Netzwerkmanagement mit SNMP

→ Teil 6: Remote Network Monitoring (RMON)

Prof. Dr. Norbert Pohlmann

Fachbereich Informatik

Verteilte Systeme und Informationssicherheit

Fachhochschule Gelsenkirchen

Inhalt

- **Einführung**
- **Remote Network MONitoring (RMON1)**
- **RMON2**
- **Zusammenfassung**

Inhalt

- **Einführung**
- Remote Network MONitoring (RMON1)
- RMON2
- Zusammenfassung

Einführung (1/4)

- Die Verwaltung von lokalen Netzen (LAN) mit ihren Hubs, Repeatern und Bridges bilden ein wichtiges Teilgebiet des Netzwerkmanagements, weil:
  - heute sehr viel mehr Rechner (PC, Server, ...) an einen LAN angeschlossen sind als (unmittelbar) an das INTERNET (WAN, ...),
  - die auf Kommunikationsebene 1 und 2 arbeitenden Komponenten (Repeater, Bridges, Switches, ...) in LANs zahlreicher vorhanden sind als Router und
  - diese Komponenten von ihrer „Management-Intelligenz“ her eher im unteren Bereich angesiedelt sind.

Einführung (2/4)

- Der Remote-Monitoring (RMON)-Standard wurde aus der Erfahrung mit proprietären **Netz-Probes** heraus entwickelt.
- Probes sind **Meßwerterfassungskomponenten**, die man in den verschiedenen LAN-Segmenten zur **Überwachung des LAN-Verkehrs** einsetzt und deren erfaßte Werte einer Auswertekomponente, i.d.R. einem LAN-Monitor oder -Analysator, zugefügt werden.
- In den Probes kann eine gewisse Vorbereitung der Daten erfolgen.
- Die RMON-MIB (RFC 1757) beschreibt Managementobjekte eines standardisierten entfernten Netzüberwachungsgerätes (Remote Network Management Device), sie ist gewissermaßen die Abstraktion eines Probes, einer Meßsonde.
- Ihre Objekte stellen natürlich **höhere Anforderungen** an den unterstützenden Agenten als die Standard-MIB II, denn RMON definiert u.a. als Managementobjekte auch **Ergebnisse von Statistikberechnungen**.

Einführung (3/4)

- Der durch Polling bedingte Netzverkehr kann etwas vermindert werden, da in den **Agenten mehr Vorbearbeitung** geschieht.
- Ferner wird durch die RMON-MIB die Menge der mittels SNMP standardisiert verwaltbaren Ressourcen vergrößert, da RMON insbesondere die LAN-Überwachung, also unterhalb der IP-Ebene, ausgerichtet ist.
- Falls die Agenten-Ressourcen ausreichen, können Überwachungsdaten auch weiter gesammelt werden, wenn die SNMP-Verbindung zum Manager unterbrochen ist.
- Die RMON-Agenten können darüber hinaus grundsätzlich von mehreren Managern verwaltet werden.
- Durch RMON ist ein **flexibles Monitoring** möglich.

Einführung (4/4)
→ Typische Funktionen eines Network Monitors

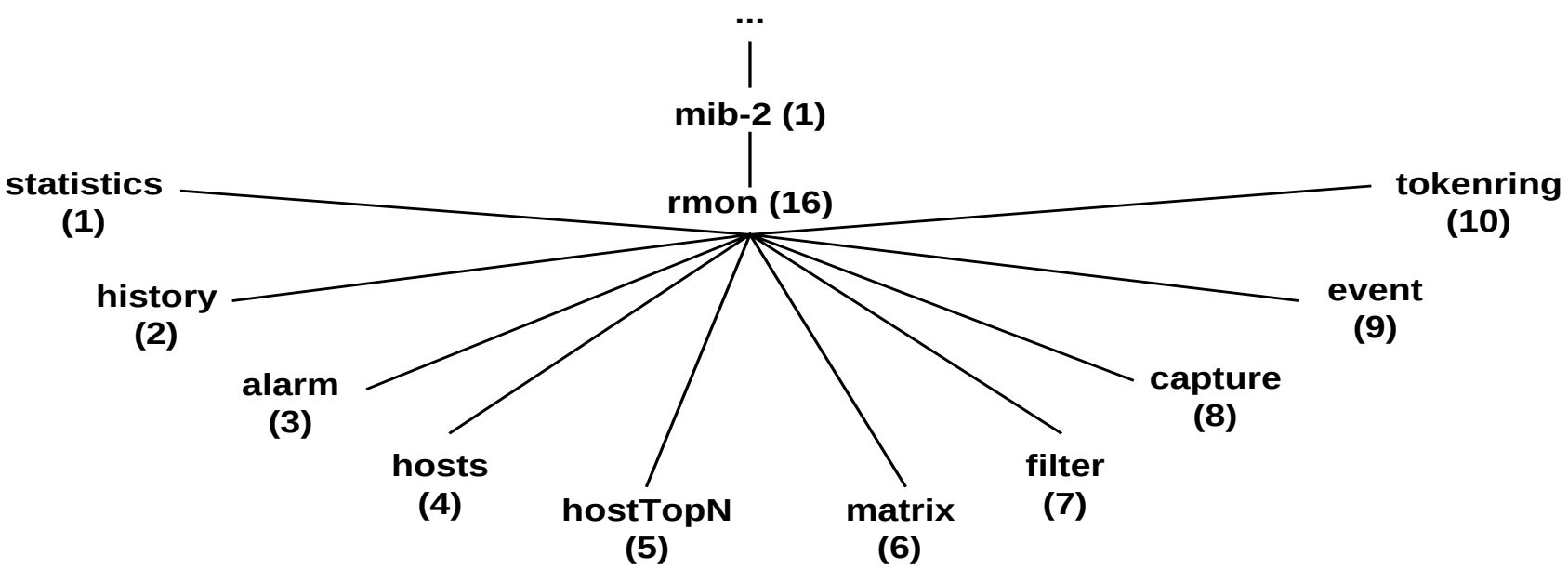
- Identifikation der am LAN angeschlossenen Stationen über ihre physikalische Adresse
- Ermittlung und graphische Darstellung der Netzbelastung
- Ermittlung und Darstellung des Datenverkehrsaufkommens der Stationen, wie z.B.
  - Liste der zehn aktivsten Sender (Top Ten Talkers)
  - Matrix des Verkehrsaufkommens zwischen jeweils zwei Stationen,
- Ermittlung und Darstellung der prozentualen Anteile der einzelnen höheren Kommunikationsprotokolle (TCP/IP, IPX/SPX, NetBios, usw.)
- Erfassung von Broadcast- und Multicast-Frames, sowie von besonderen Ereignissen (z.B. Kollision)
- Beobachtung einzelner Stationen
- Durchführung von Test.

Inhalt

- Einführung
- **Remote Network MONitoring (RMON1)**
- RMON2
- Zusammenfassung

RMON
→ Remote Network MONitoring

- Die RMON-MIB (RFC 1757) belegt den Teilbaum 16 unterhalb des Strukturknotens MIB II im Internet-Registrierungsbaum.
- Er besteht aus 10 MIB-Gruppen.



RMON1, Standard-RMON

- Die später entwickelte RMON2-MIB (RFC 2021) besteht derzeit aus weiteren Gruppen, die als zusätzliche Teilbäume unter MIB-2.16 eingehängt sind.
- Die ersten 10 Gruppen werden als RMON1 oder Standard-RMON bezeichnet.
- Insgesamt umfaßt RMON mehr als 200 Managementobjekte.
- Alle RMON-Gruppen sind optional, d.h. „RMON“-konforme Produkte müssen nicht alle Gruppen unterstützen.

Die RMON1-MIB
→ statistic-Gruppe (1)

- Die statistic-Gruppe enthält Statistik-Werte über den Paketverkehr auf dem Netz, die der Monitor auf seinen LAN-Interfaces erfasst.
- Es ist zu berücksichtigen, dass ein Monitor an mehrere LAN-Segmente gleichzeitig angeschlossen sein kann.
- Die statistic-Gruppe stellt (pro Segment) u.a. die folgenden Managementinformationen zur Verfügung:
  - Anzahl von Paketen, Bytes, Broadcast, Multicast und deren Verteilung
  - Paketverluste, Kollisionen, CRC-Fehler, zu kleine bzw. große Pakete
- Ein Teil der Größen kommt auch in der Interface-Gruppe der MIB-II vor, bezieht sich aber dort auf Einzelgeräte, während hier mehr die **Verkehrslast und die Fehlerraten eines LAN-Segmentes** gemeint sind.

Die RMON1-MIB
→ history-Gruppe (2)

- Die history-Gruppe liefert die Basis für eine Trendanalyse, indem die Aufzeichnung von Überwachungsinformationen der statistics-Gruppen ermöglicht wird.
- In einer Steuertabelle (controlTable) können Beobachtungshäufigkeiten und Meßintervalle für einzelne Schnittstellen festgelegt werden.
- Die Ergebnisse werden dann in weiteren Tabellen (historyTable) abgelegt.
- Das Tabellenmanagement (Konventionen, Arithmetik, Veränderung und Löschen von Tabellenzeilen etc.) im SNMP-Umfeld ist recht kompliziert.
- Originaldokument ist RFC1757.

Die RMON1-MIB
→ alarm-Gruppe (3)

- Die alarm-Gruppe dient dazu, auf der Basis von Schwellwertanalysen Alarmauslösungen zu definieren.
- Mittels oberer und unterer Schwellwerte, werden die einzelnen Meßgrößen (z.B. Lastwerte, Fehlerraten) zugeordnet.
- Dann kann ein Hysterese-Mechanismus bezogen auf absolute bzw. relative Änderungen der Meßgrößen festgelegt werden.
- Die Alarme werden dann über Trap-Nachrichten von SNMP an den Manager geschickt.

Die RMON1-MIB
→ host-Gruppe (4)

- Die host-Gruppe enthält statistische Informationen zu jedem Netzverkehr verursachenden Host im Segment, die durch das Beobachten der MAC-Adressen in den Paketen zustanden kommen.
- Die host-Gruppe besteht ihrerseits wieder aus Tabellen.
- Eine Steuertabelle (hostControlTable) definiert die zu überwachenden Hosts und den Meßzeitraum.
- Die hostTable enthält die Meßdaten nach MAC-Adressen geordnet (gesendete/empfangene Pakete, Broadcasts, fehlerhafte Pakete, usw.).
- Die hostTimeTable enthält im wesentlichen die gleichen Informationen, jedoch zeitlich nach dem Entstehungszeitpunkt geordnet.

Die RMON1-MIB
→ hostTopN-Gruppe (5)

- Die hostTopN-Gruppe ermöglicht es, Statistiken von denjenigen N Host zu erhalten, die die Statistiklisten bzgl. vorzugebenden Meßgrößen anführen.
- Dabei wird diese Auswertung vom Agenten, nicht vom Manager für vorzugebende Meßintervalle durchgeführt, wodurch der SNMP-Verkehr reduziert wird.

Die RMON1-MIB
→ matrix-Gruppe (6)

- Die matrix-Gruppe gestattet, für zu definierende Quell-Senken-Paare von MAC-Adressen (Hosts) Verkehrsmatrizen richtungsbezogen aufzustellen.

Die RMON1-MIB
→ filter-Gruppe (7)

- Die filter-Gruppe ermöglicht die Definition und die Anwendung von Filtern, d.h. die Bedingungen, für die Aufzeichnung von Paketen.
- Datenfilter spezifizieren das Selektieren von Paketen auf der Basis von Bitmuster in den Paketen.
- Zustandsfilter definieren die Auswahl anhand von Zustandsinformationen wie CRC-Fehler, Paketlängen-Verletzung u.ä. Komplexe Filterbedingungen.
  Diese können über Bedingungsausdrücke (AND/OR-Verknüpfungen) formuliert werden.
- Der Paketstrom, der erfolgreich einen Filtertest passiert, wird Channel genannt.
- Mit einem Channel können Zähler und Ereignisse assoziiert werden.

Die RMON1-MIB
→ packetCapture-Gruppe (8)

- Die packetCapture-Gruppe stellt die Mechanismen bereit, um Pakete, die die in der Filtergruppe definierten Channel passiert haben, in Puffer abzulegen und durch die Managementstation abzurufen.
- Dabei können die Pakete in voller Länge oder nur die ersten n Bytes abgelegt und abgerufen werden.
- Ein wichtiges Einsatzgebiet für die packetCapture-Gruppe sind die Trace-Anwendungen auf der Managementstation.

Die RMON1-MIB
→ event-Gruppe (9)

- Die event-Gruppe schließlich unterstützt das Definieren von Ereignissen, die dann gegebenenfalls Aktionen auslösen, die an anderer Stelle in der MIB definiert sind.
- Auch die Bedingungen für die Ereignisse können in anderen RMON-MIB-Gruppen definiert sein.
- Beispiele von Ereignissen sind:
  - keine
  - Log-Eintrag
  - es wird ein Trap gesendet
  - Log und Trap

Inhalt

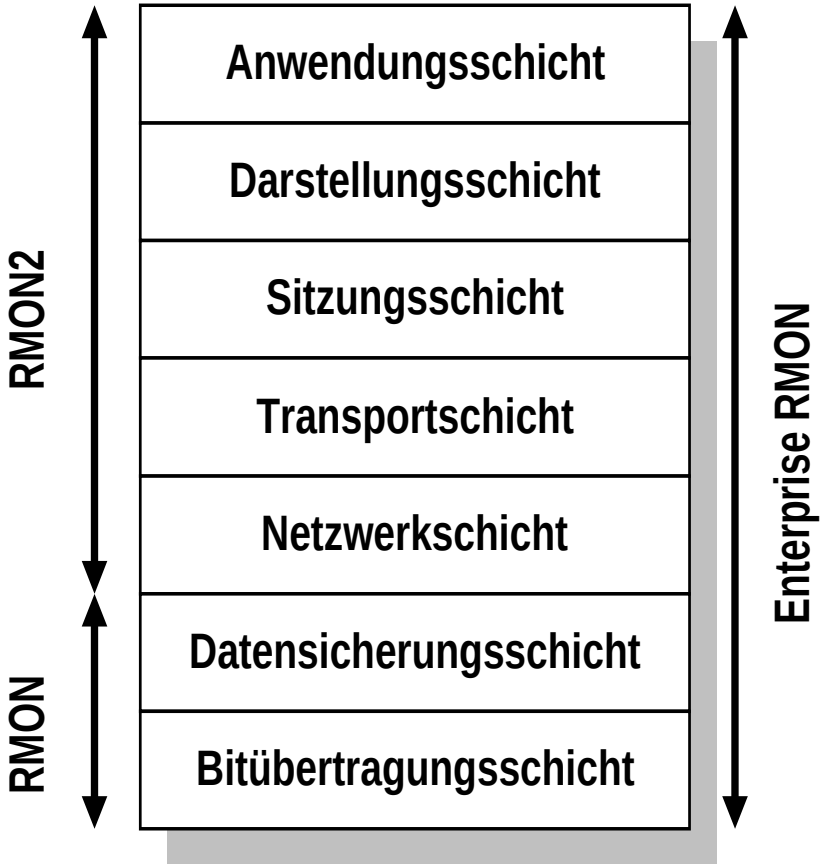
- Einführung
- Remote Network MONitoring (RMON1)
- **RMON2**
- Zusammenfassung

RMON2

- Während RMON1 im wesentlichen eine Protokollanalyse der OSI-Ebenen 1 und 2 durchführt, erweitert RMON2 (RFC2021) die Analyse auf die Ebenen 3-7.
- Damit kann sowohl das Internetworking als auch die Anwendungsebene (E-Mail, Filetransfer, WWW, ...) besser überwacht werden.
- Die wesentlichen Informationen für den Manager werden schon auf dem RMON-Agenten aufbereitet.

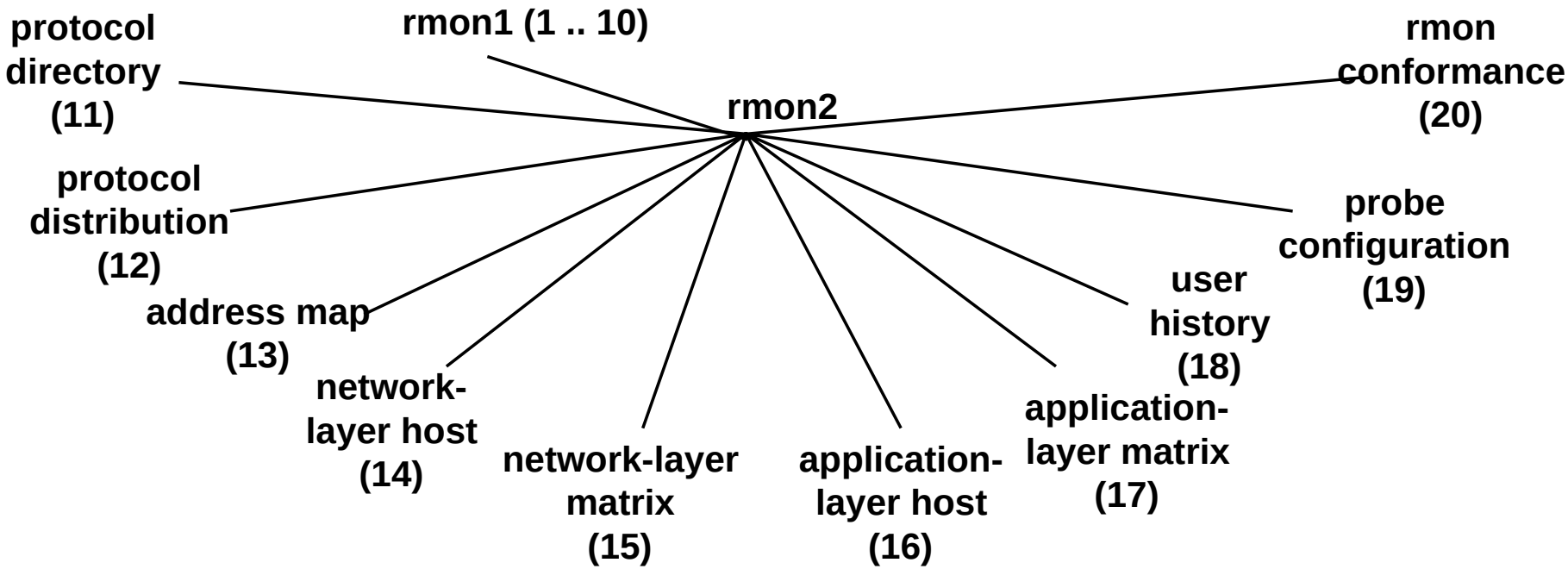
RMON1 vs. RMON2

- RMON1 (Standard-RMON):
  - nur Monitoring der unteren beiden Schichten des ISO/OSI-Referenzmodelles
  - keine End-to-End-Überwachung möglich
- RMON2:
  - Monitoring Schichten 3-7
  - dadurch auch Applikations-Monitoring möglich, z.B. E-Mail, Filetransfer, WWW, usw.



RMON2 MIB

- RMON2 ergänzt RMON durch 10 weitere MIB-Gruppen (11-20).



Die RMON2-MIB
→ protocolDir-Gruppe (11)

- Die protocolDir-Gruppe listet alle Protokolle in einer Tabelle auf, die vom Agenten überwacht werden kann.
- Die Gruppe gibt auch Auskunft über die überwachten Protokollparameter, PDU-Strukturen u.ä.

Die RMON2-MIB
→ protocolDirtribution-Gruppe (12)

- Die protocolDirtribution-Gruppe sammelt protokollbezogene Statistiken über Pakete etc.
- Somit können schichtbezogen benötigte Bandbreiten u.ä. festgelegt werden.

Die RMON2-MIB
→ addressMap-Gruppe (13)

- Die addressMap-Gruppe enthält Abbildungen zwischen MAC- und Netzadressen und unterstützt die Erzeugung von Topologie-Karten und Auto-Discovery.

Die RMON2-MIB
→ nlHost-Gruppe (14)

- Die nlHost-Gruppe zählt den Netzverkehr (vornehmlich IP-Verkehr) bezogen auf die Netzadressen (IP Adressen), dabei können die gewünschten Daten wieder über eine entsprechende Steuertabelle vorgegeben werden.

Die RMON2-MIB

→ nlMatrix-Gruppe (15), alHost-Gruppe (16), alMatrix-Gruppe (17)

- Die nlMatrix-Gruppe enthält die Verkehrsmatrix auf Netzebene.
- Die alHost- bzw, alMatrix-Gruppen sind die entsprechenden Gruppen für die Anwendungsschicht, bei denen man bezogen auf bestimmte Hosts und die gemäß protocolDir-Gruppen unterstützten Anwendungsprotokolle gewisse Managementinformationen abfragen kann.

Die RMON2-MIB
→ usrHistory-Gruppe (18)

- Die usrHistory-Gruppe gestattet, in anwendungsspezifischer Weise unter Zuhilfenahme der alarm- und history-Gruppe Verlaufsdaten zu sammeln und zu speichern.

Die RMON2-MIB
→ probeConfig-Gruppe (19) / rmonConformance-Gruppe (20)

- Mit der probeConfig-Gruppe und der rmonConformance -Gruppe werden Informationen beschrieben, die nötig sind, um Interoperabilität von RMON-Implementierungen beurteilen und managen zu können.
- Hierzu zählt u.a. die Kenntnis über die von Agenten unterstützten MIB-Gruppen und die Werte der Konfigurationsparameter für die Probes als die RMON-Agenten.

Inhalt

- Einführung
- Remote Network MONitoring (RMON1)
- RMON2
- **Zusammenfassung**

Zusammenfassung
→ RMON (1/3)

- Insgesamt gestattet die RMON-MIB erhebliche Fortschritte gegenüber der MIB-II bei der wichtigen Aufgabe der Netzüberwachung (remote monitoring).
- Vorteile von RMON sind u.a.:
  - Reduktion des Netzverkehrs
  - offline-Erfassung sowie
  - mehrere Manager für die RMON-Agenten.
- Voraussetzung ist, dass die Probes an einer „sinnvollen“ Stelle im Netz plaziert sind.
- Nachteile von RMON sind:
  - kompliziertes Tabellenmanagement und die
  - Notwendigkeit komplexerer Agenten.
- Die komplexerern Agenten können zur Folge haben, dass hierfür dedizierte Geräte erforderlich sind.

Zusammenfassung
→ RMON (2/3)

- Es gibt schon eine Reihe von Netzkomponenten (z.B. Hubs und Switches), die einen RMON-Agenten integriert haben; häufig werden aber nur die ersten 4 Gruppen unterstützt (statistics, history, hostTable, alarm).
- Bei der Beurteilung von RMON-Produkten müssen u.a. folgende Punkte betrachtet werden:
  - die Zahl der unterstützten RMON-Gruppen,
  - die max. Anzahl der überwachten Knoten,
  - die CPU- und Speicherkapazitäten für das Filtern, Erfassen und Speichern von Verkehr,
  - der Paket-Durchsatz bzw. die zeitlich maximale Auflösung und
  - die auf der Managementplattform verfügbaren RMON-Anwendungen.

Zusammenfassung
→ RMON (3/3)

- Die RMON-Anwendungen betreffen die nachgelagerten Verfahren zur Bedarfsfestellung, QoS-Management, Kapazitätsplanung und zum Berichtswesen.
- Die RMON-Probes können zwar alle möglichen Daten sammeln, aber die Manager bleiben für die managementrelevanten Reaktionen durch geeignete Anwendungen zuständig.

Netzwerkmanagement mit SNMP

→ Teil 6: Remote Network Monitoring (RMON)

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

norbert.pohlmann@informatik.fh-gelsenkirchen.de

Fachhochschule Gelsenkirchen