„Capture Guidelines“

Stand: 2009-11-24

Vorwort & Hinweis auf TraceCommander

Synapse:Networks gibt die vorliegenden *Capture Guidelines* seit vielen Jahren an Partner und Kunden heraus, um die Aufzeichnung von Messdaten in korrektem Format zu gewährleisten und um Hilfestellung zu geben beim Einrichten der Messpunkte (Mirror Ports etc.).

Inzwischen raten wir dringend dazu, Messdaten nur noch mit dem von **Synapse:Networks** geschaffenen LAN-Analyzer **TraceCommander** aufzuzeichnen.

TraceCommander leitet den Anwender in seinem Modul **CaptureWizard** durch die nicht immer triviale Konfiguration des Capture-Jobs und bietet Funktionen, die insbesondere für Dauer-Aufzeichnungen extrem wichtig, aber bei Produkten des Mitbewerbs regelmäßig nicht zu finden sind (Verwaltung der Messdaten, Nachtschaltung, Vorauswertung mit **MiniMagic** u.a.m.).

Dank **TraceCommander** sind in den meisten Fällen die Teile der Capture Guidelines, die sich mit der Konfiguration des LAN-Analyzers zur Messdaten-Aufzeichnung beschäftigen, gegenstandslos bzw. durch die Menü-Führung des **CaptureWizard** -Moduls ersetzt worden.

Lediglich das Setzen des Messpunktes, etwa über einen Mirror-Port, muss weiter mit Bedacht vorgenommen werden. Aber auch hier bietet der **CaptureWizard** Hilfe, da ein „**Link+Capture Test**" die Qualität der vom Messpunkt gelieferten Daten bewertet, etwa: Handelt es sich wirklich um einen Mirror Port (und nicht etwa nur um einen unkonfigurierten Switch-Broadcast-Port)? Handelt es sich wirklich um Rx/Tx-Daten?

Info + Download → www.tracecommander.net

Vorbereitungen durch den Kunden / Vorbereitung der MessPunkte

Synapse:Networks ist darauf angewiesen, dass seitens des Kunden die notwendigen und ggf. abgesprochenen MessPunkte vorbereitet bzw. eingerichtet werden.

Technische Bereitstellung durch den Auftraggeber

Der Kunde stellt für die Messungen den Zugang zu den Datenkommunikationsanlagen sowie den ebenfalls nötigen Messpunkt sicher.

Der Kunde stellt weiterhin das Personal zur Verfügung, das zur Einrichtung der MessPunkte sowie zur Beschaffung der erforderlichen Auskünfte und Dokumentationen notwendig ist.

Ein Vertrag zwischen Kunde und Synapse:Networks, der eine LAN-Analyse zum Gegenstand hat, beinhaltet immer, dass der Kunde die MessDaten zur Verfügung stellt, sei es aktiv (Zugang zum Datennetz über Messpunkte), sei es passiv (Überlassung von Messdaten, die der Kunde selbst gesammelt und gespeichert hat).

Klärung der Begriffe

Unter **"Messgerät"** im Sinne dieses Vertrages ist zu verstehen: Üblicherweise sog. Protokoll-Analysatoren (Ethereal, EtherPeek, Observer, etc).

Bei Messungen durch **Synapse:Networks** vor Ort gilt:

Die Messung erfolgt jeweils an einem vom Kunden zur Verfügung gestellten und eingerichteten Messpunkt, das Messgerät wird im Regelfall von **Synapse:Networks** gestellt bzw. mitgebracht.

Unter **"Messpunkt"** im Sinne dieses Vertrages ist zu verstehen: Ein Daten-Übergabe-Punkt, an dem Kommunikationsdaten des Daten-Netzes des Kunden zum angeschlossenen Messgerät hin zum Zwecke der Aufzeichnung und Auswertung ausgegeben werden. Messpunkte sind meistens in Form sog. Verteiler gegeben (Hubs, Repeater, Switches, Router) und können wie folgt beschaffen sein:

1. **Mirror-Ports**, bei denen der Daten-Verkehr eines Verteilers auf die Anschlußbuchse des Analyzers in Kopie ausgegeben wird.
2. **Ethernet-Repeater** (10/100 Mbps) oder Token-Ring **Ringleitungsverteiler** (4/16 Mbps) im Halb-Duplex-Modus, die den gewünschten Datenverkehr bedingt durch ihre Bauweise auf allen Buchsen ausgeben.
3. Im Einzelfall (und nur nach Absprache) sog. **Media-TAPs** oder **Media-Splitter**, die eine Voll-Duplex-Leitung in Rx/Tx-Buchsen zwecks Datenausgabe auftrennt. Da hier erheblicher Zusatzaufwand nötig ist, um die so gewonnenen Messdaten auswerten zu können (was zudem nur mit starken Einschränkungen möglich ist), oder wegen des Erfordernisses zusätzlicher Hardware-Module, bedarf es der Absprache im Einzelfall.
4. Der Zugriff auf **RMON-Agenten** via SNMP. Da diese Methode weniger zuverlässig ist und vor allem im Zeit- und Mengen-Verhältnis beschränkt (und außerdem wenig verbreitet) ist, sollte sie nur nach Absprache bzw. ersatzweise beim Fehlen besser geeigneter Messpunkte angewendet werden.

Bei Zusendung von Messdaten auf CD-ROM hat der Kunde für jede einzelne Messung den genauen Messpunkt gegenüber **Synapse:Networks** zu dokumentieren, da sonst die Auswertung eingeschränkt oder sogar unmöglich sein kann.

Unter **"Messdaten"** im Sinne dieses Vertrags ist zu verstehen: Insofern Inhalte des Datenverkehrs am Messpunkt gespeichert werden, handelt es sich um "Messdaten". Diese können vorliegen in Form von Binär-Daten (Traces) oder Statistiken (z.B. CSV-Dateien) oder Log-Dateien (z.B. Server-Error-Logs).

Unter **"Auswertung"** im Sinne dieses Vertrages ist zu verstehen: Die Durchsicht der Messdaten, das gezielte Suchen nach Auffälligkeiten / Fehlern sowie das Protokollieren der Ergebnisse in Form von Messberichten. Die Auswertung kann je nach Anlaß und Gegenstand voll- oder teil-automatisch bzw. voll- oder teil-manuell erfolgen, wobei es **Synapse:Networks** überlassen bleibt, die Vorgehensweise zu bestimmen.

Unter **"Messbericht"** ist zu verstehen: Die vorgelegten Auswertungen, ggf. mit weiteren Stellungnahmen oder Zusammenfassungen.

Richtlinien zum Einrichten von Messpunkt(en) und Messrechner(n)

Grundregeln

Folgende Erfordernisse sind gegeben, um die richtigen Daten am richten Ort im richtigen Format aufzuzeichnen:

Das Setzen des Mirror Ports:

- Rx/Tx: Der Mirror-Port muss den LAN-Traffic beider Richtungen ausgeben, also Rx und Tx.
- Eine Ausnahme ist dann gegeben, wenn alle Ports eines Switches ausgespiegelt werden (oder alle Ports eines VLANs): Dann dürfen nur Rx –oder- nur Tx-Pakete ausgegeben werden, weil sonst die LAN-Pakete doppelt in der Aufzeichnung wären: Mal als Rx-Ereignis, mal als Tx-Ereignis des Switches.
- VLANs: Es kann sinnvoll sein (muss aber nicht), auch die VLAN-Tags auszugeben. Dies ist zu vorab klären.

Das Einrichten der *Capture Engine* (der Aufzeichnungs-Software):

- Es müssen alle LAN-Pakete aufgezeichnet werden (keine Online- bzw. Capture-Filter).
- Es müssen die LAN-Pakete in voller Länge aufgezeichnet werden (kein „Packet Slice“).
- Es muss der Packet-Buffer (Capture Buffer) als „Clear Buffer“ konfiguriert sein (nicht als „Wrap Buffer“ / „Ring Buffer“).
- Es sollten je Aufzeichnungs-Datei (Trace File) zwischen 50.000 und 100.000 LAN-Pakete gespeichert sein. – Dies führt in der Praxis bei einer üblichen Client-Server-Landschaft meistens zu einer Datei-Größe von ca 32 MB. Bei Terminal-Server-Traffic ist es bisweilen nötig, auf bis zu 4 MB Datei-Größe herunter zu gehen, bei der Aufzeichnung von Router-Traffic an der WAN-Schnittstelle desgleichen.
- Die Datei-Namen der Capture-Files müssen bei alpha-numerischer Sortierung der chronologischen Reihenfolge entsprechen.

Bitte lesen Sie hierzu den Abschnitt:

> Frage & Antworten: "Welche Einstellungen sollte die Capture_Engine haben?"

Logischer Messpunkt → Auswahl des Messpunktes

MessPunkt = Config- und Domain-Server

Es wird grundsätzlich angestrebt, früh morgens das LOGIN bzw. die Netzwerk-Anmeldung der Clients mitzulesen.

Hierzu sollte der LAN-Verkehr der folgenden Server (sofern vorhanden) mitgelesen werden:

- BOOT / DHCP Server
- WINS Server
- DNS Server
- Kerberos Server
- Active Directory Server (ADS)
- Windows PDC / BDC Server
- NetWare NDS Server
- ggf. weitere, bei LOGIN beteiligte Server.

Die einfachste Variante ist, vom Core-Switch aus den Uplink zu einer repräsentativen Client-Workgroup am Mirror-Port auszuspiegeln. Da hier praktisch der gesamte Client-Traffic zu sehen ist (und aufgezeichnet wird), ist auch der Datenverkehr der Name-Server und Config-Server zumindest diesen Clients gegenüber enthalten. In den meisten Fällen reicht dies vollauf, um das Verhalten dieser Server ausreichend zu dokumentieren.

Andere Varianten:

Da das LOGIN erfahrungsgemäß wenig Datenverkehr umfasst, können insbesondere die Name Server / Config Server (DHCP, DNS, WINS) über den selben Messpunkt abgegriffen werden, sofern dies anlagentechnisch möglich ist, etwa: über den selben Fast-Ethernet-Hub (sofern mit Half-Duplex Fast-Ethernet angebunden), oder über das Spiegeln mehrerer Server-Ports auf einen gemeinsamen Switch-Mirror-Port.

Es können auch mehrere Server auf einen gemeinsamen Fast-Ethernet-Hub (half-duplex Repeater) gelegt werden, sofern die zu erwartenden Datenraten dies zulassen.

MessPunkt = Name Server

Bei Messungen, welche die Namensdienste (Name Services) zum Gegenstand haben, ist zu berücksichtigen:

In den Auswertungen, die das TraceMagic-Modul "HostMagic" liefert, sind die Ergebnis-Statistiken der WINS/DNS-Aktivitäten nur bewertbar, wenn klar ist (durch einwandfreie bzw. genaue Dokumentation), wo genau der Messpunkt war.

Dies zielt z.B. darauf ab, dass WINS-Requests, die per LAN-Broadcast gesendet werden, überall im Netz verbreitet werden (und somit auch bis hin zum Messpunkt) - aber ein etwaiger WINS-Reply eines WINS-Servers (oder sonstigen WINS-Teilnehmers) muss durchaus nicht notwendig ebenfalls am MessPunkt vorbei kommen.

Dies kann z.B. in einer Load-Balancing-Umgebung geschehen, und zwar in der Art, dass die WINS-Requests Verkehrsweg A nehmen ("links herum", also über Weg A), die WINS-Replies jedoch den Verkehrsweg B ("rechts herum", also über Weg B); und wenn nun der Messpunkt an Verkehrsweg A liegt, ist in den Messdaten nichts von dem zu sehen, was über Verkehrsweg B lief.

Die Deutung der Daten ist später ggf. erheblich behindert, wenn der MessPunkt nicht vollständig dokumentiert wurde.

Daher müssen Messpunkte, welche die Namensdienste im Blick haben, wohl überlegt und gut dokumentiert sein.

Messungen unmittelbar vor WINS-Server und DNS-Server sind daher immer hilfreich.

Siehe hierzu auch weiter unten die Ausführungen zu HSRP, Load Balancing, Adapter Teaming etc.

MessPunkt = Datenserver

Den Applikationen entsprechen in aller Regel bestimmte Applikations-Server bzw. Daten-Server.

Je nach Aussagen der Anwender darüber, bei welchen Applikationen Probleme auftreten, sollte auch der LAN-Verkehr dieser Daten-Server mitgelesen werden.

Auch hier sind die Mirror-Ports an den Switches entsprechend zu schalten.

Es können auch mehrere Server auf einen gemeinsamen Fast-Ethernet-Hub (half-duplex Repeater) gelegt werden, sofern die zu erwartenden Datenraten (und die Server-Link-Einstellungen) dies zulassen.

Für den Fall, dass der Server mit Adapter-Teaming arbeitet, sind besondere Maßregeln zu berücksichtigen (s.u.).

MessPunkt = Client-Workgroups

Das Geschehen lässt sich nur verstehen, wenn es auch aus der Sicht der Client-PCs nachvollzogen wird. Daher sollte der LAN-Traffic von zwei, drei Client-Workgroups (möglichst repräsentativ) aufgezeichnet werden.

Ideal ist es, den Uplink des jeweiligen Workgroup-Switches zum Core-Switch auf den Mirror-Port auszuspiegeln, da somit der gesamte LAN-Verkehr der Client-Workgroup aufgezeichnet werden kann.

Es können auch mehrere Clients auf einen gemeinsamen Fast-Ethernet-Hub (Half-Duplex Shared-Media Repeater) gelegt werden, da die Datenraten der Clients dem meistens nicht entgegen stehen.

Die Messung über einen Hub hat u.a. wesentlich den Zweck, auch etwaigen Quer-Verkehr von-Client-zu-Client nachvollziehen zu können; dies wäre nicht möglich, wenn nur der Uplink (per Mirror-Port) Gegenstand der Aufzeichnung wäre.

Der Grund für diese Maßnahme liegt darin, dass Windows-Clients (insbesondere, wenn sie mit NetBIOS arbeiten) bei Mängeln in den Namensdiensten die Neigung entwickeln, ihre Eingliederung in die sog. "Netzwerk-Umgebung" (Network Neighbourhood) durch Abfragen bzw. Meldungen von Client zu Client zu organisieren.

MessPunkt = Mirror Ports

Die einfachste und schnellste Vorgehensweise ist die Messung über Mirror-Ports.

Im Gegensatz zu Media-Splittern / Taps, die in der Regel nur am Wochenende oder nachts eingerüstet werden können, sind Mirror-Ports jederzeit beliebig verfügbar, da sie lediglich einer logischen Schaltung bedürfen.

Taps sind eher für den ständigen Verleib in einem Server-Link oder Inter-Switch-Link gedacht; dies ist durchaus sinnvoll, aber für externe Dienstleister, die kurzfristig einrücken, nicht anwendbar.

Nun Einzeilheiten zur MessDaten-Aufzeichnung via Mirror-Port:

Technischer Messpunkt → Auswahl des Mediums

Media Splitter / Tap

Messungen über Media Splitter bzw. Taps haben Vorteile und Nachteile.

Vorteile:

Im Gegensatz zum Mirror-Port gibt ein Tap auch physikalisch defekte Frames aus. - Die Packets werden im Falle von VLAN-Trunks immer im Original-Format *mit* VLAN-Tag ausgegeben, was beim Mirror-Port oft nicht erwünscht ist, oft aber auch schon gar nicht möglich ist. - Die Leistung des Switches wird nicht beeinträchtigt, da ein unabhängiges Modul die Arbeit leistet und nicht die CPU des Switches bzw. Routers.

Nachteile:

Ein Tap kann nicht kurzfristig in die Leitung zwischen Server und Switch eingebaut werden, da zu befürchten steht, dass der Server danach den Physical-Link nicht wieder korrekt aufbaut (sondern im schlimmsten Fall sogar abstürzt) - mit der Folge, dass Client-Server-Sessions verloren gehen; und mit der Folge, dass deswegen der Server herunter gefahren und neu gebootet werden muss.

Taps eignen sich daher für den ständigen, festen Einbau, nicht aber für den externen Dienstleister, der kurzfristig einrückt und an vielen, verschiedenen Messpunkten handlungsfähig sein muss.

Viele Tap-Fabrikate erlauben nur, entweder den Rx-Kanal oder den Tx-Kanal zum LAN-Adapter des Analyzers zu führen, nicht aber Rx/Tx gemeinsam. Die daraus entstehende Aufzeichnung ist daher praktisch unbrauchbar („ony-way traffic").

Diese Einschränkung lässt sich nur umgehen

- (a) mit einem Dual-Port-Adapter im Analyzer, der somit sowohl den Rx-Kanal wie auch den Tx-Kanal aufnehmen kann,
- (b) mit einem Luxus-Tap, der von sich aus schon die Rx/Tx-Kanäle wieder zusammen führt und als gesammelten Datenstrom zum Analyzer hin ausgibt.

Im Falle von (b) kann Buffer-Overflow auftreten, da 2 x 1 Gbit/sec die Kapazität der Ausgabe-Leitung (nur 1 Gbps) überschreitet.

Produkt-Beispiele und weitere Erläuterungen (ohne Gewähr):

http://www.networkcomputing.de/das-ohr-auf-der-leitung/
http://www.network-taps.de/products/products_aggregationtaps.php
http://www.brandt-data.de/ethernet/profitap/profitap.html

PC-Adapter-Bridge

Ab Windows-XP ServicePack-2 können mehrere PC-Netzwerk-Adapter zu einer sog. „Bridge" (Brücke, Überbrückung) zusammen geschaltet werden; der PC agiert dann wie ein Switch.

Messtechnisch bedeutet dies: Der PC bzw. Laptop kann in die Leitung zwischen zwei Switches oder zwischen Server und Switch eingeschliffen werden; der den PC durchlaufende Datenverkehr kann dann aufgezeichnet werden.

Die Erfahrung zeigt: Solange kein extrem starker Datenverkehr gegeben ist, hat sich diese Art der Aufzeichnung als gute Ersatz-Technik erwiesen, wenn weder Mirror-Port, noch Media-Splitter/Tap gegeben sind.

Hubs: 10/100 Ethernet Repeater

Bei Verwendung eines Hubs (Shared-Media Repeater) muss folgendes berücksichtigt werden:

- Ein Hub arbeitet halb-duplex und "gestattet" daher Paket-Kollisionen, die in einem *Switched Network* nicht mehr möglich sind. Sollte der Hub nur zu Mess-Zwecken eingebaut worden sein, müssen daher die Kollisionen gedanklich heraus gerechnet werden, da sie ohne Messung in der reinen Switching-Umgebung gar nicht vorhanden gewesen wären.
- Soll ein Hub zwischen Switch und Endgerät(e) geschaltet werden, muss berücksichtigt werden, dass ggf. Endgeräte und/oder Switch-Port fest eingestellt sind auf "full-duplex" statt "half-duplex" oder "Auto-Negotiation / Auto-Sensing". Das Zwischenschalten eines Hubs kann also ggf. erfordern, dass der Switch-Port bzw. die LAN-Adapter der Endgeräte neu konfiguriert werden, um mit dem Repeater/Hub konform arbeiten zu können. Geschieht dies nicht, kommt ggf. kein Physical-Link zu Stande.

Ansonsten sind Messungen über Hubs simpel und schadlos, so lange die Kollisionen nicht übermäßig auftreten.

Da aber Halb-Duplex-Hubs nicht mehr im Handel erhältlich sind, können nur noch alte, historische Geräte verwendet werden. Diese Technik stirbt also aus.

RMON Agent

Messungen über RMON Agent sind kaum empfehlenswert, da die einlesbare Datenmenge extrem gering ist und daher nur kurze Zeitfenster abgebildet werden und daher kaum sinnvolle Aussagen getroffen werden können.

Für Stichproben kann das hinnehmbar (ggf. sogar notwendig) sein; für wirklich "echte" Messungen sind sie nicht brauchbar.

Adapter-Teaming

Manche Server sind mit einem Doppel-Adapter in *der* Form ans Netzwerk angeschlossen, dass je 1 LAN-Adapter auf jeweils einen anderen Switch geführt ist. Auf diese Weise wird Redundanz (Ausfall-Sicherheit) erreicht sowie je nach Architektur zusätzlich noch ein Load-Balancing (gleichmäßige Last-Verteilung).

Hier ist messtechnisch zu erwägen, eine „3M"-Messung anzulegen.

3M-Messung: 3-Mirror-Port-Messung (2 Server-Switches, 1 Capture-Switch)

3M-Capturing

Es kann ggf. erforderlich bzw. hilfreich sein, eine Messung über 3 Mirror-Ports durchzuführen.

Dies ist dann der Fall, wenn der Datenverkehr eines Servers aufgenommen werden soll, der mit Adapter-Teaming arbeitet und also an zwei verschiedene Switches angeschlossen ist und der beide Switches aktiv nutzt, was besagt, dass nicht nur der erste Adapter arbeitet und der zweite stand-by arbeitet (passiv, bis ein Ausfall von Adapter Nr. 1 das Failover verlangt), sondern dass beide Adapter arbeiten (in der Regel mit einem Load-Balanding).

Würde nun nur ein einziger Mirror-Port geschaltet an einem der beiden beteiligten Switches, so würde nur die Hälfte des Server-Traffics erfasst und aufgezeichnet.

Um sämtlichen Server-Traffic aufzuzeichnen, ist wie folgt vorzugehen:

An beiden Switches wird ein Mirror-Port gelegt, und zwar in der Art, dass jeweils einer der beiden Server-Adapter gespiegelt wird.

Von beiden Mirror-Ports wird eine Kabel-Verbindung hergestellt zu einem dritten Switch, der ausschließlich nur zur Messung aufgebaut ist und ausschließlich die Mirror-Port-Ausgaben der beiden Server-Switches aufnimmt.

Dieser dritte Switch vereinigt sodann die beiden Rx-Datenströme zu einem einzigen Tx-Datenstrom, indem die Mirror-Port-Daten der beiden Server-Switches auf den Mirror-Port des dritten Switches gelenkt werden.

An diesem Mirror-Port des dritten Switches ist dann der LAN-Analyzer bzw. die Capture-Engine angeschlossen.

Diese "3M"-Messung verlangt zwar etwas Aufwand, ist aber gut einsetzbar.

Eine andere Variante wäre, zwei Taps in den beiden Adapter-Links des Servers einzubauen und sodann die Traffic-Ausgaben dieser beiden Taps auf den Capture-Switch zu legen. Ob dann jedoch die Zeit-Synchronisation der Pakete noch stimmt, ist nicht hinreichend klar.

Eine weitere Variante wäre, den Mirror-Port des einen Server-Switches auf einen Rx-Port des zweiten Server-Switches zu legen; dort werden dann der vom ersten Switch kommende Datenstrom sowie die vom zweiten Switch empfangenen Server-Daten gemeinsam auf einen Mirror-Port gelegt.

Das Zwischenschalten eines dritten Switches (Capture-Switch) muss berücksichtigen, dass ggf. VLAN-Packets, die statt max. 1.518 Octets wegen des VLAN-Headers bis zu max. 1.522 Octets lang sein können, von einem Non-VLAN-Switch nicht korrekt behandelt werden.

Mirror Ports: Besonderheiten und Einschränkungen

Einschränkungen müssen immer bedacht sein, die eine Messung via Mirror-Port mit sich bringt:

- Physikalisch defekte Frames werden i.d.R. am Rx-Port des Switches verworfen und daher nicht am Tx-Port ausgegeben, und somit auch nicht am Mirror-Port.
- VLAN-Management-Packets bzw. Trunk-Management-Packets werden ggf. nicht am Mirror-Port ausgegeben.
- Sind Server via Adapter-Teaming an zwei verschiedenen Switches angeschlossen, bringt der Mirror-Port nur eines Switches ggf nur die Häfte des Server-Traffics in die Aufzeichnung.
- Ggf. ist eine Messung über "Media Splitter / Tap" zu erwägen (siehe unten); ggf. sollte mit einer 3M-Messung gearbeitet werden ("3M": siehe unten).

Mirror Port: Rx/Tx

Zu Messungen via Mirror-Port müssen die in Frage kommenden Knotenpunkte (Router, Switches) in der Lage sein, aktive Rx/Tx-Ports auf Mirror-Ports auszuspiegeln.

Es ist ungenügend, wenn der Switch nur Rx oder nur Tx ausspiegeln kann.

Wichtig ist, dass der Mirror-Port sowohl Rx wie auch Tx gemeinsam ausgibt.

Ausnahme: Falls die alle Ports des Switches oder alle Ports eines VLANs ausgespiegelt werden, darf nur eine Verkehrsrichtung aufgezeichnet werden (nur Rx –oder- nur Tx), da sonst die LAN-Pakete doppelt in der Aufzeichnung wären.

Mirror Port: Port Mirroring / Group Mirroring

Einige Switch-Typen können nicht nur einzelne Ports auf den Mirror-Port spiegeln, sondern Port-Gruppen (also mehrere Ports auf Mirror-Port).

Dies ist für die Praxis oft hilfreich, da es die Messung beschleunigen und Zusammenhänge besser sichtbar machen kann.

Es ist nicht unbedingt erforderlich, dass die Switches über diese Fähigkeit verfügen, aber nützlich.

Wird der LAN-Traffic von Rechnern aufgezeichnet, die gemeinsam in einer solchen Port-Gruppe angeschlossen sind, ist davon auszugehen, dass die LAN-Pakete doppelt in den Messdaten auftauchen, sofern am Switch sowohl Rx wie auch Tx ausgegeben wurden.

Mirror Port: Rx/Tx-Ausgabe bei mehr als 1 Source-Port bzw. bei mehr als 1 VLAN

Group Mirroring:

Falls *alle* aktiven Ports auf den Mirror-Port gespiegelt werden, darf von *allen* Ports jeweils nur Rx oder nur Tx ausgespiegelt werden, da sonst alle Packets doppelt am Mirror-Port ausgegeben würden.

Werden *einige* aktive Ports auf dem Mirror-Port gespiegelt, vervielfältigt sich mit der Zahl der Source-Ports auch die Zahl der Paket-Inkarnationen bei Broadcasts; denn da jedes Broadcast-Paket an jedem Port ausgegeben wird, wird jede Paket-Ausgabe eines Broadcasts an jedem der aktiven Ports somit auch per Kopie am Mirror-Port ausgegeben; dies führt (nur am Mirror-Port) zu einer (logisch scheinbaren, physikalisch tatsächlichen) Vervielfältigung des jeweiligen Broadcast-Pakets - und damit zu einer Paket-Vervielfältigung in den Messdaten.

Daher muss unbedingt die Konfiguration des Mirror-Ports vollständig dokumentiert sein, damit es nicht später eine Missdeutung der Daten im Zuge der Auswertung gibt.

VLAN Mirroring (1) / Broadcasts etc.:

Ähnliches gilt, wenn mehr als 1 VLAN am Core-Switch ausgespiegelt wird:

- da ggf. IP-Broadcasts an 255.255.255.255 in alle VLANs verteilt werden;
- da ggf. IP-Helper für die VLAN-übergreifende Broadcast-Verteilung sorgen;
- da ggf. NetBEUI-Pakete etc. VLAN-übergreifend verteilt werden.

Da je nach Konfiguration bestimmte Paket-Typen wie Broadcasts oder DHCP-Anfragen etc. über alle VLANs geflutet werden, muss auch hier die Konfiguration des Mirror-Ports präzise dokumentiert werden, um nicht bei der nachfolgenden Auswertung/Deutung der Messdaten in Missverständnisse zu kommen.

VLAN Mirroring (2) / VLAN Tags:

TraceMagic: Bis **TMv3** werden VLAN Tags ignoriert; ab **TMv4** werden auch LAN-Pakete mit VLAN-Tags unterstützt.

LAN-Analyzer: Sollte der zur Aufzeichnung verwendete LAN-Analyzer VLAN-Tags nicht unterstützen, sollte beim Mirror-Port darauf geachtet werden, dass ggf. Trunk-Packets ohne VLAN-Tag ausgespiegelt werden.

Mirror Port: Line Speed / Bit Rate

Es kann im Gigabit-Bereich wahlweise wie folgt vorgegangen werden:

(1)

1 x Gigabit -> Gigabit Mirror-Port

Ein einzelner Gigabit-Port wird auf einen Gigabit-Mirror-Port ausgespiegelt.

Hier sind bei leistungsstarken Switches keine (oder nur geringe) Paket-Verluste zu erwarten.

Bei Messungen mittels EtherPeek NX (WildPackets) am Gigabit-Mirror-Port hat sich gezeigt, dass bis ca 60-80% Netzlast (fast) vollständig bzw. verlustfrei aufgezeichnet werden kann.

(2)

n x Gigabit -> Gigabit Mirror-Port

Werden mehrere Gigabit-Ports auf einen einzigen Gigabit-Mirror-Port gespiegelt, sollte bedacht werden:

Die hierbei früher oder später auftretenden Buffer-Overflows am Mirror-Port sind in der Regel hinnehmbar, da TraceMagic Langzeit-Auswertungen ermöglicht und es daher unwahrscheinlich ist, dass Fehler nur 1 x auf der Leitung sind und ausgerechnet nur zu Buffer-Overflow-Zeiten.

Da TraceMagic Paket-Verluste erkennt bzw. die Unterscheidung ermöglicht, ob Pakete bereits auf der Leitung fehlten (zwischen Client und Server) oder erst am Messpunkt verloren gingen (wegen Puffer-Überlaufs), ist hier eine Bewertung der MessDaten hinsichtlich ihrer Aussagekraft i.d.R. zuverlässig möglich.

Performance:

An einem einzigen Gigabit-Switch mehrere Server-Ports auf einen einzigen Mirror-Port zu spiegeln, ist z.B. bei Cisco-6000er-Switches erfahrungsgemäß problemlos möglich. Bei anderen Herstellern/Fabrikaten bzw. bei älteren Modellen ist dies ggf. nicht so gut möglich und kann sogar zu Switch-Abstürzen führen.

(3)

Gigabit -> 100 Mbps Mirror-Port

Werden Gigabit-Ports auf 100-Mbps-Mirror-Ports gespiegelt, kann davon ausgegangen werden, dass dies bei geringem Datendurchsatz ohne große Bedenken durchgeführt werden kann; hier gelten weitgehend die Ausführungen zu Punkt (2).

(4)

100 Mbps Hub (kein Mirror-Port)

Es sollten bei einer jeden Messung auch Messpunkte an die Peripherie gelegt werden, um die "Sicht" der Client-PCs bzw. um die Datenkommunikation der Client-PCs vollständig und ungefiltert aufnehmen zu können. Dies wäre mit Messpunkten nur im Core-Backbone nicht möglich.

Im Falle fehlender Gigabit-Messrechner können ggf. vorhandene 100-Mbps-Messrechner an der LAN-Peripherie wertvolle und in vielen Fällen sogar voll ausreichende Arbeit leisten, insofern sie als *Capture-Engines* Daten aus Workgroup-Segmenten liefern, die (bezogen auf die Clients) uneingeschränkt gültige Auswertungen bzw. Aussagen zulassen.

TcpDump / Wireshark / TShark

(1) Unix / Linux

Unix/Linux-Server bieten in aller Regel die Möglichkeit, auf dem LAN-Adapter des Servers intern eine Capture_Engine laufen zu lassen vermittels der Software TcpDump, die auf den meisten Unix-Servern zum Inventar gehört.

Der resultierende Trace ist vergleichbar mit dem Trace eines am gegenüber liegenden Switch arbeitenden Mirror-Ports. - Über FTP oder USB-Platte holt man sich dann die Trace-Files auf den TraceMagic-Rechner zwecks Auswertung.

Wo weder Mirror-Port noch Tap zur Verfügung stehen, ist diese Vorgehensweise nicht nur möglich, sondern sogar empfehlenswert.

Nachteil: Ist der Server-Administrator nicht anwesend oder nicht einverstanden, entfällt diese Variante.

Vorteil: Ist der Switch-Administrator nicht anwesend oder nicht einverstanden, ergibt sich diese Variante.

(2) Windows

TcpDump hat eine Windows-Adaption gefunden mit "Wireshark" btw. "TShark":

Wireshark → Windows-Oberfläche, "normaler" Analyzer

TShark → Kommandozeilen-Variante, ohne GUI (daher schneller).

(3) Capture mit TcpDump / TShark

TShark erzeugt, wenn es mit Default-Settings betrieben wird, nur eine einzige Trace-Datei, ggf. mit Größen von mehr als 1 GByte.

Da **TraceMagic** nur bis zu max. 500.000 LAN-Pakete je Aufzeichnungs-Datei verarbeitet, und da TraceMagic erfahrungsgemäß am besten arbeitet bei 50.000-100.000 LAN-Paketen je Datei (entspricht meistens einer Datei-Größe von 16-32 MB), dürfen diese Default-Settings (heißt: nur 1 Datei, und diese endlos groß) nicht verwendet werden.

TcpDump und TShark dürfen daher nur eingesetzt werden, wenn die richtigen Betriebsparameter eingestellt sind: (1.) Aufzeichung in endlos vielen, durchnummerierten Dateien. (2.) Begrenzung der Datei-Größe auf 16 oder 32 MB.

Download: Wireshark / TShark / WinPCap

Wireshark samt TShark und WinPCap-Treiber gibt es hier:

→ http://www.wireshark.org/

Bitte die dort angegebenen Urheber- und Nutzungsrechte beachten.

Zusammenhang von Wireshark/TShark und TraceCommander/MiniMagic

Das von **Synapse Networks** entwickelte Aufzeichnungs-Tool **TraceCommander** (bzw. das Modul **Capture-Wizard**) arbeitet im Hintergrund mit TShark via WinPCap-Treiber.

Da dies so ist, wird für dieses Capture-Tool seitens Synapse Networks kein Geld genommen. Anders verhält es sich mit dem Modul zur Auswertung der Messdaten (**MiniMagic**) – hier wird für die Nutzungslizenz auch Geld verlangt.

Es ist unbedingt darauf zu achten, dass die MessDaten, die im TcpDump-Format gespeichert werden (TcpDump, Ethereal, Tethereal), mit der Datei-Endung " .DMP " abgelegt werden, da sie sonst von TraceMagic nicht erkannt werden.

Die Aufruf-Syntax von TEthereal (DOS-Box bzw. Eingabeaufforderung) ist wie folgt (Beispiel):

tethereal -i CE3 -q -s 1518 -b filesize:32000 -b files:100 -F libpcap -w tracefile_.dmp

Hierbei bedeuten:

"**-i**" gibt an, über welches LAN-Interface das Capture laufen soll. (Ist nicht klar, welche Interfaces es gibt bzw. wie sie heißen, so wird dieses mit "tethereal -D" abgefragt; das "-D" muss GROSS geschrieben werden.)

"**-q**" gibt an, dass während des Capture nicht die Anzahl der erfassten LAN-Pakete angezeigt wird; der Zähler kostet Prozessor-Zeit und kan dazu beitragen, das LAN-Frames verloren gehen. Der Parameter "-q" erhält keinen eigenen Wert nachgestellt.

"**-s**" gibt die Frame_Size an bzw. den Frame_Slice; heißt: Sollen die LAN-Frames in voller Größe eingelesen werden, oder nur die ersten x Octets/Bytes? Bei Ethernet bedeutet die Angabe "-s 1518", dass die LAN-Frames in voller Länge eingelesen werden.

"**-b filesize:**" gibt an, bis zu welcher Datei-Größe gearbeitet wird; der Parameter "filesize:32000" führt zu einer Trace_File_Size von 32 MB (empfohlen für die Verarbeitung durch TraceMagic).

"**-b files:**" gibt an, wie viele Trace_Files (Aufzeichnungs-Dateien) maximal erzeugt werden; gleichzeitig bedeutet der Schalter, dass mit einem Ring_Buffer gearbeitet wird: Ist die Höchstzahl bzw. Gesamtzahl der zu schreibenden Trace_Files erreicht, wird die älteste Datei mit den aktuell eintreffenden LAN-Frames überschrieben. Im aktuellen Beispiel werden bis zu 100 Dateien erzeugt. Bei einer jeweiligen Größe von 32 MB ergibt das eine Gesamt-Aufzeichnungs-Menge von max. 3,2 GB.

"**-F**" (verzichtbar) gibt das Aufzeichnungs-Format an; "-F libpcap" ist das gängige Format.

"**-w**" gibt den Datei-Namen an, unter dem die Trace_Files abgespeichert werden sollen. Hinter dem hier deklarierten Namen wird noch ein Zeit-Stempel bzw. eine laufende Nummer angehängt.

Folgende Syntax sollte beim Aufruf von TcpDump unter Unix/Linux zum Erfolg führen:

Syntax: tcpdump -w [tracefilename] -s [framelength] -C [filelength]

Beispiel: $> tcpdump -w capture_01_ -s 1518 -C 32000

Fragen und Antworten

Frage: "Welche Einstellungen sollte die Capture Engine haben?"

Im Wesentlichen sind folgende Einstellungen wichtig:

(1) Kein Ring-Buffer („Clear Buffer“ statt „Wrap Buffer“)

KEINE "Wrap Around" –Einstellung für den Capture-Buffer (Packet-Buffer) !

Der Capture-Buffer (für Paket-Aufnahme reservierter Hauptspeicher) muss auf „Clear Buffer“ gesetzt werden. Will sagen: Wenn der Capture-Buffer voll ist und folglich die LAN-Pakete auf die Festplatte geschrieben werden, soll der Capture-Buffer gelöscht und das erste neue LAN-Paket zu Beginn des Speicher-Segments abgelegt werden.

Falsch wäre „Ring Buffer“, was bewirken würde, das das erste neue LAN-Paket hinter der Speicher-Adresse des letzten vorigen LAN-Pakets abgelegt würde. Diese Art der Speicherung kann zu Problemen bei der Auswertung durch TraceMagic führen.

(2) Keine Online-Filter (alle LAN-Pakete aufzeichnen)

KEINE "Online Filter" während der Aufnahme der LAN-Pakete.

ALLE LAN-Pakete sollen bzw. müssen eingelesen werden!

Das Filtern lässt sich nachträglich in TraceMagic über das Modul "FilterMagic" erledigen.

(3) Kein Packet-Slice (volle Paket-Länge aufzeichnen)

KEIN "Packet Slice", heißt:

Es darf KEINE Verkürzung der Daten-Inhalte eingestellt werden; anders gesagt: Die LAN-Pakete müssen IN VOLLER LÄNGE eingelesen und abgespeichert werden. Anderenfalls wäre ggf. nur noch TCP/IP-Analyse möglich, nicht aber Applikations-Analyse.

(4) Größe der Aufzeichnungs-Dateien: 32 MB (Daumenregel)

CAPTURE FILES: 32 MB

Die Größe der Aufzeichnungs-Dateien ("Capture Files", "Trace Files") muss nach zwei Kriterien beschränkt werden:

- Die Datei-Größe sollte idealerweise bei 16 MB oder 32 MB liegen.
  Dies ermöglicht erfahrungsgemäß die durchschnittlich beste und schnellste Verarbeitung.
- Verarbeitung in TraceMagic: Es dürfen nicht mehr als 500.000 LAN-Pakete je "Trace File" gespeichert sein. - Dieses Limit wird in der Regel nicht überschritten, wenn die oben genannten Datei-Größen eingehalten werden. - Ausnahmen:
- Bei Applikationen, die mit sehr vielen, sehr kleinen LAN-Paketen arbeiten, muss die Datei-Größe eher mit 8 MB bis 16 MB veranschlagt werden.

  Dies gilt insbesondere für Terminal-Server-Umgebungen, also:

  * Citrix Metaframe (Protokoll: ICA)
  * Windows Terminal Server (Protokoll: RDP)
  * TELNET

(5) Überlegung: VLAN-Tags ?

KEINE VLAN-Tags

Die Capture-Engine sollte seitens eines etwaigen Mirror-Ports die LAN-Pakete *ohne* VLAN-Tags ausgegeben bekommen, da viele LAN-Analyzer bis heute die Verarbeitung bzw. Darstellung von LAN-Paketen mit VLAN-Tags nicht unterstützen.

(6) Durchgehende Nummerierung der Capture-Files

Alphabetisch-numerische Reihenfolge = chronologische Reihenfolge

Die Capture-Files müssen bei apha-numerischer Sortierung in exakt chronologischer Reihenfolge liegen.

Richtig:	**Falsch:**

`Capture_File_00001_20060505112748.dmp`
`Capture_File_00001_20060505112752.dmp`
`Capture_File_00001_20060505112758.dmp`
`Capture_File_00001_20060505112815.dmp`
	`Mon 08 May 2006 112748.bfr`
	`Fri 12 May 2006 073820.bfr`
	`Tue 09 May 2006 093819.bfr`
	`Wed 10 May 2006 123129.bfr`

Die meisten Analyzer bieten die für TraceMagic erforderliche Form der Namensgebung an.
Im Falle von Ethereal/TEthereal sollte das „TEthereal Starter Programm" verwendet werden.

Frage: "Welche Ausstattung bzw. welche Merkmale braucht der MessRechner?"

(1) "Promiscuous Mode"

Das Mitlesen/Abspeichern von LAN-Paketen ergibt nur Sinn, wenn der MessRechner in der Lage ist, die vom Netzwerk (Koax,Repeater,Hub,Switch) gelieferten Daten auch anzunehmen und abzuspeichern.

Die Mindest-Anforderung in diesem Sinne ist, dass der LAN-Adapter den sog. "primiscuous mode" unterstützt: Dieser Betriebs-Modus veranlasst den LAN-Adapter, nicht nur die an ihn selbst per MAC-Adresse gerichteten LAN-Pakete einzulesen, sondern alle physikalisch eintreffenden LAN-Pakete anzunehmen (und an das Betriebssystem bzw. an die Analyse-Software weiter zu geben).

Bei Messdaten-Aufzeichnung via WLAN-Adapter ist erfahrungsgemäß der „Promiscuous Mode" abzuschalten (das klingt widersinnig, hat sich aber so bestätigt).

(2) "Prozessor & Festplatten-Architektur"

Bis 100 Mbps (Fast Ethernet) kann allgemein auf allen gängigen Intel-Pentium-Prozessoren (und vergleichbare CPUs) eine befriedigende bzw. voll ausreichende Leistungskraft erreicht werden.

Bei 1000 Mbps (Gigabit Ethernet) jedoch ist eine schnelle und leistungsfähige Festplatten-Architektur hilfreich.

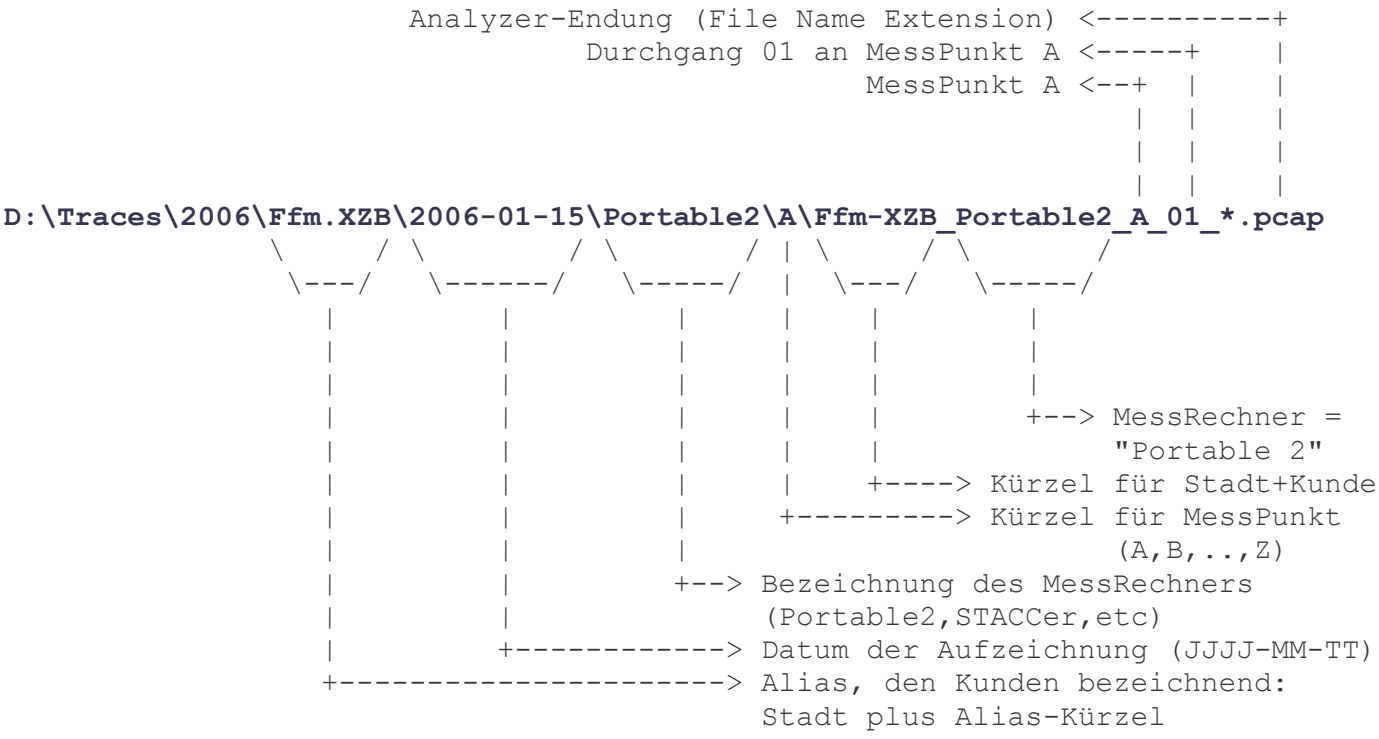
Aber auch gängige Festplatten, ja, sogar USB-Platten sind gut einsetzbar, da die Verluste bei der Aufzeichnung erfahrungsgemäß sehr gering sind.

Problematisch jedoch ist das Aufzeichnen von Gigabit-Datenströmen mittels Laptop. Diese Geräte-Architektur ist für derlei Dauer-Belastungen nicht ausgelegt.

Frage: "Wie sollten die MessDaten auf der Festplatte organisiert sein?"

Die Capture-Files (Trace Files) sollten je MessPunkt getrennt bekannt und in getrennten Unterverzeichnissen abgelegt (und später auch getrennt ausgewertet) werden.

Eine sinnvolle Ordnung auf der Festplatte könnte etwa so aussehen:



© Frank R. Walther / Synapse:Networks GmbH

Alle Rechte vorbehalten.
Übernahme und Kopie nur mit schriftlicher Genehmigung des Urhebers bzw. Rechte-Inhabers.

Synapse Networks GmbH
Bonner Str. 10
D-53424 Rolandseck bei Bonn
GERMANY

0700-synapse-C = Telefon
0700-synapse-F = Fax

http://www.synapse.de/ http://www.tracemagic.net
info-kontakt@synapse.de http://www.tracecommander.net

#