Anforderungen an die Managebarkeit von Netzwerk-Komponenten

Ergebnispapier der Arbeitsgruppe
"Anforderungen an ein Netzwerk-Management System"
Untergruppe der Benutzergruppe Netzwerke BGNW

Stand 05.08.1993

Vorbemerkungen

Die Erstellung eines Anforderungskataloges für die Verwaltbarkeit von Netzwerk-Komponenten war die logische Konsequenz aus dem zuvor erstellten Papier "Anforderungen an ein Ne~werkmanagement-System", da ein NM-Plattform-System nur dann einsetzbar ist, wenn eine entsprechende Management-Funktionalität, insbesondere in Form von Manauement-Aqenten, durch die zu verwaltenden Netzwerk-Komponenten

Dieser Anforderungskatalog soll die aus Sicht der Arbeitsgruppe notwendige Funktionalität für Netzwerk-Komponenten zusammenfassen. Die Anforderungen wurden nach wichtigen System- und Funktionsbereichen gegliedert.

In diesem Papier

"Anforderungen an die Managebarkeit von Netzwerk-Komponenten"

wird soweit möglich eine deutsche Terminologie verwendet. Abweichend davon wird der für die Verwaltung bzw. die Administration eines Netzwerkes der allgemein gebräuchliche Begriff "Management" als Sammelbegriff verwendet. Für den Begriff "managen" wird der Begriff "verwalten" benutzt. Es ist damit der volle Bedeutungsumfang des englischen Begriffs "managen" gemeint. Da der Begriff "Accounting" kein bedeutungsgleiches deutsches Äquivalent hat, wird "Accounting" (Abrechnung und Ressourcenzuteilung)

Im Rahmen dieses Papiers werden aus Gründen des Umfangs nicht alle RFC-Anforderungen explizit aufgeführt; wichtige Anforderungen werden jedoch genannt, da nicht bei allen Lesern Detailwissen über die vorhandenen RFC's vorausgesetzt werden soll.

Abkürzungen, die im Netzwerk-Bereich gebräuchlich sind und in diesem Papier verwendet werden, sind im Anhang 1: Abkürzungen des Papiers "Anforderungen an ein Netzwerkmananement-System" erläutert.

1. Altgemeines

Basis-Protokoll für die Verwaltung von Netzwerk-Komponenten soll **mindestens SNMP sein, zusätzlich** ist OSI (CMIP) wünschenswert.

1.1 SNMP

Gefordert werden volle Unterstützung von SNMP und darüber hinaus entsprechende **Erweiterungen, d.h.**

MIB II (inkl. GET und SET)

* Folgende SNMP RFCs geben hierzu Informationen RFC 1229 Extensions to Generic Interface MIB RFC 1230 IEEE 802.4 Token Bus MIB RFC 1231 IEEE 802.5 Token Ring MIB

EXPERIMENTAL MIBs und/oder einer PRIVATE MIB soweit für die Komponente erforderlich)

Wie ist das Mengen-Verhältnis der unterstützten Variablen PRIVATE MIB zu denienigen in MIB II und EXPERIMANTAL MIB?

* Wie verteilen sich die MIB-Informationen prozentual auf
management (2) experimental (3) (FDDI SNMP
MIB, Token Ring MIB, ...) private (4)
(enterprise-specific MIBs)

Wie wird die PRIVATE MIB zugänglich gemacht? Gefordert wird die Einlesbarkeit über einen entsprechenden elektronischen Datenträger. Grundsätzlich hat die Offenlegung aller privaten MIB-Erweiterungen für eine Komponente zu erfolgen.

Wie werden Updates der PRIVATE MIB realisiert?

Hardwaremäßige Updates (PROM-Tausch) sind unerwünscht.
Softwaremäßige Updates per Download sind gefordert.
Die Updates sollen automatisch vom Anbieter zur Verfügung gestellt werden.
Der Anbieter muß ein definiertes Verfahren zur Verteilung neuer Releases angeben können.
Updates sOllen in ASN.1, concise MIB erfOlgen, damit sie über einen entsprechenden MIB-Compiler einlesbar sind. (RFC 1212 Concise MIB Definition, IAB, März 1991)

Für die Unterstützung der PRIVATE MIB ist ein entsprechendes Applikationsmodul im NMS erforderlich. das die Werte der MIB-Variablen entsprechend aufbereitet.

Erforderliche Angabe:
- Zu welchen NMS gibt es ein Applikationsmodul?
- Bietet das Appl.-Modul eine menügeführte/grafische Oberfläche? Welche Parameter, Counter und Statistiken werden zusätzlich zu Textinformationen auch in Grafischer Form dargestellt?

1.2 OSI, CMIP, Migration

Der Anbieter soll angeben, wie die zukünftige Migration zur Unterstützung von OSI/CMIP geplant ist.

Unterstützt werden sollen ebenfalls Managementfunktionen nach IEEE 802.1 B und die aktuelle Version des FDDI SMT.

2. Festlegung zu venNaltender Komponenten

Als relevante Netzwerk-Komponenten, die in einem NMS verwaltet werden sollen, hat die Arbeitsoruppe festgelegt:

Hub
Brücke
Router
Terminalserver / Steuereinheit
Netzwerk-Schnittstelle (Adapterkarte)
(Gateway ist wie Endgerät mit Adapterkarte zu behandeln)
(TK-Anlage mit LAN-Anschluß ist wie Endgerät mit Adapterkarte zu behandeln)

3. **Allgemeine Anforderungen an alle Komponenten**

Folgende Angaben/Parameter über Netzwerk-Komponenten sollten für ein NMS (siehe dazu Papier "Anforderungen an ein Netzwerkmanagement-System") verfügbar/verwaltbar sein: Kurzbeschreibung Hersteller Produktbezeichnung Produktions-Serien-Nr Typ

Upgradefunktionen für MIB-Variablen und neue Releases der Management-Software:
- automatisches Upgrade per Download und RebootNVarm Reset für z.B. SNMP MIB FDDI SMT

SNMP Parameter Setup / COnfiguration

- Station- und System-Parameter Agent IP Address, IP Network Mask, Default Address
  Sende-Konfiguration von Traps
  Trap Destination, Trap-Adreßtabellen
  Community Strings für GET und SET
  Anzeige der PRIVATE MIB Version
  Offenlegung und Einlesbarkeit der kompletten Private MIB mit allen Erweiterungen
  Upgrade-und Downloadmöglichkeit für neue MIB-Versionen

Support durch den Hersteller / Anbieter

- Qualifizierter Hotline Support seitens des Herstellers mit garantierter Reaktionszeit; (Der Hersteller soll z.B. eine Dokumentation des aktuellen Kundenequipments führen, damit nicht bei jedem Hotline Call wiederholte Angaben über die vorhandene Konfiguration erforderlich sind.)
  Der Komponentenhersteller soll in der Lage sein, über die HOtline auch vor Ort Support für Fehler- und Konfigurationsmanagement zu leisten.
  Fehler im Handbuch sollen über automatisierte Updates, nicht erst auf Nachfrage korrigiert werden.
  Fernwartung der Hersteller/Distributoren soll als Option angeboten werden

4. **Sternkoppler t Hub's**

Die in Literatur und Praxis nicht genau definierten Begriffe Sternkoppler und Hub haben ihren Ursprung in der sternförmigen 10 Mbps-Version des CSMA/CD-Verfahrens. Die Hubs bilden die Nachfolge-Generation der im Ethernet-Bereich verwendeten Sternkoppler, die sich als Repeater mit der Möglichkeit des Medienwechsels (zwischen Lichtwellenleiter-, Twisted-Pairund Koax-Kabel) beschreiben lassen. Aufgrund gestiegener Anforderungen wie höhere Anschlußzahlen, verstärkte Subnetz-Bildung und höherer Integrations-Notwendigkeit bildeten sich die Hub's als neues Koppelelement heraus. Uber das Sternkoppler-Merkmal des Medienwechsels hinaus bieten Hub's folgende

i.d.R. wesentlich höhere Anschlußdichte als Sternkoppler
i.d.R. mehrere (unterschiedliche) Bussysteme (für Ethernet, FDDI, ..)
i.d.R. Integration von weiterführenden (d.h. über die Repeater-Funktionalitäl hinausgehenden) Koppelelementen wie Brücken, Router, Terminal-Server etc. in Form von Einschüben - meist OEM-Module von Brücken / Router / Terminal-Server-Herstellern

In der Praxis werden zusätzlich weitere, ähnlich definierte Begriffe wie z.B. "Intelligent Hub" oder "Modular Hub" oder "Konzentrator", "Backbone-Konzentrator" verwendet, wodurch an dieser Stelle die Notwendigkeit einer konsistenten Begriffs-Abgrenzung entsteht. Im folgenden werden Hub's in zwei Gruppen: "Homogene Hubs" und "Modulare Hub's"

Als homogene Hub's im Sinne dieses Papiers werden **kleinere, nichtmodulare** Verteilerkomponenten mit typischerweise

max. 3 HE (HE = Höhen-Einheit)
nur einem Bussystem
min. 8 homogenen Anschluß-Ports verstanden. Auf die Aufstellung spezifischer Anforderungen wird verzichtet, da diese sich vollständig in den Anforderungen an Modulare Hub's abbilden lassen.

Als weiterführende Variante der Sternkoppler/homogenen Hub's entwickelten sich die Modularen Hub's. Ein Modularer Hub integriert eine Vielzahl von unterschiedlichen

Ethernet-Module für unterschiedliche Medien (LWL, Koax, TP, ...)
FDDI-Module für unterscheidliche Medien (LWL, TP) und Anbindungsformen (DAS, SAS, DAC, SAC)
Brücken-Module für EtherneVEthernet-Kopplung, EtherneVFDDI-Kopplung
... Router-Module für die Kopplung von EtherneVFDDI
Management-Module für EtherneVFDDI
Terminal-Server-Module für asynchrone Terminals unter TCP/IP

in einem einzigen Grundgerät. Um diese Integration zu bewerkstelligen, bieten die Modular Hubs mehrere unterschiedliche Bussysteme (Ethernet, FDDI, ...) in unterschiedlicher Anzahl auf ihrem Backplane an. Somit ist die Bildung von zwei (oder mehr, je nach System) getrennten Ethernet-Subnetzen innerhalb eines Modularen Konzentrators möglich. Die Verbindung dieser Ethernet-Subnetze untereinander kann über einen internen EtherneVEthernetBrücken- oder Router-Modul hergestellt werden, ebenso wie die Anbindung der Subnetze an ein übergeordnetes FDDI-Netz durch einen Router-Modul. Nachfolgend wird statt "Modularer Hub" nur noch der Benriff "Hub" verwendet

4.1 Aufteilung in funktionale Einschübe

C-,mndfunktion

- Hub
- Power
- interner Bus
- SNMP-Agent (Karte oder Software), der alle anwendbaren RFC MIBs bis Ebene 2 unterstützt (z.B. Hub MIB = IEEE 802.3 Repeater MIB, Chassis MIB)

Konzentrator-Funktionen

- Steuereinheiten IBM 3x74 und kompatible
- DEC Terminal-Server
- TCP/IP Terminal-Server
- Ringleitungsverteiler (RLV)
- Multiport-Transceiver

Netzwerk-Komponenten

- Medi en -Sch
- Rittstelle
- Repeater
- Brücke
- Router

Anmerkung:
Sternkoppler, Bridges, Router und Gateways wachsen immer stärker zu multi-funktionalen Hubs zusammen. Aus diesem Grunde ist es entsprechend schwierig, die einzelnen Hubs als ganzes zu beschreiben. Es ist bedeutend einfacher, den Hub als Summe von Funktionen anzusehen und sich auf die Betrachtung der Einzel-Funktionen zu beschränken. Die meisten F"nktinn~bincke eines Hubes sind auch als eigenständige Geräte

Nachfolgend werden in diesem Kapitel nur noch Medien-Schnittstelle, Repeater und Ringleitungsverteiler als Einschub-Module in einen Hub betrachtet. Für andere Elnschub-Module (höherer Intelligenz) sollen die gleichen Anforderungen wie für Standalane Komponenten (Brücken, Router, Terminal-Konzentratoren) gelten.

4.2 Generelle Anforderungen:

- Management-Zugang für alle Funktionen sowohl über alle Netzwerke asl auch outband
- Selbständiges Anmelden des Hub's bei Kaltstart, Warmstart und Reset
- Automatische Anzeige und Generieren einer Meldung bei Fehlern und Hardwareänderung
- Einfache bedienerfreundliche Menuführung, je nach Anwahl, Hub, Module und Port erscheint ein entsprechendes Auswahlmenu
- Automatisches Umschalten von In- auf Outband (Modem, etc.);wenn das Netz nicht mehr verfügbar ist, soll ein Trap an das Outband-Board erfolgen
- Grundeinstellung über ASCII-Terminal mit mindestens VT100-Funktionalität (IP-Adr., GW-Adr., Standort) konfigurierbar
- Software (Update) downloadbar für Agent

Freie Definition /Ausblenden der Meldungen (Info, Alarm etc.)
Standardbasierte grafische Anwendung (X.11, OSF/Motif, PM) für mindestens ein NM

4.2.1 Konfiguration

Reset Hub

Trap Reporting ein-/ausschaltbar

Öffnen von Port Gruppen

Funktionen pro Steckplatz
Reset Steckplatz
Jumpereinstellungen sollten Buslesbar und mit entsprechender Interpretation versehen
sein
Trap Reporting für Ein-/Ausschalten
manuelle, automatische Verwaltung (remote,lokal)
Aktivieren/Deaktivieren des internen Busses
Bus-Redundanz (Backup)

Fort
Alarme ausblenden
Aktivieren / Deaktivieren

4.2.2 Performance

Performance Reporting ein-/ausschaltbar
aktuelle und durchschnittliche Last pro internem Bus / Karte / Port per Zähler
Spitzenlast pro internem Bus
Setzen eines Threshold Wertes pro Bus für definierte Schwellwerte von Alarms oder Abschalten des Hub's

4.2.3 Fault

Statusanzeige des Hub's prozentuale Fehlerrate pro Bus, Aufschlüsselung nach Art der Fehler (Kollision, CRGFehler, Jabber, Runts, etc.)

Unintelligente Module (ohne eigenen Agenten): Port
Status Meldungen (Tx, Rx, Down, Partitioning, usw.) zu
kurzerlange Pakete CRC-Fehler Kollisionen Ring Fehler
Token Fehler Token Ring Bypass

Aktivieren/Deaktivieren des Ports
SEE ein-/ausschalten

4.2.4 Sicherheit

Zuordnen von SNMP Community Strings zu IP-Adresse(n) der zugriffsberechtigten Management-Systeme
Zugriffsschutz durch Paßwortvergabe für einzelne User und das berechtigte Management-System
Paßwörter mit abgestuften Zugriff auf die Parameter der Station z.B. User, Local Network Manager, Global Network Manager, Field Engineer
Schützen besonders kritischer Befehle mit Paßwörtern (z.B. Boot-Befehl)
Zuordnung unterschiedlicher SET Community Strings
standardisierte Verschlüsselungs-Mechanismen
Meldung an NMS bei Mismatch zwischen der an einem Port konfigurierten MAC Adresse und der tatsächlich gesehenen MAC-Adresse

5. **Brücken, Router und Brouter**

Eine Brücke verbindet Subnetze gemäß Ebene 2 des OSI-Referenzmodells. Die meisten Brücken verbinden gleichartige Subnetze auf MAC-Ebene (Ebene 2a), als sogenannte MACLayer Brücken. Die OSI-Definition beschränkt eine Brückenverbindung jedoch nicht auf gleichartige LANs, es können auch unterschiedliche MAC-Ebenen (Ethernet - Token Bus, Ethernet - FDDI ...) verbunden werden.

Erreicht wird eine Kopplung physikalisch unabhängiger Netze, die eine Oberwindung der LAN-Restriktionen für maximale Segmentlänge und maximale Stationszahl bewirkt. Zusätzlich werden die Funktionen der MAC (und LLC) Ebene ausgeführt, d.h. z.B. die Checksumme und Framelänge überprüft. Fehlerhafte Frames (z.B. durch Übertragungsfehler oder Kollision) werden nicht weitergeleitet, wodurch eine Fehlerbegrenzung (von Data Link Fehlern) auf die jeweiligen Subnetze erfolgt.

Darüber hinaus wird durch Entkopplung des lokalen Verkehrs vom subnetzübergreifenden Verkehr eine Lasttrennung und somit bessere Netzkapazität erreicht. Die Weiterleitung erfolgt auf der Basis von MAC-Adressen, die bei Brückenkopplung im gesamten Netz eindeutig sein müssen. Um die Transportentscheidung zu treffen, werden alle Pakete interpretiert (Arbeitsweise: sogenannter promiscuous Mode). Defaultmäßig, d.h. wenn die Brücke nicht entscheiden kann, ob es sich um lokalen oder übergreifenden Verkehr handelt, werden Pakete transportiert, um die Kommunikationsfähigkeit zwischen Subnetzen sicherzustellen. Die Konsequenz ist, daß insbesondere auch alle Broadcasts transportiert

Trotz Lasttrennung stellen Brücken eine protokolltransparente Subnetzkopplung Dar, da sie die höheren Protokollebenen nicht interpretieren. In der Praxis bedeutet das, daß eine Brücke unterschiedslos alle Protokolle überträgt, die auf den verbundenen MAC-Ebenen aufsetzen (Ethernet, FDDI, ...), z.B. AppleTalk, DECnet, IPX, LAT, NetBIOS, OSI, TCP/IP, XNS.... auf der Basis eines MAC-Standards (CSMA/CD. FDDI, ...).

Durch Schielfenerkennungs- und -unterdrückungsmechanismen (Source Routing im Token Ring Bereich, Spanning Tree im Ethernet- und FDDI-Bereich) lassen sich mit Brückeneinsatz redundante Netz-Strukturen aufbauen (Wegeredundanz, Brückenredundanz), die ohne Brücken (oder höhere Koppelelemente) nicht möglich sind.

Weitergehende Laststeuerung kann durch Filtereinsatz und Lastverteilungs-Funktionalität (Distributed Load Sharing, Triangulation) erreicht werden.

Aufgrund der Realisierung der MAC-Funktionalität benötigen Brücken für die Paketbearbeitung eine Verarbeitungszeit im Bereich von -Sekunden bis Millisekunden. Bei hohem subnetzübergreifenden Verkehr stellt daher eine Brücke einen potentiellen Engpaß dar. In diesem Fall ist u.U. ein Redesign der Subnetzstruktur erforderlich.

Prinzipiell sind zwei Brückentypen zu unterscheiden: Lokale und remote Brücken.

Die **Lokale Brücke** hat zwei oder mehr Ports, über die sie ihre angeschlossenen Subnetze (zwei oder mehr) verbindet. In der überwiegenden Anzahl der Fälle sind es LANs gleichen Typs, z.B. Ethernet - Ethernet, manchmal aber auch unterschiedlichen Typs wie Ethernet - FDDI, Ethernet - Token Ring.

Lokale Brücken verbinden LAN-Segmente direkt, als Subnetzkopplung innerhalb eines Unternehmens- oder Campus-Netzes. Die Verbindung wird über die LAN-Eingangsports und -Busgangsports der Brücke hergestellt, d.h. mit Ein- und Ausgangsgeschwindigkeiten der LAN-Bandbreite. Handelt es sich um LANs gleichen Typs, erfolgt die Verbindung relativ problemlos. Handelt es sich um verschiedene MAC Protokolle an den Ein- und Ausgangsports, muß zur Umsekung vom "schnelleren" LAN (z.B. 100 MbiVs) zum **"langsameren"** LAN (z.B. 10 MbiVs) ausreichend Pufferplatz für eine Zwischenspeicherung der Pakete vorhanden sein.

Die **Remote Brücke** verbindet ihrem Namen entsprechend Subnetze über Weitverkehrsstrecken (bloße Backbone-Strecken ohne eigene angebundenen Endstationen). Diese Brücken treten immer mindestens paarweise auf. An beiden Endpunkten einer Weitverkehrs-Strecke zwischen zwei LAN-Subnetzen wird dann jeweils eine Remote Brücke installiert.

Eine Remote Brücke kann einen oder mehrere lokale Ports (Ethernet, Token Ring, ...) sowie einen oder mehrere remote Ports haben. Viele Weitverkehrs-Brücken haben genau einen lokalen und je nach Bedarf ausbaudar 1 - 8 remote Ports, die z.B. über X.21 mit Geschwindigkeiten von 9.6 kbps bis 2 Mbps arbeiten. Oft ist die aggregierte Bandbreite, auch Summenkapazität genannt, jedoch auf maximal 2 oder 4 Mbps begrenzt, d.h. es können nicht alle 8 Ports mit 2 Mbps installiert werden - dies würde die Verarbeitungs- und Pufferkapazität rar Brücke bei voller Auslastung aller Weitverkehrsstrecken überschreiten.

Da Remote Brücken je nach Kapazität der DFV-Leitungen sehr große Kapazitätsunterschiede vom LAN zum Weitverkehrsnetz ausgleichen müssen, spielt Pufferplatz (Abfangen von Lastspitzen) und Puffer-Organisation hier eine wesentlich größere Rolle als bei Lokalen Brücken zur reinen LAN-LAN Kopplung. Auch die Implementierung eines Spanning Tree Algorithmus (Unterdrückung von Paketzyklen, die in den nachfolgenden Kapiteln beschrieben wird) ist komplexer.

Die Beschreibung der Anforderungen an WAN-Schnittstellen von Remote Brücken und Routern geht über den Umfang dieses Papiers hinaus, d.h. die hier gestellten Anforderungen beziehen sich auf System-Informationen, Protokoll-Parameter und

5.1 Systemmanagement / Physikalische Konfiguration

- Lesen der Stations-Parameter
  z.B. Hardware- und Software-Version, Performance-Modul
  Lesen der Hardware-KonfiguratiOn
  z.B. Prozessoren, Boards,
- Lesen und Setzen von Default-Parametern
  z.B. Rücksetzen aller Parameter
- Lesen der Hardware-Informationen zu Adapter oder Board
  z.B. Prozessor, Hardware-Version
- Download-Möglichkeiten für:
  Upgrade von Betriebssystem-Software

5.2 Konfigurationsmanagement
5 2 1 Gemeinsame Anforderungen für Brücken und Router

Hilfefunktion zur Konfigurierung, d.h. Menüführung für Outband-Management und Konfiguration vor Ort über serielle Schnittstelle
Download von vordefinierten Konfigurationsfiles und autOmatisiertes Update von ROuting-, Adreß- und Filtertabellen (z.B. durch Einsatz von Flash-Memories)
Remote Login mit symbolischen Namen, auch kaskadierbares Login
Remote Login übers Netz per Telnet
Abschottung gegen weitere Logins, falls aktuell schon eine Management-Verbindung besteht (über Netz und über V.24; Abschottung aller Zugriffe über verschiedene Protokolle wie SNMP und CMOL (IBM LAN Manager) gegeneinander)
Remote Boot Möglichkeit
Jumpereinstellungen sollten Buslesbar und mit entsprechender Interpretation versehen

5.2.1.1 Schnittstellen-Management auf physikalischer Ebene

Lesen und Setzen der Port Status-Parameter Lesen und Setzen der Port Geschwindigkeit mit Plausibilitätsprüfung

5.2.1.2 Management auf MAC-Ebene: Parameter der Zugangsverfahren

LAN-Port-Parameter und MAC-Parameter entsprechend der medienspezifischen Zugangsverfahren (CSMA/CD, Token Ring, Token Bus, FDDI) z.B. FDDI SMT Parameter mit SMT Version MAC Adresse Target Token Rotation Time TTRT Valid Transmission Time

S.2.2 Brücken
5.2.2.1 Brücken-Parameter

Lesen und Setzen der Lernfunktion Lesen und Setzen der Aging-Parameter Lesen und Setzen des Aning Intervalls, max. Alter der Adressen

5.2.2.2 Lern- bzw. Adreßtabellen (Filtering Database)

Lesen und Setzen der statischen Einträge Lesen der dynamischen Einträge Verwaltbarkeit der Tabellengröße (vergrößern, verkleinern um Speicherplatz zu sparen)

5.2.2.3 Spanning Tree Bridge PrOtocol Parameter

Lesen und Setzen der ST Brücken- und Port-Parameter (Bridge Priority, Designated Root, Root Path Cost, Port ID, Port Prlority, ...) Lesen und Setzen des ST Port-Status (Listening, Learning, Forwarding, Blocking)

5.2.2.4 Source Routing Parameter

Lesen und Setzen der SR Port-Parameter (TR Ring Number, Bridge Number, Single Route Broadcast, Hop Count Limit, Largest Frame Size, ...) Lesen und Setzen von SRT Bridging, Ein-/Ausschaltbar

5.2.2.5 Filterprogrammierung

Lesen und Setzen der Adreßfilterung nach Ziel- und Quelladresse
Lesen und Setzen von getrennter Filter-Programmierung von Broadcast- und Multicast-Adressen
Lesen und Setzen der Schwellwerte zur Unterdrückung von Broadcasts
Lesen und Setzen der Protokollfilter (Vergleich von Typ- und Längenfeld, LLC-Header,
Header für höhere Protokolle)
Verknüpfungsmöglichkeiten für die verschiedenen Filter
Ausführen aller Filteraktionen, die die Brücke erlaubt (Positive oder negative Logik setzen, Count & Exec, Count, Threshold Triggered)

5.2.3 Router

Konfigurationsmöglichkeiten für Routing-Protokolle und geroutete Protokolle
unterstützte Protokolle aktivieren und deaktivieren
Anzeigen der aktuellen Verbindungen aktivierter Protokolle
Lesen und Setzen der Map-Tabellen, Hostnamen-Netzwerkadressen
Lesen und Setzen der Schnittstellen-Parameter zu den unterstützten Protokollen
Status der Schnittstelle, Knotenparameter, Routing-Status der Protokolle
Protokollspezifische Parameter für die einzelne Schnittstelle
Lesen und Setzen der dynamische und statische Adreßtabellen und Subnetz-Masken
Lesen und Setzen der Routing-Tabellen und Routing-Protokoll-Parameter (insbesondere Kostenparameter)
Download von vorkonfigurierten Tabellen
Lesen und Setzen der Access Lists, Filter auf der Basis von Netzwerkadressen
Lesen und Setzen der Adreßfilterung nach Ziel- und Quell-Adresse
Lesen und Setzen der Schwellwerte zur Unterdrückung von Broadcasts
Lesen und Setzen der Protokollfilter (Vergleich von Typ- bzw. Längenfeld, LLC-Header, Header für höhere Protokolle)
Filteraktionen - Ausführen aller Filteraktionen, die der Router erlaubt (positiv. negativ)
Downloadmöglichkeit von vorkonfigurierten Filtertabellen

5.3 Fehlermanagement

5.3.1 Fehlermanagement auf physikalischer Ebene

Up/Down Anzeige für alle Ports

Jumperzuordnungen zu Steckplätzen oder sonstigen Einstellungen sollen logisch/assoziativen Funktionen entsprechen, um die Einstellungen leicht einprägbar zu halten

Eingesteckte Schnittstellen-Karten, sowohl für LAN- als auch für WAN-Anbindungen, die nicht angeschlossen sind, dürfen das Netz in keiner Weise

5 3.2 Fehlermanagement auf MAC-Ebene

MAC-Counter entsprechend den medienspezifischen Zugangsverfahren für CSMA/CD, Token Ring, Token Bus und FDDI

Lesen der Ethernet MAC Counter z.B. Sende-, Empfangs- und Fehlerzähler (CRC Errors, Collisions,..)

Lesen der Token Ring MAC Counter Frame und Error Counter z.B. "Frame copied" Errors, Token Errors

Lesen der FDDI MAC Counter / SMT Counter z.B. TVX Experations, Lost Frames, Faulty Frames, Transitions to Ring Operational State

FDDI SMT Operations, SMT Frame Services z.B. Station Information Frames SIF, Link Error Monitor LER

5.3.3 Brücken

Anzeige von Pufferüberläufen

Cold Reset und Warm Reset, soll jeweils mißohne Selbsttest und Diagnosefunktionen möglich sein

Meldung über SPT Bekonfigurationen (Anzeige, Häufigkeit)

5.3.4 Router

Anzeige von Fehlern auf Schicht 3 (Netzwerk-Ebene) und 4, z.B. für Routing Protokolle und Kommunikations-Protokolle Protokoll-Timeouts

Lokale EvenVFehler Log Datei des Systems

Cold und Warm Reset soll jeweils mißohne Selbsttest und Diagnosefunktionen möglich sein

antivierbare Diagnosemöglichkeiten für die einzelnen Routing-Protokolle und gerosteten Protokolle

5.4 Performance Management

5.4.1 Gemeinsame Anforderungen an Brücken und Router

CPU Auslastung
Port-Auslastung
Pufferauslastung
Netzauslastung auf MAC-Ebene: Filtering- und Forwardingraten der einzelnen Ports in
* Frames/s und Byte/s
Funktionen zur Einstellung des Monitorintervalles
Darstellung von Spitzen-, Durchschnitts- und Augenblickswerten, Zeitmarken
Alarm-Begrenzungen, Schwellwerte
Statistiken in einfacher Form über V.24 Porl

4 2 Brücken

Gesendete/Empfangene Frames/Byte je Filter Gesendete/Empfangene Broadcast Frames und Multicast Frames Verhältnis von Broadcasts zu Non-Broadcasts Paketzähler für Protokolle und Stationen Anzeige der aktiven Stationen pro Port Brückenaktivität der einzelnen Ports in Frames/s und Byte/s Kommunikatonsmatrix mit Forwardingraten zwischen den Ports in Frames/s und Byte/s

5.4.3 Router

Prozeßlaufzeit einzelner Protokollprozesse
Statitistikwerte je gerouteten Protokoll (z.B. TCP/IP, DECnet) und je Routing-Protokoll (z.B. RIP, OSPF), wie
Empfangene Pakete/Byte
Gesendete Pakete/Byte
Broadcasts
Timeouts
Hop Counts
Fragmentierung
Reassemblierung
Verbindungsaufbau

5.5 Sicherheitsmanagement

Vergabe von SNMP Community Strings mit IP-Adresse
Zugriffsschutz durch Paßwortvergabe für einzelne User und das berechtigte Management-System
Paßwörter mit abgestuften Zugriff auf die Parameter der Station z.B. User, Local Network Manager, Global Network Manager, Field Engineer
Schützen besonders kritischer Befehle mit Paßwörtern (z.B. Boot-Befehl)

Zuordnung unterschiedlicher SET Community Strings standardisierte Verschlüsselungs-Mechanismen Meldung an NMS bei Mismatch zwischen der an einem Port konfigurierten MACAdresse und der tatsächlich gesehenen MAC-Adresse

5.6 Herstellerspezifische Management-Protokolle

Proprietäre Management-Protokolle für Token Ring-Brücken werden nicht als Lösung angesehen und sind zu vermeiden.

6. **Terminalkonzentratoren**

Terminalkonzentratoren sind Netzwerk-Komponenten, die niedrig-intelligenten Endgeräten (Terminals und andere seriell angeschlossene GErätewie Drucker, Meßgeräte, Steuergeräte etc.) den Netzzugang ermöglichen, indem sie herstellereigene Terminalprotokolle auf Netzwerk-Protokolle umsetzen und entsprechende Kommunikations-Aktionen, auch bidirektional, für die angebundenen Endgeräte tätigen. (externe Netzwerk-Intelligenz für unintelligente Endgeräte). In diesem Sinne sind Steuereinheiten (Host-Welt, z.B. IBM, Siemens) und Terminalserver (z.B. Digital-, UNIX-Welt) gleichzusetzen; als neutraler Begriff wurde im Rahmen dieses Papiers der Begriff Terminalkonzentratoren gewählt. Im Vergleich zu externen Netzwerk-Schnittstellen binden sie jedoch nicht nur ein Endgerät, sondern stets (potentiell) mehrere Endgeräte an das Netzwerk an. Steuereinheiten/Terminalserver können natürlich auch "non-LAN"-Anbindungen realisieren (KOAX-, SDLC-, HDLC-Protokolle), solche Anbindungen liegen jedoch nicht im Zielbereich dieses Papiers und werden nachfolgend

Folgende Angaben/Parameter über Terminalkonzentratoren sollten für ein NMS verfügbar verwaltbar sein:

6.1 Gesamter Terminalkonzentrator

Anzahl Netzwerk-Schnittstellen LANNVAN
Anzahl Terminalports Hardwareversion
Softwareversion logischer Name
Betriebsstatus Managementstatus
Manugementdomain Managementpasswort
Zeit seit letztem Reset (sysuptime)
Logeinträge seit letztem Reset Aktivierung
Selbsttestfunktion aktivierbare/te
Charakteristika (z.B. Protokolle)

2 Netzwerk-Schnittstelle LAN/WAN

Kurzbeschreibung physikalische Adresse logische Adresse (z.B. Node number, IP-Adresse) Hardwareversion Softwareversion Typ (Ethernet, Token-Ring, etc.) Anschlußart (DB9, RJ45, MMJ, etc.) Ubertragungsgeschwindigkeit logische Bezeichnung Mananementstatus

Verkehrsstatus/statistik Netzwerk-Schnittstelle
- Auslastung
- Kollisionen bzw. Token-Rotation-Time
- Spitzenwert der Auslastung, Durchschnittswert der Auslastung
- Summe der empfangenen Daten
- Summe der gesendeten Daten
- Summe der zurückgewiesenen Daten
- Summe fehlerhafte Daten

3 Terminalschnittstellen/Ports

Nummer
Name
Beschreibung
Managementstatus
Managementpasswort
Zugangspasswort
Konfigurationsparameter
Zeichenlänge
Parität
Flow Control
Ubertragungsverfahren (synchron, asynchron)
Modemkontrollfunktion
Ubertragungsgeschwindigkeit
Anzahl der Sessions
aktivierte Charakteristika (Autoconnect, Broadcast, etc.)
preferred Service
~etneDsstatus
Betriebsmodus (Protokoll-Modus, transparenter Modus)
Angaben zum Terminal / Endgerät
Terminaltyp
Name
Standort
AKov~erung/Deaktivierung jedes einzelnen Ports
SLIP-Informationen (z.B. IP-Adressen der Ports etc.)
PPP-Informationen
Informationen über andere Ebene-2-Protokolle der Konzentratofen

7. **Netzwerk-Schnittstelle (Adapterkarten)**

Netzwerk-Schnittstelle stellen die Anschluß-Komponente eines Endgerätes an das Netzwerk (die Netzwerk-Infrastruktur) dar. Bei Endgeräten sind dies in der Regel sogenannte Adapterkarten als Einschubkarte in den PC oder die Workstation. Bei Hosts erfolgt der Netzwerkanschluß teilweise über separate "Boxen", die das Netzwerk-Schnittstelle hardwaremäßig realisieren und selbst eine Adapterkarte zur Verkabelungsseite hin besitzen. Dieses Papier beschränkt sich auf Adapterkarten, die genannten Anforderungen sind auf externe Netzwerk-Interfaces für Hosts übertragbar.

Das Netzwerk-Schnittstelle / die Adapterkarte implementiert- die kabelunabhängige Übertragung (PLS Physical Layer Signaling) der LAN-Schnittstelle und darüber hinaus mindestens noch die MAC-Ebene sowie die Data Link Schnittstelle (z.B. NDIS, ODI), u.U. auch noch Teile der höheren Protokoll-Ebenen, die entsprechend iadbar sind. Die Adapterkarte realisiert nach oben (im Sinne des OSI-Referenzmodells) die Schnittstelle zur höheren Kommunikations-Software. Sie interagiert dabei im Verlauf des Kommunikationsvorgangs mit der System-Hardware und -Software des Endsystems.

Zu verwaltende Komponenten sind:

LAN-Adapter (Standard LANs; Für PC's, Workstations, Gateways, TK-Anlage)
WAN-Adapter (Modems, X.25, ISDN) als Bestandteil von Koppelelementen

Anforderungen an LAN- und WAN-Adapter (allg.):

Aktivieren/Deaktivieren
Möglichkeit zum Download der Software/Updates (z.B. Flash-EPROM)
Status-Informationen
Standard-Fehlermeldun
g aktive Protokolle
Konfigurationsdaten
Jumpereinstellungen sollten auslesbar und mit entsprechender Interpretation versehen sein

Bemerkungen:

Bei der Implementierung eines SNMP-Agenten im Endgerät, ist eine entsprechende CPU-Leistung vorzusehen. Dazu gehört ein entsprechender Protokollstack und ein geeignetes Betriebssystem. Da nicht jedes Endgerät ein Multitasking-OS besitzt, sind Zwischenlösungen vorstellbar. Eine davon ist die Auslagerung einzelner Teile auf eine intelligente Adapterkarte Dabei kann die Kommunikation über den HW-Bus zu Performanceproblemen führen.