein SPAN/Mirror Port Probleme bereiten dann startet man gleich mit einem TAP

HEXCOM

Erfasste Netzwerkdaten





Was mache ich mit TB große Daten ?

Wie finde ich was mich Interessiert ?

Wie Überwache ich Unternehmenskritischebereiche?

NetResident

Performante Software Tools helfen beim Bewerten der Daten und bei der…

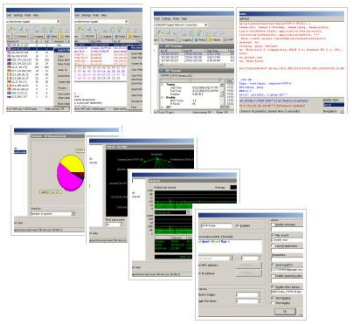
CommView

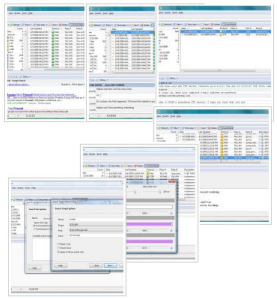
Network Analyzer

… Weitergabe an Industriestandard Analysetools …

… in vertretbaren großen Daten-blöcken

WIRESHARK





Live Vorführung
CommView und NetResident

CommView Testversion: www.hexcom.de/produkte/tamosoft/commview
NetResident Testversion: www.hexcom.de/produkte/tamosoft/netresident