

Link Layer Discovery Protocol (LLDP, IEEE 802.1AB)

Das Link Layer Discovery Protocol (englisch für Verbindungsentdeckungsprotokoll, kurz LLDP) ist ein herstellernerutrales Protokoll des Link Layers (Layer 2) womit ein an einem Ethernet Link angeschlossenes Gerät seine Identität und Eigenschaften mitteilen kann. Diese Informationen werden in der Management Information Base (MIB) abgelegt und mit dem Simple Network Management Protokoll (SNMP) eingesammelt. Bei PROFINET IO werden diese Funktionen verwendet, um die Topologie eines Netzwerkes festzustellen.

Inhaltsverzeichnis

1	Beschreibung	1
1.1	Geschichte	1
1.2	Struktur der IEEE 802.1AB	1
1.3	Wer sind meine Nachbarn?	2
1.3.1	TLV-Blöcke für das Management	3
1.3.2	Organisationsspezifische TLV-Blöcke	4
1.4	Die LLDP MIB	4
1.4.1	Variablen der LLDP MIB	5
1.5	Die Management-Software	6
2	Ethereal	6
2.1	Display Filter	6
2.2	Capture Filter	6
3	Quellen und Literatur	7

1 Beschreibung

1.1 Geschichte

Durch die Ermittlung, Darstellung und Überwachung der physikalischen Verbindungen zwischen den Geräten eines PROFINET IO Systems mit einer einzigen Software kann der Administrator auch komplexe Netze leichter überwachen und warten. Frühere Ansätze zur Topologie-Erkennung interpretierten entweder die gelernten MAC-Adressen in den Forwarding-Daten (FDB – Forwarding Database) oder werteten die Standard-MIBs (Management Information Base) aus, z.B. Bridge MIBs. Diese Ansätze waren jedoch aufwändig und die Ergebnisse unbefriedigend. Andere Verfahren, wie das „Cisco Discovery Protocol“ (CDP), wurden von nur wenigen Herstellern übernommen. Beim IEEE wurden die Aktivitäten energisch vorangetrieben, und es erfolgte im Mai 2005 die Verabschiedung des Standards IEEE 802.1AB, der sowohl das „Link Layer Discovery Protocol“ (LLDP) als auch die zugehörige „LLDP MIB“ beschreibt. LLDP ist eine Weiterentwicklung des CDP, jedoch mit diesem nicht kompatibel.

1.2 Struktur der IEEE 802.1AB

Der Standard IEEE 802.1AB beschreibt eine Management Information Base (MIB), das Protokoll für den Datenaustausch und den Aufbau der MIB. Die LLDP MIB speichert die Daten über den lokalen Agenten und die erkannten Nachbar-Agenten und ermöglicht die Konfiguration des LLDP. Das LLDP versendet LLDP-Pakete, so genannte LLDP DUs (Data Units), an alle physikalischen Schnittstellen eines Gerätes und baut die lokale LLDP MIB mit den Daten aus den empfangenen Paketen auf.

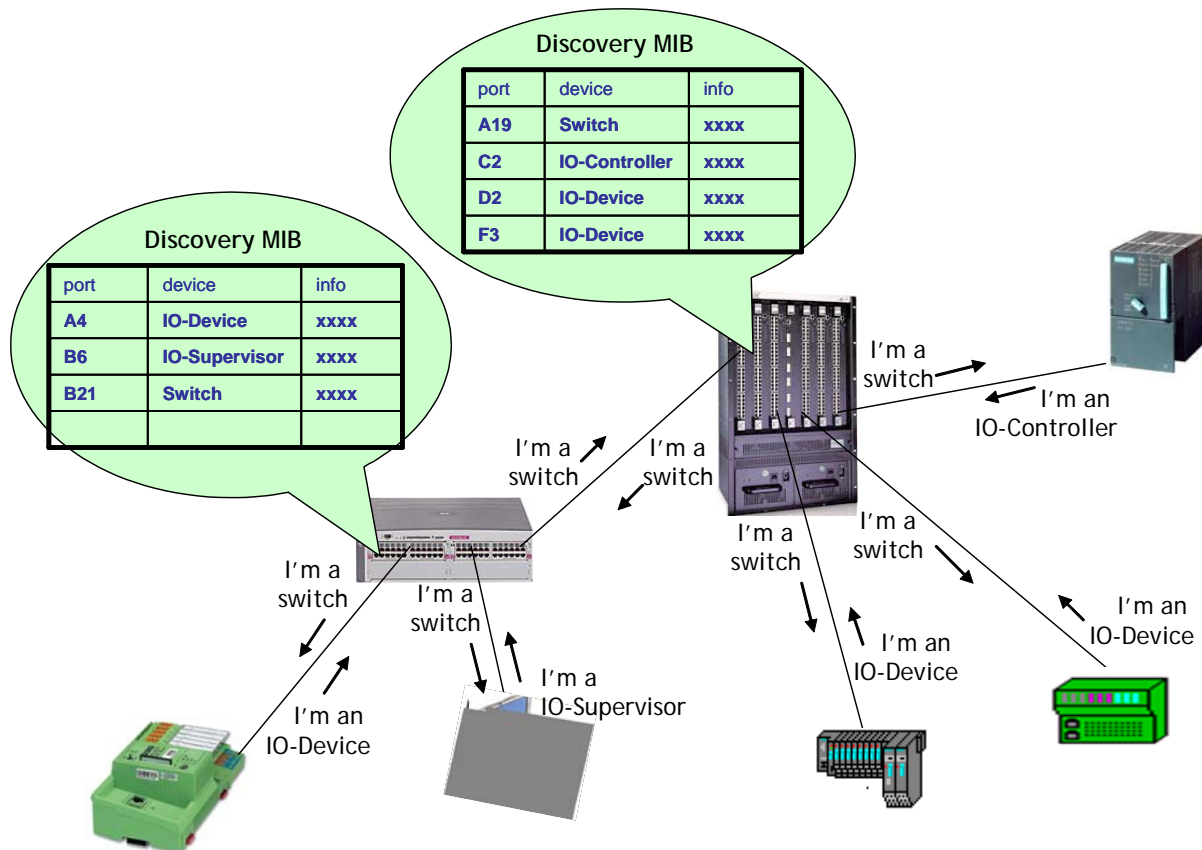


Abbildung 1 Beim Link Layer Discovery Protokoll (LLDP) tauschen die Geräte im PROFNET IO System zunächst untereinander LLDP-Pakete aus. Jedes Gerät speichert die empfangenen Informationen in seiner Nachbartabelle. Die Inhalte der Nachbartabellen werden von der Netzmanagement-Station ausgelesen, die daraus eine Topologie-Darstellung generiert.

Das Konzept beruht darauf, dass jeder Verbindungspunkt in der Topologie als „Media Service Access Point“ (MSAP) eindeutig identifiziert ist. Jeder MSAP darf in der beobachteten Netzwerk-Topologie nur einmal vorkommen, nur so kann das „Network Management System“ die Topologie eindeutig ermitteln. Ein MSAP setzt sich zusammen aus einer eindeutigen Gerätekenung (Chassis ID) und einer mindestens für dieses Gerät eindeutigen Portkennung (Port ID).

1.3 Wer sind meine Nachbarn?

LLDP ist ein Protokoll, das die Erkennung des nächsten Nachbarn ermöglicht. Es versetzt ein Gerät im Netzwerk in die Lage, Informationen über sich selbst zu versenden und von seinen Nachbargeräten empfangene Informationen in der LLDP MIB zu speichern. Diese Informationen können von einer Netzwerk-Management-Station (NMS) über das SNMP (Simple Network Management Protocol) abgefragt werden. Das LLDP stellt nur die Basis für die Anwendungen zur Verfügung, die auf der Ebene der NMS zu realisieren sind. Das heißt, dass sich die „Intelligenz“ in der Anwendungssoftware auf der NMS befindet und nicht in den verteilten LLDP-Agenten. Der Standard IEEE 802.1AB macht hierzu keine Vorgaben, er beschreibt lediglich das Protokoll und die MIB auf der Agenten-Ebene.

Das LLDP ist ein einfaches „Einweg-Protokoll“, das in periodischen Intervallen – in der Grundeinstellung alle 30 Sekunden – an den Ports des Netzwerk-Gerätes Pakete mit Informationen über sich selbst aussendet und an diesen Ports auf den Empfang solcher LLDP-Pakete wartet. Sende- und Empfangsteil arbeiten dabei unabhängig voneinander, d.h., für ausgesendete LLDP DUs wird keine Antwort oder Bestätigung des Empfängers erwartet. Die LLDP DUs sind Datenpakete ohne „Tag“ (Kennzeichnung) auf der Sicherungsschicht (Schicht 2) mit dem Ethertype 0x88CC, die an die Zieladresse 01:80:C2:00:00:0E geschickt werden. Da es sich bei dieser Zieladresse um eine „IEEE Multicast MAC“-Adresse (Media Access Control) handelt, wird diese von IEEE-802-konformen Switches nicht weitervermittelt, d.h., das Datenpaket erreicht in der Regel nur den an einem Port angeschlossenen direkten Nachbarn.

LLDP DUs werden auch über Verbindungen gesendet, über die sonst kein Paketverkehr stattfindet, also z.B. geblockte Spanning Tree Ports, oder solche, die administrativ auf „down“ geschaltet wurden. Dadurch können mit LLDP auch „inaktive“ Verbindungen ermittelt werden; was für ein vollständiges Abbild der Netzwerk-Topologie erforderlich ist. Der Standard IEEE 802.1AB definiert einen Satz von Informationsblöcken, die jeweils in einem „Type Length Value“-Format (TLV) codiert werden. Eine LLDP DU besteht aus solchen aneinander gehängten TLV-Blöcken. Jede LLDP DU muss mit einem „End of LLDP DU TLV“ abgeschlossen werden.

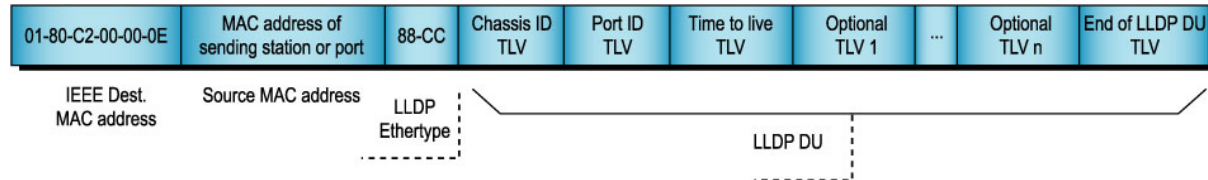


Abbildung 2 Aufbau eines LLDP-Paketes bzw. Data Unit (LLDP DU) mit Ethernet Header.

Der Standard IEEE 802.1AB erlaubt die Definition von organisations- und herstellerspezifischen TLV-Blöcken, er ist dadurch erweiterungsfähig. Dabei machen neue TLV-Blöcke auch die Definition eines zugehörigen neuen Moduls für die LLDP MIB erforderlich, das dann im „lldpExtensions“-Zweig eingehängt wird. Empfängt ein LLDP-fähiges Gerät – ein LLDP-Agent – eine LLDP DU, werden die Inhalte der TLV-Blöcke decodiert und für eine gewisse Zeit abgespeichert. Diese Inhalte können per SNMP-Zugriff auf die entsprechenden Variablen der LLDP MIB abgerufen werden. Grundsätzlich ist es dem sendenden Gerät überlassen, welche TLV-Blöcke es in seine ausgehenden LLDP DU einfügt. Das LLDP schreibt lediglich für einen minimalen Funktionsumfang die drei folgenden TLV-Blöcke vor, die stets und in dieser Reihenfolge am Anfang einer gültigen LLDP DU vorkommen müssen:

- Chassis ID TLV (Type = 1)
- Port ID TLV (Type = 2)
- Time To Live TLV (Type = 3)
- End of LLDPDU TLV (Type = 0)

Optional sind die folgenden TLVs definiert:

- Port Description TLV (Type = 4)
- System Name TLV (Type = 5)
- System Description TLV (Type = 6)
- System Capabilities TLV (Type = 7)
- Management Address TLV (Type = 8)

Die Übermittlung dieser Parameter ist die Minimalvoraussetzung für die Erkennung der Topologie mit LLDP. Die im Netzwerk eindeutige Chassis-ID, etwa die MAC-Adresse des sendenden Geräts, und die für das betreffende Gerät eindeutige Port-ID, z.B. die Port-Nummer des sendenden Ports, bieten eine eindeutige Identifikation des Verbindungspunktes in der Topologie. Dieser Verbindungspunkt wird auch „Media Service Access Point“ (MSAP) genannt. Die Abbildung der Verbindung auf der Bitübertragungsschicht zu dem lokalen MSAP – dort, wo diese LLDP DU empfangen wird – wird auf Basis dieser Daten in der NMS erstellt.

Der „Time To Live“-Wert signalisiert dabei dem empfangenden Gerät, wie lange die erhaltene Information gültig sein soll. Läuft diese Zeitspanne ab und wurde die LLDP DU nicht erneut empfangen, so wird diese Verbindung aus der Tabelle („remTable“) der lokalen LLDP MIB ausgetragen. Wird eine LLDP DU mit einem „Time To Live“-Wert „0“ empfangen, dann wird die zugehörige Verbindung sofort aus der Tabelle ausgetragen. Auf diese Weise kann sich ein LLDP-Agent bei seinen Nachbarn kontrolliert „abmelden“.

1.3.1 TLV-Blöcke für das Management

Die Parameter des „Basic Management“-TLV-Blocks heißen „Port Description“, „System Name“, „System Description“, „System Capabilities“ und „Management Address“. Sie erleichtern die Aufgabe der Darstellung der Netzwerk-Topologie. Mit dem „Port Description“-TLV-Block, dem „System Name“-TLV-Block und dem „System Description“-TLV-Block lassen sich den eher kryptisch codierten Chassis-IDs und Port-IDs als Klartext lesbare Beschreibungen zuordnen. „Port Description“ enthält in der Regel den Wert von „ifDescr“ (RFC 2863), „System Name“ den Wert von „sysName“ (RFC 3418)

und „System Description“ den Wert von „sysDescr“ (RFC 3148), falls diese MIB von dem betreffenden Gerät unterstützt werden.

Mit dem „System Capabilities“-TLV-Block kann die Gerätekategorie übermittelt werden, also ob es sich um einen Repeater, einen Switch, einen Router, einen WLAN Access Point, ein Telefon oder ein sonstiges Endgerät handelt. So kann das Gerät in einer Topologie-Darstellung eindeutig abgebildet werden. Mit den „Management Address“-TLV-Blöcken können die Management-Adressen übermittelt werden, über die das Gerät erreichbar ist. Damit lässt sich die Topologie der Verbindungsschicht des Netzwerks ermitteln, darüber hinaus kann sich die NMS auf Basis der ermittelten Management-IP-Adressen von Agent zu Agent in der Topologie „vorarbeiten“ und Inhalte der LLDP MIBs auslesen.

1.3.2 Organisationsspezifische TLV-Blöcke

Die organisationsspezifischen TLV-Blöcke des Standards IEEE 802.1 lauten „Port VLAN ID“, „Port&Protocol VLAN ID“, „VLAN name“ und „Protocol Identity“. Mit diesen Parametern können die unterschiedlichen Topologien der Sicherungsschicht ermittelt werden, wie die VLAN-Topologie oder die „Spanning Tree“-Topologie. Eine „intelligente“ NMS kann darüber Fehlkonfigurationen zwischen Geräten erkennen, z.B. falsch konfigurierte VLANs oder inkompatible Redundanz-Protokolle an miteinander verbundenen Ports.

Zu den organisationsspezifischen TLV-Blöcken des IEEE 802.3 zählen Konfiguration und Status des MAC, die „Power via MDI“-Einrichtung (Power via Media Dependent Interface), die „Link Aggregation“ und die maximale Größe der Frames. Diese Parameter dienen hauptsächlich der Fehlererkennung auf der Bitübertragungsschicht. Es lassen sich hiermit inkompatible Port-Konfigurationen auffinden; hierzu zählen Datenübertragungsrate, Duplex-Fähigkeit, Autonegotiation, Link Aggregation und die maximale Paketlänge.

□ Organizationally Specific TLV (Type = 127)

Das Längenfeld des Organizationally Specific TLV wird gefolgt von einem 3 Byte (24 bit) langen Organizationally Unique Identifier (OUI) gefolgt von einem 1 Byte langen Untertyp.

Die folgenden Werte sind dabei schon bekannt:

OUI	Organisation	Subtyp	Bedeutung
00-80-C2	IEEE 802.1	1	Port VLAN ID TLV
		2	Port And Protocol VLAN ID TLV
		3	VLAN Name TLV
		4	Protocol Identity
00-12-0F	IEEE 802.3		
00-12-BB	TIA TR-41 Committee Media Endpoint Discovery (LLDP-MED)	1	MAC/PHY Configuration/Status TLV
		2	Power Via MDI TLV
		3	Link Aggregation TLV
		4	Maximum Frame Size TLV

1.4 Die LLDP MIB

Die LLDP MIB ist die Schnittstelle zwischen dem LLDP-Agent und dem NMS. Sie besteht aus zwei verschiedenen MIB-Modulen: der Basis-MIB und den organisationsspezifischen Erweiterungs-MIBs. Die IEEE 802.1AB schreibt die MIB-Implementierung in einem LLDP-Agenten nicht zwingend vor. Das kann z.B. bei Endgeräten der Fall sein, auf die das Management-System nicht zugreifen kann; für diese reicht meist ein einfacher LLDP-Sendemechanismus aus. Bei PCs wiederum ist die Implementierung des Empfangsmechanismus sinnvoll, weil der Benutzer oder der Servicetechniker damit auf einfache Weise herausfinden kann, wo der betreffende PC in der LAN-Topologie angeschlossen ist. Um die Topologie-Erkennung mit Switchen und Routern realisieren zu können, muss dort die LLDP MIB für den Sende- und den Empfangszweig implementiert sein. Eingehängt ist die LLDP MIB im Zweig „iso std(0)/iso8802(8802)/ieee802 dot1(1)/ieee802dot1mibs(1)“.

1.4.1 Variablen der LLDP MIB

Die Variable „lldpRemoteSystemsData“ ist die wichtigste in der LLDP MIB, da hier die empfangenen Nachbarinformationen abrufbar sind (Bild 5). Der erste Index „lldpRemTimeMark“ ist ein Zeitstempel, an dem abgelesen werden kann, wann der Nachbareintrag angelegt wurde. Der zweite Index „lldpRemLocalPortNum“ gibt Auskunft, an welchem lokalen Port die LLDP DU vom Nachbarn empfangen wurde, der dritte Index „remIndex“ sagt aus, um den wievielten Nachbareintrag an diesem lokalen Port es sich handelt, falls mehrere Nachbargeräte über einen Repeater (Hub) an diesem Port angeschlossen sind. Dieses Schema wiederholt sich in allen Nachbartabellen der LLDP MIB. Die Variablen „lldpRem-ChassisId“ und „lldpRemPortId“ enthalten die empfangenen Werte der Gegenseite und kennzeichnen deren MSAP, also einen eindeutigen Punkt in der Topologie. Zusammen mit dem lokalen MSAP, der aus der „lldpLocalChassisId“ und der „lldpLocalPortId“ des Ports in „lldpRemLocalPortNum“ besteht, bildet der benachbarte MSAP eine Verbindungslinie in der Topologie.

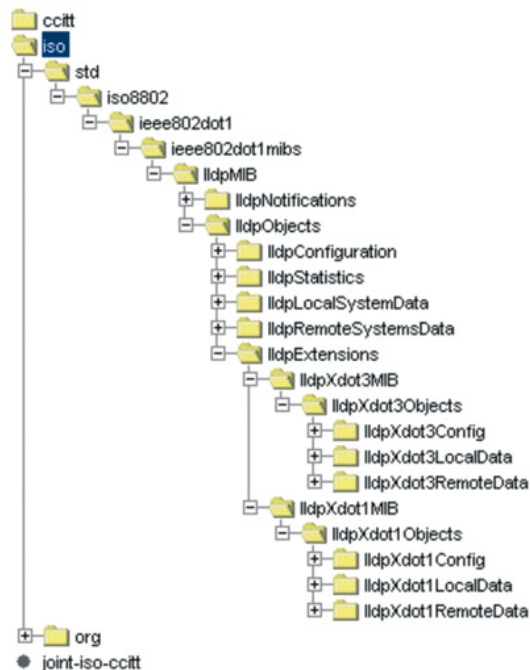


Abbildung 3 Die LLDP MIB (IldpMIB) in der Baumstruktur des Protokolls. Die wichtigsten Untergruppen sind „lldpRemoteSystemsData“, „lldpLocalSystemData“, „lldpConfiguration“ und „lldpStatistics“.

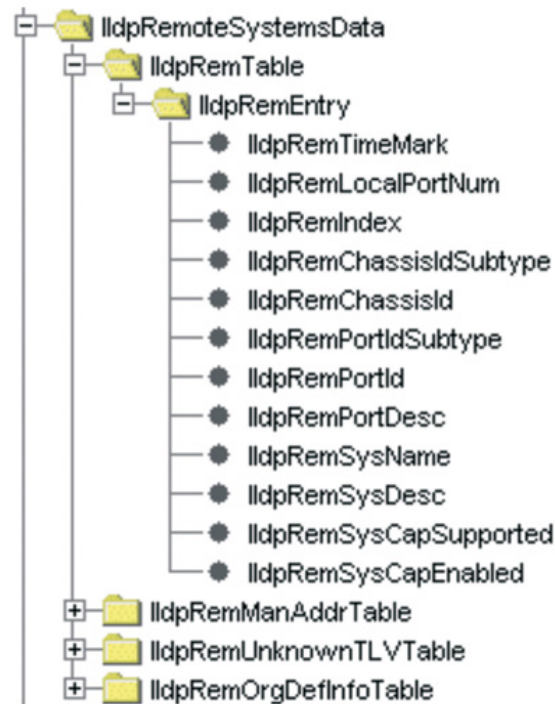


Abbildung 4 Die Untergruppe „IldpRemoteSystemsData“ enthält die empfangenen Nachbarinformationen; auf diese Daten greift das NMS zu, um die Topologie zu erstellen.

Die Variable „IldpConfiguration“ stellt globale und portabhängige Konfigurationsmöglichkeiten für den lokalen LLDP-Agenten zur Verfügung. „IldpStatistics“ enthält Statistik- und Fehlerzähler für die Sende- und die Empfangsrichtung. „IldpLocalSystemData“ enthält alle lokalen Daten, welche auch in den LLDP DUs an die Nachbarn versendet werden. „IldpExtensions“ enthält die organisationsspezifischen Erweiterungs-MIBs, falls diese auf dem betreffenden Gerät implementiert sind. Jede dieser Erweiterungs-MIBs hat grundsätzlich wiederum die bereits bekannte Struktur der Basis-MIB.

1.5 Die Management-Software

Zur umfassenden Ermittlung der Netzwerk-Topologie muss eine Netzwerk-Management-Station (NMS) diese Daten aus den LLDP MIBs aller Geräte in ihrem Erfassungsbereich abfragen und sammeln. Anschließend kann auf Basis dieser Daten die Topologie ermittelt, aufbereitet und grafisch dargestellt werden. Zudem lassen sich Daten auf Plausibilität überprüfen und so Fehlkonfigurationen ermitteln. Für die Darstellung eines Ausschnitts aus dem gesamten Netzwerk reicht es aus, nur die diesen Ausschnitt betreffenden Daten aus den Geräten auszulesen.

Beim Einlesen einer unbekanntenen Topologie muss die NMS bei einem beliebigen, bekannten LLDP-Agenten beginnen (z.B. bei sich selber, Voraussetzung hierfür ist ein LLDP-fähiger NMS-PC) und sich anhand der dort gewonnenen Nachbardaten sukzessive weiterarbeiten. Auf der NMS müssen hierzu geeignete Algorithmen implementiert werden, damit dieses Vorgehen auch in großen Netzen möglichst effizient und zielgerichtet erfolgt. Die Anwendung von LLDP setzt immer voraus, dass eine entsprechende Netzmanagement-Software vorhanden ist.

2 Ethereal

Das LLDP wird ab Ethereal Version 0.10.13 unterstützt.

2.1 Display Filter

Um nur LLDP Pakete darzustellen kann der Filter **lldp** verwendet werden.

2.2 Capture Filter

Um nur LLDP Pakete aufzuzeichnen kann der Filter **ether proto 0x88cc** verwendet werden.

3 Quellen und Literatur

Diese Kurzbeschreibung wurde zusammengestellt unter der Verwendung der folgenden Unterlagen:

[LLDP 1] Markus Rentschler: **Die Entdeckung der Netzwerk-Topologie**, Elektronik 24/2005; <http://www.elektroniknet.de/topics/kommunikation/fachthemen/2006/0001/index.htm> (Stand 4.2006)

Die LLDP Norm kann kostenlos heruntergeladen werden von:

[LLDP 2] IEEE Std 802.1AB-2005: **IEEE Standard for Local and metropolitan area networks Station and Media Access Control Connectivity Discovery**, <http://standards.ieee.org/getieee802/download/802.1AB-2005.pdf>

Einen „shareware“ LLDP Agent für Windows findet man hier:

<http://www.hanewin.de/lldp-e.htm>