Editor (Hrsg.): 11. DFN-Forum Kommunikationstechnologien,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2018 1

Protokollgestützte Selbstbeschreibung in Zugangsnetzen

Tobias Guggemos[1], Vitalian Danciu[1], Annette Kostelezky[1]

Abstract: Die Selbstbeschreibung leitungsgebundener Anschlüsse ist für die Erstkonfiguration und Fehlersuche hilfreich. Die Modellierung eines Managementszenarios in einem Hochschulnetz erlaubt die Isolation von Fehlertypen, die mit Hilfe eines in dieser Arbeit vorgestellten Protokolls zur Selbstbeschreibung adressiert werden können. Die Untersuchung des Einsatzes dieses Protokolls in mehreren Netzen weist seine Eignung für großflächigere Nutzung auf.

Keywords: Selbstbeschreibung; LAN; VLAN; Zugangsnetz

1 Einführung

Die Zugangsnetze eines Hochschulnetzes können sich als virtuelle Netze bzw. VLANs in die Institute der Universität erstrecken, um dort Endgeräte miteinander und mit dem Internet zu verbinden. Die Nutzung des Zugangsnetzes erfolgt durch die Institute selbst, die manche Aspekte ihrer Struktur mitbestimmen und mitverwalten. Die einer virtuellen Netztopologie inhärente Flexibilität erfordert ein verteiltes Management der Zuordnung von Ressourcen wie Adressen, Portgruppen, Netzanschlüssen (Dosen) in Arbeitszimmern, VLAN-IDs auch für leitungsgebundene Anschlüsse. Zur Vermeidung von Fehlern und Erleichterung der Initialkonfiguration ist eine Selbstbeschreibung erforderlich, wie sie etwa von 802.11-Netzen bekannt ist.

Szenario
Betrachten wir ein Hochschulnetz bestehend aus einem zentral betriebenen Kernnetz, Zugangsnetzen und lokal, jeweils in den Instituten verwaltete Endgeräte (Server, Terminals, Drucker etc). Administratoren an den Instituten fordern am Service Desk des zentralen Netzbetreibers Netzressourcen an. Der Netzbetreiber schaltet die erforderlichen Anschlüsse als VLANs an den entsprechenden Switchports, weist entsprechende IP-Subnetze zu und sorgt für die Vermittlung der IP-Adressen dieser Subnetze im Hochschulnetz. Der Übergabepunkt des Dienstes sind die mit den Switchports fest verbundenen Wanddosen.

Der Administrator hat als *Besitzer* der zugewiesenen Ressourcen folgende Aufgaben bei der Inbetriebnahme: 1. Überprüfung von a) Zusammengehörigkeit der Switchports bzw. Wanddosen in einem VLAN b) Korrektheit der zugewiesenen VLAN-ID c) Korrektheit des

[1] MNM-Team, Ludwig-Maximilans-Universität München, Oettingenstr. 67, 80538 München, Germany
Email: {guggemos, danciu, kostelezky}@nm.ifi.lmu.de

zugewiesenen IP-Subnetzes und der Vermittlungsfunktion 2. Konfiguration von IP-Adressen und sonstigen Parametern für den Netzzugang an den Endgeräten 3. Anschluss von a) Servern an die Switchports b) Arbeitsplatzrechnern/Terminals und Peripherie an die Wanddosen, sowie 4. Reklamation eventueller Konfigurationsfehler an den Netzbetreiber.

Diese trivial erscheinenden Aufgaben des Besitzers stellen Herausforderungen aufgrund der Verteilung der Information über die Ressourcenzuweisung zwischen Netzbetreiber und -besitzerdomäne sowie aufgrund der Freiheiten in der dynamischen Zuweisung der Adressen und Ports: in einem Laborraum mit einer signifikanten Anzahl Wanddosen ist es selbst bei ihrer korrekten Beschriftung nicht ohne weitere Aufzeichnungen ersichtlich, an welche Dose ein Rechner mit einem bestimmten Zweck angeschlossen werden soll. Fehlerfälle können sowohl die mitgeführten Aufzeichnungen als auch die Konfiguration seitens des Netzbetreibers in Zweifel ziehen.

Beitrag und Übersicht dieser Arbeit
Die im Szenario aufgezeigten Herausforderungen werden in Abschnitt 2 in einem Modell gefasst, dass eine Unterscheidung der in dieser Arbeit betrachteten Teilprobleme erlaubt. Als Lösungsansatz wird ein Protokoll zur Selbstbeschreibung in Abschnitt 3 eingeführt und sein bisheriger praktischer Einsatz in Abschnitt 5 diskutiert. Abschnitt 6 diskutiert den Stand der Technik und verwandte Arbeiten zu Selbstbeschreibung und *Discovery*. Schließlich werden in Abschnitt 7 weiterführende Ideen für die Selbstkonfiguration in Zugangsnetzen vorgestellt.

2 Problemraum

Die Formalisierung des Szenarios in Abschnitt 1 erarbeitet die Relationen zwischen den Elementen in den verschiedenen Managementdomänen auf sowie die Informationen, die zwischen Besitzer und Betreiber (im folgenden auch „ISP“) abgeglichen werden müssen. Die besprochenen Konzepte werden in Abb. 1 illustriert.

2.1 Modell

Wir definieren die relevanten Begriffe und Rollen, beschreiben Annahmen bezüglich des Wissens der jeweiligen Rollen sowie bezüglich des Verwaltungsprozesses für Netzressourcen.

Begriffe
Die folgenden zu verwaltenden Elemente sind für den Managementanwendungsfall relevant. Großbuchstaben ’X’ verstehen sich als „Menge aller x”, ein Subskript „frei“ oder „belegt“ gibt die freie bzw. belegte Teilmenge der x an.

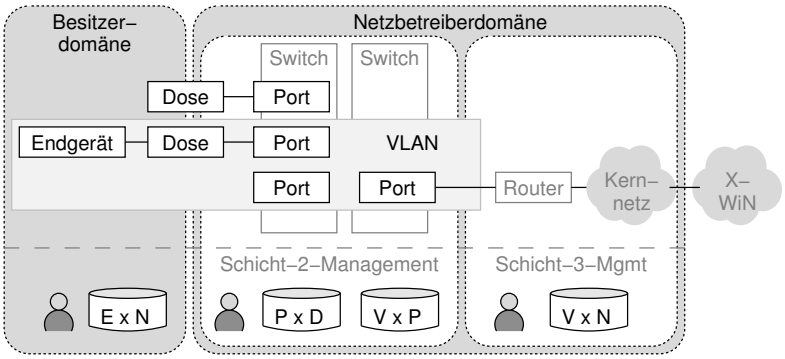


Abb. 1: Elemente und Domänen

e Endgerät: ein Rechner, der an eine Dose angeschlossen ist
d Dose: Endpunkt in der Wand, nicht am Switch
a Anschluss: die Verbindung zwischen einem Endgerät und einer Dose; kann korrekt oder falsch sein.
p Port: am Switch
v VLAN: $v \subset P$ d.h. Untermenge der Menge aller Ports
n IP-Netz: eine Menge von IP-Adressen eines IP-Netzes in einer BC-Domäne
z Zweck: eine Nutzungsabsicht für eine Ressource

Rollen
Wir unterscheiden zwischen den folgenden Rollen und ihren typischen Funktionen.

b Besitzer: Nutzer eines VLAN bzw. IP-Subnetz und Administrator der daran angeschlossenen Endgeräte
ISP/L2 Netzmanager für die Sicherungsschicht: Vergabe Portgruppe/VLAN, Konfiguration der Switches
ISP/L3 Netzmanager für die Vermittlungsschicht: Vergabe IP-Adressen, Konfiguration der Router

Zuweisungsfunktionen werden vom Besitzer ausgelöst und umfassen: 1. Zuweisung eines neuen VLAN (neue VLAN-ID) an den Besitzer. 2. Zuweisung eines Ports und Einbindung in ein bestehendes VLAN des Besitzers. 3. Umschaltung eines Ports zwischen zwei VLAN des Besitzers.

2.2 Fragestellung

Aufgabenstellung dieser Arbeit ist die Unterstützung des Besitzers bei der Erstellung korrekter Anschlüsse. Ein Anschluss a ist korrekt, wenn gilt:

Abbildung	*verantwortlich*	*Fehlerbeispiel*
$E \mapsto N$	b	falsche IP-Adresse, falsche Netzmaske
$N \mapsto V$	ISP/L3	Port vergessen, Port in falschem VLAN
$V \mapsto P$	ISP/L2	falscher Eintrag in RT
$P \mapsto D$	ISP/b	falscher Patch, falsche Beschriftung

Tab. 1: Abbildungen und Beispiele für Fehler

- e hat eine IP-Adresse aus n
- n wird in v geroutet
- p gehört zu v
- p führt zu d

Die Abbildungen zwischen Netzelementen sind in Tab. 1 dargestellt.

Einschränkungen
Wir schließen die Betrachtung der folgenden Aspekte aus: 1. Eigenschaften von Ports (z.B. tagged/untagged): ein erfolgreich zugewiesener Port ist eingeschaltet und zweckmäßig konfiguriert; sonst gilt er als nicht erfolgreich zugewiesen. Wir nehmen ferner an, dass der ISP keine von Besitzern nutzbare Informations- und Konfigurationsdienste bereitstellt. Dazu gehören 2. Dienste seitens des ISP/L2 (z.B. Identifizierung des Switch mit LLDP) sowie 3. Dienste seitens des ISP/L3 (z.B. DHCP). 4. Die Rückgabe von Ressourcen an den ISP wird nicht berücksichtigt: diese Arbeit fokussiert sich auf die korrekte Zuweisung und Konfiguration.

Systematik der Fragestellung
Die in Tab. 2 dargestellten Fälle repräsentieren das Vorkommen von Fehlern in den in Tab. 1 aufgezählten Abbildungen. Ein Mechanismus zur Selbstbeschreibung sollte in der Lage sein, einen Teil dieser Fälle direkt zu unterstützen (z.B. Fall 3) und manche mittelbar (z.B. kann für Fall 9 eine Überprüfung der Schicht-3-Konnektivität erfolgen). Ambiguität liegt vor, wenn aufgrund der Kenntnis der Broadcast-Domäne, ihrer VLAN-ID sowie des Netzpräfix eine scheinbar korrekte Funktionsweise denkbar ist.

3 Protokoll zur Selbstbeschreibung

Der Name des Protokolls, *A-NetBeacon*, deutet auf sein Funktionsprinzip hin, durch periodische Nachrichten in einer Broadcast-Domäne der Sicherungsschicht über die Eigenschaften dieser Broadcastdomäne zu informieren. Das wichtigste Ziel beim Entwurf des Protokolls ist ein möglichst großer Bereich seiner Anwendbarkeit. Es macht daher keine Annahmen bezüglich der Vermittlungsschicht, sondern wird direkt in Rahmen der Sicherungsschicht transportiert. Die Annahmen bezüglich der Sicherungsschicht beschränken sich auf die durch die Ethernet-Hardware gegebenen Eigenschaften. Weiterhin werden die übertragenen Daten auch in einer menschenlesbaren Fassung in den Nachrichten kodiert, um eine

	N × V	V × P	P × D	N × E	Rolle	Ambig?	Fehlerbeispiel
1	.	.	.	.	–	-	keine Fehler
2	.	.	.	✘	b	-	e falsch konfiguriert
3	.	.	✘	.	b	-	Dose falsch beschriftet
4	.	.	✘	✘	b	✔	2 und 3
5	.	✘	.	.	L2	-	Port in falschem VLAN
6	.	✘	.	✘	b, L2	✔	2 und 5
7	.	✘	✘	.	L2	✔	falsches VLAN an falsch beschrifteten Port
8	.	✘	✘	✘	b, L2	✔	4 und 5: Schicht-2-Fehler
9	✘	.	.	.	L3		falscher Eintrag in RT für n in v
10	✘	.	.	✘	b, L3	✔	e falsch konfiguriert im falschen Netz
11	✘	.	✘	.	L2, L3	✔	falsches Netz an falscher Dose
12	✘	.	✘	✘	alle	✔	2 und 10
13	✘	✘	.	.	L2, L3	✔	falsches Netz im falschen VLAN
14	✘	✘	.	✘	alle	✔	2 und 13
15	✘	✘	✘	.	L2, L3	✔	Konfiguration in ISP-Domäne falsch
16	✘	✘	✘	✘	alle	✔	alle Fehler

Tab. 2: Betrachtete Fehlerfälle: ✘ bezeichnet Fehler

leichte Lesbarkeit der Selbstbeschreibungsnachrichten mit generischen Werkzeugen zu ermöglichen.

Funktion

Eine “Beacon”-Nachricht wird im Ethernet-Broadcast über einen Anschluss des Besitzers im VLAN verbreitet (vgl. Abb. 2). Sie kann an allen anderen Dosen bzw. Ports empfangen werden und lässt die Gruppenzugehörigkeit von Ports nachweisen. Die Information in den Nachrichten gibt direkte Hinweise auf mindestens die folgenden Fehlerfälle aus Abschnitt 2, Tab. 2: die Fälle (2, 3, 4) in alleiniger Verantwortung des Besitzers, und isolierte Fehler (5, 7) in der Schicht-2-Konfiguration des Netzbetreibers. Grundlage für weitere Diagnoseschritte wird für die Fälle (9, 10, 13) gegeben.

Sicherheit

Zur Wahrung von Integrität und Authentizität der für das Netzmanagement genutzten Informationen ist ein Challenge-Response-Verfahren vorgesehen mit dem Clients signierte Nachrichten vom Server anfordern können. Der Client sendet eine Nonce in der Anfrage, die von dem Server zusammen mit einem Zeitstempel und der Selbstbeschreibungsinformation signiert wird. Das Verfahren bietet Schutz vor Replay-Angriffen, bei denen die Nachrichten eines Servers in ein anderes Netz kopiert werden.

Datenmodell

Die gesendeten Daten sind Name-Wert-Paare, die im Prototyp als LLDP-Tripel (Typ, Länge, Wert) codiert werden. Dieses erweiterbare Schema umfasst derzeit als optionale Felder 1. VLAN-ID 2. VLAN Name 3. Benutzerdefinierter Freitext 4. IPv4 Netz 5. IPv6 Netz 6. E-Mail-Adresse des Domänenbesitzers 7. Authentifizierung (siehe Abschnitt 3) 8. Repräsentation aller Inhalte in ASCII.

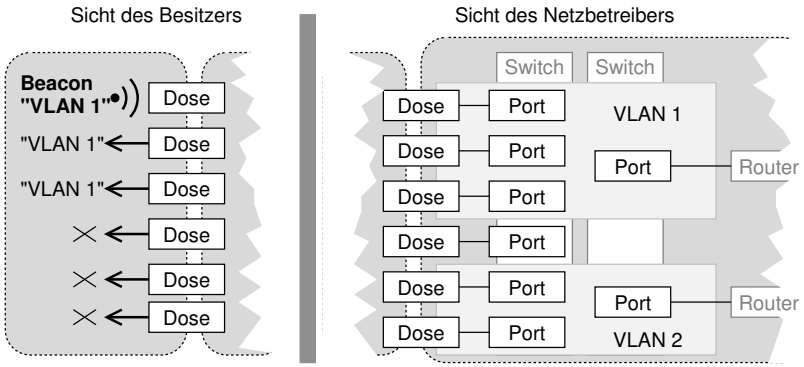


Abb. 2: Funktionsprinzip und Sichten

Um die Unterdrückung des Broadcast durch LLDP-fähige Switches zu vermeiden benutzt *A-NetBeacon* einen *Local Experimental Ethertype* mit Typcode `0x88b5`.

Prototyp
Ein Prototyp wurde in C implementiert[2] und auf einem Kleinstrechner (Banana Pi mit einem angeschlossenen Bildschirm erprobt. Der Prototyp implementiert sowohl den Server als auch eine Client-Anwendung, welche die in LLDP transportierten Informationen einfach menschenlesbar auf dem Bildschirm darstellt. Neben der Verwendung des Clients ist es aber auch möglich, die Informationen mittels eines Werkzeugs zur Netzanalyse (z.B. *tcpdump*) anzuzeigen. Abb. 3 zeigt beide Fälle.

4 Nutzung des *A-NetBeacon*

Die Auslöser zur Nutzung des *A-NetBeacon* sind Abweichungen des Erwartungswertes von ExN (durch Störungsmeldungen) oder geplante Änderungen in VxN oder PxD

Daraufhin entwickelt der Administrator der Besitzerdomäne eine Diagnosestrategie (für Störungen) bzw. eine Überprüfungsstrategie (für Änderungen). Dazu gehören die zu überprüfenden VLANs (inkl. IP-Adressbereichen) und die dazu gehörenden Dosen zur Prüfung von VxP. PxD kann als korrekt angenommen werden, wenn es dem Erwartungswert von ExN entsprechend konfiguriert sein sollte.

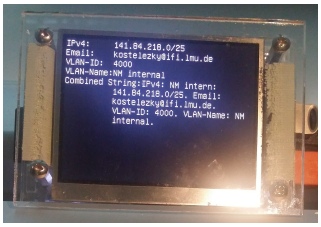
Anschließend wählt der Administrator der Besitzerdomäne eine oder mehrere Platzierungen für den Sender des *A-NetBeacon* mit entsprechenden Parametern, so dass die Überprüfung bzw. die Diagnose unterstützt wird.

Aus der Diagnose-/Überprüfungsstrategie ergeben sich die zu erwartenden empfangbare *A-NetBeacon* an Endgerät E und lässt wiederum einen entsprechenden Ergebnisschluss zu.

[2] Die Implementierung steht quelloffen zur Verfügung: `https://github.com/mnm-team/LANbeacon`

```
08:07:48.380203 b8:27:eb:0d:b2:0e (oui Unknown) > Broadcast, ethertype Unknown (0x88b5),
 length 255:
        0x0000:  0207 04b8 27eb 0db2 0e04 0703 b827 eb0d  ....'........'..
        0x0010:  b20e 0602 0014 fe18 cc4d 55cb 0a99 3300  .........MU...3.
        0x0020:  180a 9907 8019 81bb d600 1881 bbe4 0018  ................
        0x0030:  fe12 cc4d 55cd 7262 6740 6966 692e 6c6d  ...MU.rbg@ifi.lm
        0x0040:  752e 6465 fe06 cc4d 55c8 03ca fe0c cc4d  u.de...MU......M
        0x0050:  55c9 4946 4920 4e65 747a fe93 cc4d 55d9  U.IFI.Netz...MU.
        0x0060:  4950 7634 3a20 4946 4920 4e65 747a 3a20  IPv4:.IFI.Netz:.
        0x0070:  3130 2e31 3533 2e35 312e 302f 3234 2c20  10.153.51.0/24,.
        0x0080:  3130 2e31 3533 2e37 2e31 3238 2f32 352c  10.153.7.128/25,
        0x0090:  2031 3239 2e31 3837 2e32 3134 2e30 2f32  .129.187.214.0/2
        0x00a0:  342c 2031 3239 2e31 3837 2e32 3238 2e30  4,.129.187.228.0
        0x00b0:  2f32 342e 2045 6d61 696c 3a20 7262 6740  /24..Email:.rbg@
        0x00c0:  6966 692e 6c6d 752e 6465 2e20 564c 414e  ifi.lmu.de..VLAN
        0x00d0:  2d49 443a 2039 3730 2e20 564c 414e 2d4e  -ID:.970..VLAN-N
        0x00e0:  616d 653a 2049 4649 204e 6574 7a2e 2000  ame:.IFI.Netz...
        0x00f0:  00                                       .
```

(a) Informationsanzeige mittels tcpdump



(b) Prototyp auf Kleinstrechner im Einsatz

Abb. 3: *A-NetBeacon* im Einsatz

5 Evaluation in der Praxis

Zur Bewertung der Einsatzfähigkeit wird *A-NetBeacon* in Produktivnetzen am Institut für Informatik der LMU erprobt. Abb. 4 illustriert diesen Einsatz in realen Besitzerdomänen sowie in virtualisierter Laborinfrastruktur.

Einsatz 1: Eine Besitzerdomäne.
Im Fall (siehe (1) in Abb. 4), der die Konzeption dieser Arbeit ausgelöst hat, soll ein Administrator in Besitzerrolle die korrekte Konfiguration durch den ISP testen und überprüfen. Die *A-NetBeacon*-Serveranwendung wird auf einem unter der Kontrolle des Administrators stehenden Server mit einer Schnittstelle in allen VLANs der Domäne betrieben und anschließend an allen im VLAN zugänglichen Dosen empfangen werden.

Anekdote aus dem Alltag eines Sysadmins:
Im Regelfall sind alle genutzten TP-Zimmerdosen mit der dahinterliegenden VLAN-Konfiguration in für den Mitarbeiter „übersetzter Form“ beschriftet, z.B *Laptop*. Für die Bereitstellung eines weiteren Anschlusses für einen Laptop an einer unbeschrifteten Dose wird zur Prüfung der aktuellen Konfiguration der tragbare Kleinstrechner mit dem *A-NetBeacon*-Client angeschlossen und festgestellt, dass die Dose zwar gepatched aber in ein fremdes VLAN eingebunden wurde. Dadurch konnte eine explizite Serviceanfrage an den ISP gestellt werden, wohingegen ohne das *A-NetBeacon* im Falle einer korrekten Konfiguration unnötige Arbeit verursacht worden wäre.

Einsatz 2: Überlappende Besitzerdomänen.
Neben der Verwendung in der „eigenen“ Domäne ist in manchen Szenarien auch eine Kooperation mehrerer Besitzer nötig, beispielsweise wenn Netze von Besitzern verschiedener Domänen geteilt werden. Dieser Anwendungsfall wurde am Beispiel des Institutsnetzes der Informatik der LMU München erprobt (siehe (2) in Abb. 4). Dabei wurde die Serveranwendung des *A-NetBeacon* auf einem am sogenannten „IFI Multinet“ angeschlossenen Geräten gestartet und konnte dann domänenübergreifend empfangen werden.

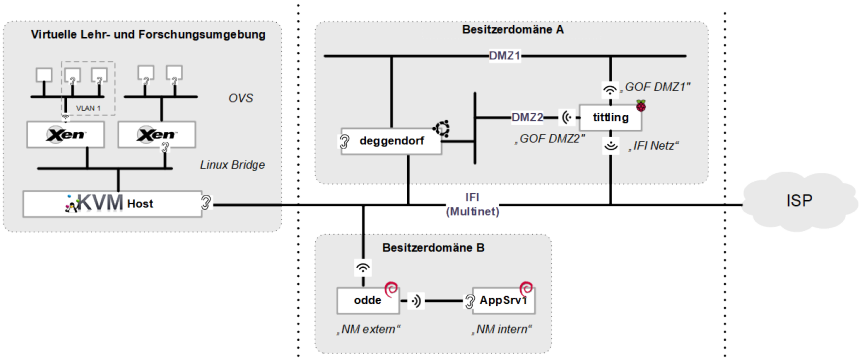


Abb. 4: *A-NetBeacon* in unterschiedlichen Besitzerdomänen

Einsatz 3: In der Rolle eines Netzbetreibers.
Zur Untersuchung der Eignung für den ISP-seitigen Einsatz agiert der Besitzer der Domäne A im dritten Szenario (siehe (3) in Abb. 4) als ISP für ein in sich geschlossenes Lehr- und Forschungsnetz und sendet *A-NetBeacon*-Nachrichten, die von allen an der virtuellen Infrastruktur angeschlossenen Geräten empfangen werden.

Einsatz 4: Virtuelle Netzkomponenten.
Aufbauend auf Szenario 3 wurde das Beacon auch in einem virtuellen Netz innerhalb einer geschichteten Labor- und Lehrinfrastruktur [DGK] getestet, um Einschränkungen an virtuellen Netzkomponenten ausschließen zu können. Dabei konnten *A-NetBeacon*-Nachrichten über die virtuellen Switches (als Linux Bridges und OpenVSwitch, konfiguriert mit tagged, untagged und ohne VLAN-ID) verteilt und empfangen werden. Lediglich beim Zusammenspiel von getaggten und ungetaggten VLANs innerhalb einer Infrastruktur kam zu Duplizierung der Rahmen auf Grund der Broadcast-Implementierung von OpenVSwitch.

Die Nutzung des Protokolls hat in den bisherigen Versuchen Besitzer und Netzbetreiber entlastet, indem die Prüfung korrekter Anschlüsse Serviceanfragen vermeidet. Für Laborinfrastruktur kann der Besitzer in ISP-Rolle gegenüber z.B. Praktikumsbetreuern mittels des Protokolls die Netze und Konfigurationsoptionen bekannt geben und Rückfragen vermeiden. Ein Einsatz in größerem Rahmen wird derzeit geprüft.

6 Themenverwandte Arbeiten

Das durch *A-NetBeacon* angesprochene Problem kann in den Bereich der Topologieerkennung bzw. *Topology Discovery* eingeordnet werden. Hassan Gobjuka [Go10] stellt einen Algorithmus zur Ermittlung der Netztopologie heterogener Netze vor. Er beschreibt die Ermittlung in VLAN als deutlich komplexer als in physischen Netzen (LAN) und bezeichnet sie als *NP-hart*. Andere Arbeiten (exemplarisch: [BDF04; Br00]) beschreiben Topologieerkennung in lokalen Netzen und Ermittlung der genutzten IP-Netze im Rahmen

von *Network Discovery*. Schichtübergreifende Erkennung ist durch datenbankgestützte aktive Verfahren möglich [LOG01] z.B. gestützt auf Inhalte der *Management Information Base* (MIB [IE09]) von SNMP-Agenten, aber auch Ansätze, die den Spannbaum [St02] bzw. die *Forwarding Tables* [SWS05] zur Topologieermittlung.

Diese Verfahren untersuchen die Gesamttopologie des Netzes, erfordern Zeit und stehen bei der Konfigurationsaktivität, wie sie im Szenario besprochen wird, nicht unmittelbar zur Verfügung. Häufig eingesetzte Techniken zur Überprüfung eines korrekten Anschlusses nutzen „Bordmittel“ der Netzdiagnose (*ping, traceroute, portscan*, etc.). Das an einer Dose angeschlossene VLAN ist bei *tagged* Rahmen anhand der VLAN-ID im 802.1Q Header möglich, sollte der Verkehr im Zugangsnetz in solchen Rahmen transportiert werden.

Das in dieser Arbeit vorgestellte *A-NetBeacon*-Protokoll schließt diese Lücke, indem es ein Informationssystem für die Besitzerdomäne bereitstellt. Bereits vorhandene Funktionen der Netzkomponenten, vor allem *Link Layer Discovery Protocol* (LLDP) 802.1 AB [IE15] und seine herstellerspezifischen Varianten (Cisco CDP, Microsoft LLTP) könnten trotz ihres Fokus auf automatische Erkennung zwischen Geräten eingesetzt werden, erfordern jedoch administrativen Zugriff auf alle betroffenen Netzkomponenten.

7 Zusammenfassung und Ausblick

Die Erstellung eines korrekten Anschlusses eines Endgerätes im Zugangsnetz kann durch Selbstbeschreibung mit dem vorgestellten *A-NetBeacon*-Protokolls auch ohne die Erfordernis administrativer Rechte im Zugangsnetz unterstützt werden. Seine Erprobung in der Praxis weist es als Hilfestellung des realen Betriebs aus.

Unser Problemmodell weist aber auch Fälle auf, die nur mittelbar durch Einsatz des Protokolls analysiert werden können und somit Kandidaten für weitere Untersuchungen darstellen. Darüber hinaus sind Weiterentwicklungen basierend auf der Selbsbstbeschreibungsfunktion denkbar, etwa der Abgleich der Konfiguration von Managementdiensten (z.B. DHCP, Intrusion Detection, Paketfilter). Die Integration des Protokolls in die Software der Netzkomponenten würde die Überprüfung der Selbstbeschreibungsdaten erlauben. Solche Entwicklungen könnten die Haltung von Managementdaten konsolidieren und möglicherweise Ansätze für die zusammengesetzten Fälle des Problemmodells erlauben.

Danksagung
Die Autoren bedanken sich herzlich bei Herrn BSc Bitzer, der leider an der Erstellung dieses Papiers nicht teilnehmen konnte. Im Rahmen seiner Bachelorarbeit [Bi17] arbeitete er an der Konzeption des Protokolls mit und entwickelte den Prototypen, der bei unseren Versuchen eingesetzt wurde.

Literatur

[BDF04] Black, R.; Donnelly, A.; Fournet, C.: Ethernet topology discovery without network assistance. In: Proceedings of the 12th IEEE International Conference on Network Protocols, 2004. ICNP 2004. S. 328–339, Okt. 2004.

[Bi17] Bitzer, D.: LAN-Beacon: Ein Protokoll zur authentifizierten Selbstbeschreibung lokaler Netze, Ludwig-Maximians-Universität München, Juni 2017.

[Br00] Breitbart, Y.; Garofalakis, M.; Martin, C.; Rastogi, R.; Seshadri, S.; Silberschatz, A.: Topology discovery in heterogeneous IP networks. In: Proceedings IEEE INFOCOM 2000. Conference on Computer Communications. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (Cat. No.00CH37064). Bd. 1, 265–274 vol.1, 2000.

[DGK] Danciu, V.; Guggemos, T.; Kranzlmüller, D.: Schichtung virtueller Maschinen zu Labor- und Lehrinfrastruktur. In: 9. DFN Forum Kommunikationstechnologien. Bd. 2016. GI–Edition Lecture Notes in Informatics, Rostock Deutschland.

[Go10] Gobjuka, H.: Topology Discovery for Virtual Local Area Networks. In: 2010 Proceedings IEEE INFOCOM. S. 1–5, März 2010.

[IE09] IEEE: IEEE Standard for Local and metropolitan area networks- Virtual Bridged Local Area Networks Amendment 8: Management Information Base (MIB) Definitions for VLAN Bridges. IEEE Std 802.1ap-2008 (Amendment to IEEE Std 802.1Q-2005)/, S. c1–323, März 2009.

[IE15] IEEE: IEEE Standard for Local and metropolitan area networks– Station and Media Access Control Connectivity Discovery Corrigendum 2: Technical and Editorial Corrections. IEEE Std 802.1AB-2009/Cor 2-2015 (Corrigendum to IEEE Std 802.1AB-2009)/, S. 1–68, März 2015.

[LOG01] Lowekamp, B.; O'Hallaron, D.; Gross, T.: Topology Discovery for Large Ethernet Networks. In: Proceedings of the 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications. SIGCOMM '01, ACM, San Diego, California, USA, S. 237–248, 2001, ISBN: 1-58113-411-8.

[St02] Stott, D. T.: Layer-2 path discovery using spanning tree MIBs. Avaya Labs Research, Avaya Inc 233/, 2002.

[SWS05] Sun, Y.; Wu, Z.; Shi, Z.: The physical topology discovery for switched Ethernet based on connections reasoning technique. In: IEEE International Symposium on Communications and Information Technology, 2005. ISCIT 2005. Bd. 1, S. 44–47, Okt. 2005.