

OCIT[®]

Open Communication Interface for Road Traffic Control Systems

Offene Schnittstellen für die Straßenverkehrstechnik

OCIT-Outstations Profil 3 – Ethernet mit DHCP

OCIT-O-Profil_3_V1.0_A01

OCIT Developer Group (ODG)

OCIT[®] ist eine registrierte Marke der Firmen Dambach, Siemens, Signalbau Huber, STOYE und Stührenberg

OCIT-Outstations

Profil 3 – Ethernet mit DHCP

Dokument: OCIT-O-Profil_3_V1.0_A01

Herausgeber: OCIT Developer Group (ODG)

Kontakt: www.ocit.org

Copyright © 2009 ODG. Änderungen vorbehalten. Dokumente mit Versions- oder Ausgabestände neueren Datums ersetzen alle Inhalte vorhergehender Versionen.

Inhaltsverzeichnis

Spezifikationen.....	4
Referenzierte Standards	5
1 Einführung.....	6
2 Übertragungsprofil (Profil 3).....	6
2.1 Einsatzmerkmale.....	6
3 Festlegungen zum Profil 3.....	8
3.1 Einsatz von DHCP.....	8
3.2 Anforderungen an die Zentrale.....	8
3.2.1 Per DHCP übermittelte Informationen.....	8
3.2.2 Interaktion von mehreren DHCP-Servern.....	10
3.2.3 Zentraler Systemzugang	10
3.3 Anforderung an das Feldgerät	11
3.3.1 Ethernetinterface.....	11
3.3.2 DHCP.....	11
3.3.3 Anforderungen an Zentrale und Feldgerät.....	13
4 Anforderung an das Kundennetz.....	14
4.1 Ethernetinterface der Fernleitung zur Anbindung des Feldgerätes.....	14
4.2 Transparenz der Übertragungsstrecke	14
4.3 Geswitchter Betrieb.....	15
4.4 Gerouteter Betrieb.....	15
4.4.1 Einstellungen des Routings.....	16
4.4.2 Einsatz eines DHCP Relay	17
4.4.3 Benötigte Dienste zwischen Zentrale und Feldgerät	18
Glossar	21

Dokumentenstand

Version Ausgabe	Verteiler- kreis	Datum	Kommentar
V 1.0 A01	PUBLIC	11.08.09	Neues Dokument

Spezifikationen

Das **OCIT-Outstations Konfigurationsdokument OCIT-O KD Vx.x** enthält eine Übersicht über alle von der ODG urheberrechtlich verwalteten Spezifikationen und ordnet Versionen und Ausgabestände nach:

- zusammengehörenden Spezifikationen der Schnittstelle „OCIT-Outstations für Lichtsignalsteuergeräte“ mit Referenz auf die dazugehörigen OCIT-Instations Spezifikationen,
- gibt Hinweise zum Einsatz der Übertragungsprofile und
- enthält eine Übersicht über Pakete von Spezifikationen für Schnittstellen, für deren Nutzung von der ODG eine Schutzgebühr verlangt wird

Der jeweils aktuelle Stand ist auf www.ocit.org veröffentlicht.

Referenzierte Standards

Standard	Organisation	Titel / Erklärung
RFC 2131	IETF	Dynamic Host Configuration Protocol DHCP (März 1997)
RFC 2132	IETF	DHCP Options and BOOTP vendor extensions (März 1997)
RFC 3942	IETF	Reclassifying Dynamic Host Configuration Protocol version 4 (DHCPv4) Options (Nov 2004)
RFC 3046	IETF	DHCP Relay Agent Information Option (Januar 2001)
10BaseT	IEEE	Ethernet mit 10 Mbit/s auf zwei Paaren UTP-Kabeln, Bestandteil von IEEE 802.3, max. 100m
100BaseTX	IEEE	Ethernet mit 100 Mbit/s auf zwei Paaren UTP- oder STP-Kabeln, Bestandteil von IEEE 802.3, max. 100m
IEEE 802.1d	IEEE	Transparentes Bridging

1 Einführung

Übertragungsprofile sind Definitionen für ein Datenübertragungssystem, die die Übertragungswege, Übertragungsprotokolle und wenn nötig Übertragungsgeräte betreffen. Das vorliegende Dokument spezifiziert die Eigenschaften eines OCIT-Outstations Übertragungsprofils für Ethernet¹ mit DHCP (Dynamic Host Configuration Protocol). DHCP ermöglicht die automatische Zuweisung der Netzwerkkonfiguration an die im Netz angeschlossenen Geräte. Dadurch ist die Einbindung eines neuen Geräts in ein bestehendes Netzwerk ohne dessen manuelle Konfiguration möglich. Das Gerät bezieht die IP-Adresse und weitere Adressinformationen von einem DHCP-Server. Bei Topologieänderungen ist keine deshalb keine manuelle Änderung der Konfiguration aller Geräte im Netz nötig. Die entsprechenden Vorgaben werden vom Administrator nur einmal in der Konfigurationsdatei des DHCP-Servers gemacht.

2 Übertragungsprofil (Profil 3)

Das „Übertragungsprofil Ethernet mit DHCP“ wird mit dem Kurznamen Profil 3 bezeichnet. Damit werden OCIT-O Feldgeräte über Ethernet in ein Netzwerk eingebunden. In diesem Dokument werden die notwendigen Anforderungen an das Feldgerät und an die Zentrale spezifiziert, sowie Angaben zu den Anforderungen an das Kundennetz gemacht.

Das Profil 3 kann zusammen mit Schnittstellen OCIT-O Lstg_Vx.x eingesetzt werden.

Hinweis: Obwohl grundsätzliche Philosophien des OCIT-O Profils 1 (wie z.B. die Vergabe von Netzwerkparametern durch die Zentrale) übernommen wurden, kann daraus nicht geschlossen werden, dass Feldgeräte, die das Profil 1 oder 2 unterstützen auch auf das hier spezifizierte Profil umgerüstet werden können, denn dies hängt von Art und Umfang des eingesetzten Betriebssystems und der damit verbundenen Hardware ab.

2.1 Einsatzmerkmale

Für eine Vielzahl von Übertragungsnetz-Technologien sind an den Endpunkten Ethernet-Umsetzer und Anschlüsse verfügbar. Eine OCIT-O Profil auf Basis des Ethernet Standards,

¹ Ethernet ist eine Datennetztechnik für lokale Datennetze (LANs). Sie ermöglicht den Datenaustausch zwischen den im LAN angeschlossenen Geräten. Ethernet verbindet per Kupferkabel, Glasfaser oder Funk Geräte im Nahbereich bis über weite Entfernungen. Ethernet umfasst Festlegungen für Kabeltypen und Stecker, beschreibt die Signalisierung für die Bitübertragungsschicht und legt Paketformate und Protokolle fest. Aus Sicht des OSI-Modells spezifiziert Ethernet sowohl die physikalische Schicht (OSI Layer 1) als auch die Data-Link-Schicht (OSI Layer 2). Ethernet ist eine Basis für Netzwerkprotokolle, z. B. TCP/IP.

kann daher für die Strecke zwischen Feldgerät und Zentrale verschiedenste Standleitungs-Technologien benutzen, wenn durch geeignete Umsetzung an den Endpunkten eine Ethernet-Verbindung hergestellt werden kann.

Solche Technologien zwischen den Ethernet-Endpunkten („Ethernetverlängerung“) können sein:

- SDH
- ATM mit SDH
- ATM mit ADSL
- ATM mit SHDSL
- LWL-Anbindung
- diverse proprietäre Lösungen, die an den Endpunkten jedoch Ethernet bieten

Im Unterschied zum OCIT-O Profil 1 wird im Feldgerät mit OCIT-O Profil 3 nicht eine passive Zweidrahtleitung angeschlossen, sondern es wird eine Ethernet-Komponente bis OSI-Schicht 2 integriert. Für die Verbindung zwischen dem Gerät und seinem Ethernet-Endpunkt ist üblicherweise ein Lieferant verantwortlich.

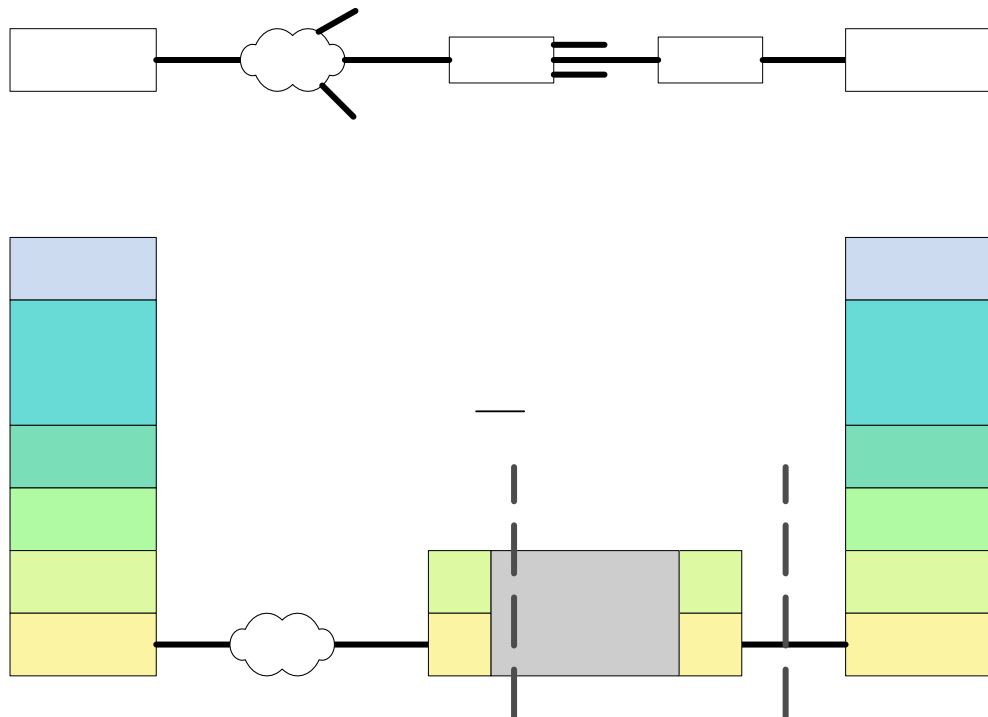


Abbildung 1: OCIT-O Profil 3 aus Sicht des ISO-Modells

Der Anteil des Kundennetzes ist optional zu sehen. Es ist aber davon aus zu gehen, dass in zunehmenden Maße vorhandene Backbone-Lösungen des Kunden mit zu benutzen sind.

3 Festlegungen zum Profil 3

3.1 Einsatz von DHCP

Die OSI-Schichten 1 und 2 des OCIT-O Profils 1 (V.24/V.34 und PPP) werden durch die Technologie Ethernet ersetzt. Die im PPP-Protokoll spezifizierte Übergabe relevanter Informationen wie IP-Adresse des Feldgerätes wird durch das DHCP-Protokoll ersetzt. Da das Ethernet faktisch ein Bussystem ist, kann das Feldgerät nicht wie beim bisherigen PPP-Protokoll anhand einer physikalisch vorhandenen Leitung identifiziert werden. Dazu gibt es zwei Lösungsmöglichkeiten:

- Einsatz von DHCP
- Erforderliche Kommunikationsparameter werden je Feldgerät individuell geplant und fest (manuell) im FG und in der Zentrale versorgt

Die automatische Zuweisung der Netzwerkkonfiguration an die im Netz angeschlossenen Geräte mittels DHCP ist die standardisierte Lösung für das Profil 3. Verwendet wird dabei ausschließlich eine Identifizierung des Feldgeräts über den DHCP-Client-Identifizier².

Wenn eine manuelle Einstellung aller oder einzelner erforderlicher Netzwerkparameter in Zentrale und Gerät gefordert werden, ist dies eine projektspezifische Erweiterung.

3.2 Anforderungen an die Zentrale

Zur Erfüllung der Anforderungen des Profils 3 **muss**³ die Zentrale über mindestens einen geeigneten DHCPv4-Server gemäß RFC 2131 und RFC 2132 verfügen. Der DHCP Server **muss** DHCP-Relays gemäß RFC 3046 unterstützen. Insbesondere **muss** er DHCP-Requests bzw. DHCP Offers sowohl als Broadcasts als auch als Unicast empfangen bzw. versenden können.

3.2.1 Per DHCP übermittelte Informationen

Ist das Feldgerät bei der Zentrale bekannt und richtig versorgt, beantwortet der DHCP-Server der Zentrale einen DHCP Request des Feldgerätes mit einem DHCP Offer. Ist das Feldgerät in der Zentrale nicht bekannt, **muss** die Zentrale keinen DHCP Offer liefern. In der folgenden Tabelle 1 sind die vom DHCP-Server der Zentrale an Feldgerät zwingend zu übergebende Netzwerkparameter aufgelistet.

² Die Identifizierung der Feldgeräte mittels der fest codierten MAC-Adressen der Ethernet-Netzwerkkarten wird nicht verwendet, da jeder Tausch dieser Baugruppen Änderungen der zentralen Einstellungen (MAC-Adressen) bedingen würde.

³ Bedeutung gemäß RFC 2119: **muss** ist eine absolute Forderung der Spezifikation; **darf** ist eine Option.

Parameter Name	Option lt. RFC 2132 + RFC 3942	DHCP Discover (FG an Zentrale)	Gefordert über Option 55 bei Discover	Offer (Zentrale an FG)	Anmerkung / Beispiel
IP Address (des FG)	Client IP address	leer	ja	Erforderlich	Beispiel: 192.5.16.1
Subnet mask	Option 1	leer	Ja	Erforderlich	Beispiel: 255.255.254.0
Broadcast Address	Option 28	leer	Ja	Erforderlich	Beispiel: 192.5.17.255
Default Router	Option 3	leer	Ja	Erforderlich	Beispiel: 192.5.17.254
DNS Servers	Option 6	leer	Ja	Erforderlich	Es werden wie im Profil 1 mind. 2 IP-Adressen für DNS-Server übergeben. Ist nur ein DNS-Server verfügbar, sind beide Einträge identisch. Beispiel: 172.5.14.254, 172.5.14.254
Domain Name	Option 15	leer	Ja	Erforderlich	Domainname Anteil des Gerätes (ohne Hostname) Beispiel: z12.beispielkunde.org
IP Address Lease Time	Option 51	leer (bzw. nicht relevant)	Ja	Erforderlich	Empfohlene Leasetimes: 1 bis 4 Std. Leasetimes kleiner 10 Minuten sind nicht zugelassen.
Parameter Request list	Option 55	Erforderlich (vgl. nächste Spalte)	n.a.	n.a.	
Client Identifier	Option 61	Erforderlich	n.a.	n.a.	Beispiel: ocit-z12-fg4711
Site-specific option "ocit-dhcp"	Option 254	n.a.	Ja	Erforderlich	Vergleiche auch Kap. 3.2.2 Interaktion von mehreren DHCP-Servern und 3.3.2.3 Verwendung der vom DHCP-Server erhaltenen Informationen

Tabelle 1: Anforderung und Übertragung zwingend erforderlicher DHCP-Parameter

Der DHCP Server der OCIT Zentrale **darf** beim DHCP Offer und beim DHCP Ack weitere Parameter versenden, wenn sichergestellt ist, dass die erforderlichen Parameter vollständig (also ohne Beschneidung) übertragen werden. Diese Informationen sind "quasistatisch" (wie auch im bisherigen OCIT-O Profil 1), d.h. im Normalfall werden vom DHCP-Server immer die gleichen Parameter, insbesondere auch nach einem Neustart des DHCP-Servers, ausgegeben.

Als Sonderfall gilt z.B. eine Netzumstrukturierung und eine damit verbundene Änderung der Netzwerkparameter. Für diesen Sonderfall ist während der Umstellung eine praktikabel kurze "IP Address Lease Time" zu vergeben.

3.2.2 Interaktion von mehreren DHCP-Servern

Damit mehrere DHCP-Server auch von verschiedenen Herstellern in der Zentrale betreibbar sind, dürfen diese DHCP-Server ausschließlich für explizit bekannt gemachte Feldgeräte (bzw. Client-Identifizier) Lease Informationen ausliefern.

Vorzugsweise sollten die Feldgeräte in Subnetzen betrieben werden, in denen nur ein DHCP-Server aktiv ist. Da nie auszuschließen ist, dass ein weiterer, nicht OCIT-O Profil 3 konformer DHCP-Server aktiv ist, der auf Requests eines Feldgeräts antwortet, wird um eine mögliche Zuordnung von falschen IP-Adressen zu verhindern wie folgt vorgegangen:

- Optionen im Bereich von 224 bis 254 sind im DHCP Protokoll gemäß RFC 3942 für „site-specific“ Erweiterungen vorgesehen. Der für OCIT-O Profil 3 eingesetzte DHCP Server **muss** die Definition solcher Optionen unterstützen.
- In der DHCP Server Konfiguration **muss** die „Site-specific“ Option „ocit-dhcp“ mit Optionsnummer 254 als Boolean Wert angelegt sein.
- Der DHCP Server ist so zu konfigurieren, dass für alle in der Zentrale konfigurierten OCIT Feldgeräte die Option „ocit-dhcp“ in den Lease Offer Paketen auf True gesetzt wird.

Hinweis: Es darf in der Zentrale mehr als einen OCIT-O kompatiblen DHCP-Server geben. Damit kann zum einen eine Anlagenskalierung erreicht werden (z.B. je fg0 einen DHCP Server). Zum anderen kann damit auch die Robustheit erhöht werden (2 redundante DHCP-Server). Im Redundanzfall dürfen die eingesetzten DHCP-Server keine widersprüchlichen OFFER-Pakete senden.

3.2.3 Zentraler Systemzugang

Routing und DNS-Konfiguration ist von der Zentrale so zu gestalten, dass ein Zugriff auf die mit dem OCIT-O Profil 3 angebotenen Feldgeräte über den Zentralen Systemzugang möglich ist. Gegebenenfalls hat das auch Rückwirkungen auf projektspezifische Anteile im Kundennetz (vgl. 4.4 Gerouteter Betrieb)

3.3 Anforderung an das Feldgerät

3.3.1 Ethernetinterface

- Das Ethernetinterface **muss** 10BaseT oder 100BaseTx oder beides unterstützen.
- Unterstützt das Ethernetinterface beide Standards **darf** es die standardisierten Autonegotiation Mechanismen verwenden um Geschwindigkeit (10 oder 100 Mbit/s) auszuhandeln.
- Das Ethernetinterface **darf** den Half/Full-Duplex Mode aushandeln.

3.3.2 DHCP

3.3.2.1 Erforderliche DHCP-Optionen

Das Feldgerät **muss** beim DHCP Request alle in Tabelle 1 genannten Parameter als zwingend erforderlich deklarieren. Weitere Optionen **darf** das Feldgerät beim DHCP Request nicht fordern.

3.3.2.2 Verwendung des Client-Identifizier

Das Feldgerät **muss** die DHCP-Variante mit dem Client-Identifizier verwenden. Dabei wird durch den DHCP-Client im Feldgerät ein Request zur Zentrale gesendet. Bei diesem Request wird das Feld Client-Identifizier (Option 61) mit einem eindeutiger DHCP Client Identifizier gefüllt, der aus der Zentralennummer und der Feldgerätenummer nach dem Muster

ocit-<ZentralenNr.>-<FeldgeräteNr.>

gebildet wird (FQDN⁴ der OCIT-O Feldgeräte).

Beispiel: ocit-z12-fg4711

Hinweis: Dieser Identifizier lässt sich vollständig aus der OSI-7-Adressierung des FG in der BTPPL-Schicht ableiten. Daher ist hier keine zusätzliche manuelle Konfiguration zur Identifizierung des FG auf OSI-Schicht 2 erforderlich.

3.3.2.3 Verwendung der vom DHCP-Server erhaltenen Informationen

3.3.2.3.1 Prüfung

Die Netzwerkparameter im Feldgerät sind zwingend vollständig aus den erhaltenen DHCP-Informationen abzuleiten und dürfen im Feldgerät nicht (auch nicht in Teilen) statisch versorgt werden.

⁴ Fully Qualified Domain Name, in diesem Fall eine absolute Adresse.

Der DHCP Client im Feldgerät ist so zu konfigurieren, dass ein DHCP-Lease nur dann akzeptiert wird, wenn

- die Option 254 („ocit-dhcp“) im Lease vorhanden ist (der im Feldgerät eingesetzte DHCP Client **muss** dazu „Site-specific options“ unterstützen)

und

- wenn alle laut Tabelle 1 als erforderlich benannten Netzwerkparameter gültig übergeben wurden.

Ist die DHCP Option 254 im DHCP-Offer nicht vorhanden (wird von OCIT-fremden DHCP Servern in der Regel nicht benutzt), **muss** der DHCP Client des Feldgeräts diese Leases verwerfen. Dadurch wird eine Zuordnung falscher IP Adressen vermieden bzw. Konflikte sehr unwahrscheinlich. Der Zustand der Option 254 (true oder false) wird im Feldgerät nicht ausgewertet.

Die übergebenen Netzwerkparameter sind ungültig, wenn der Domainname eine falsche Zentrallennummer enthält.

3.3.2.3.2 Initialisierung

Für das Feldgerät müssen folgende Punkte beachtet werden:

1. Netzwerkinterface IP, Broadcast, etc. gemäß DHCP einstellen
1. Routen setzen
2. DNS Resolver konfigurieren
3. Falls Zeitsynchronisation nach Zentrale konfiguriert ist: Zeitsynchronisation per NTP-Protokoll. Als NTP-Server gilt grundsätzlich FNr. 0 (fg0) in der Zentrale, wobei die IP-Adresse durch reverse lookup erhalten werden kann. Eine manuelle Konfiguration von NTP-Servern ist eine projektspezifische Lösung.

Sind diese Initialisierungsarbeiten erledigt, besteht aus Sicht der BTPPL-Schicht kein Unterschied zu den PPP-Standleitungsverbindungen. Dies gilt insbesondere für die erforderlichen Einträge der OCIT-Passwörter in der Datei *ocit_route1*.

Wie in Kapitel 3.2 (Anforderungen an die Zentrale) beschrieben, erfolgt die Verwaltung der Feldgeräte-IP-Adressen und anderer Netzwerkparameter im DHCP-Server quasi-statisch. Dennoch **muss** das Feldgerät eine Änderung bei allen per DHCP übergebenen und zwingend vorgeschriebenen Netzwerkparameter annehmen.

3.3.2.3.3 FG-Verhalten wenn Lease abläuft

In RFC 2131 ist das Verhalten eines DHCP-Clients bei Ablauf des Leases festgelegt. Demzufolge **darf** das Netzwerk nicht mehr für die normale Kommunikation verwendet werden und der DHCP-Client **muss** eine Neuinitialisierung des Netzwerkes anstoßen.

Es ist nicht zulässig, die Netzwerkkonfiguration über die LEASE-Dauer hinaus zu verwenden.

3.3.2.3.4 FG-Verhalten bei Änderung des Domain-Namens

Abweichend von den Festlegungen zu Profil 1 und 2 (OCIT-O Protokoll_V2.0, Kap. Änderung des Domain-Namens von Feldgeräten über einen DNS) wird hier der Domain-Name per DHCP übertragen. Das Feldgerät **muss** den per DHCP übertragenen Domain-Namen verwenden.

Das Feldgerät **darf** eine Reverse Lookup auf die eigene Feldgeräte Adresse machen. Das Feldgerät **darf** dabei die beim Reverse Lookup gewonnene Information nicht als Domain Namen verwenden.

Erkennt das Feldgerät eine Änderung des Domain-Namens, so **muss** es seine Einstellungen ohne manuellen Eingriff aktualisieren. Nach der Aktualisierung **muss** nach spätestens 2 Minuten eine BTPPL-Kommunikation wieder möglich sein.

3.3.3 Anforderungen an Zentrale und Feldgerät

3.3.3.1 BTPPL-Timeouts

Hinsichtlich der BTPPL-Timeouts wird das Verhalten von OCIT-O Profil 1 übernommen (siehe auch OCIT-O Protokoll, Kapitel Timeout).

3.3.3.2 Robustheit

Der OCIT-O Standard sieht vor, dass die jeweilige Server-Komponente einmal aufgebaute Sockets nicht mehr abbaut, solange ein IP-Verbindung vorhanden ist. Bei den Profilen 1 und 2 wird das Fehlen einer IP-Verbindung i.d.R. durch PPP signalisiert. Dadurch können die nicht mehr benötigten Sockets entfernt werden.

Im Fall des Profils 3 steht die Information über eine abgebrochene IP-Verbindung zum Peer in der Regel nicht zur Verfügung. Andererseits kann die Server-Komponente eine fehlende Verbindung an Hand ausbleibender Telegramme vom Client nicht sicher erkennen. Es ist ja legitim, dass ein Client über längere Zeit keine Telegramme sendet.

OCIT-O Server Komponenten, die das Profil 3 umsetzen dürfen das im OCIT-O Dokument „OCIT Outstations, Regeln und Protokolle“ im Kapitel „Prüfung des TCP-Kanals“ beschriebene Verfahren zur Verbindungsprüfung einsetzen. Wird dadurch eine Verbindung als abgebrochen erkannt, **darf** die OCIT-O Server Komponente die zu dieser Verbindung zugehörigen Sockets schließen.

OCIT-O Komponenten, die das Profil 3 umsetzen müssen daher zwingend OCIT-NULL-Telegramme von der Schnittstelle lesen und ohne jegliche Fehlermeldung verwerfen. (Anmerkung: diese Anforderung gilt seit OCIT-O V1.0).

4 Anforderung an das Kundennetz

Wie in Kapitel 3 beschrieben, beschreibt die vorliegende Spezifikation bewusst nicht sämtlich denkbaren Fernleitungsprofile. Dennoch ist es für die Funktionsweise des Profils erforderlich bestimmte Eigenschaften der projektspezifischen Übertragungstechnik zu fordern.

Die hier beschriebenen erforderliche Eigenschaften sind projektspezifisch bereitzustellen und **nicht** Teil der Anforderungen an OCIT-O konforme Zentralen und Feldgeräte.

4.1 Ethernetinterface der Fernleitung zur Anbindung des Feldgerätes

Das Ethernetinterface der Fernleitung zur Anbindung des Feldgerätes **muss** folgenden Anforderungen genügen:

- Passend zum Feldgerät Unterstützung von 10 und/oder 100 Mbit/s
- Autonegotiation ist erlaubt

Bei Problemen mit der Autonegotiation **muss** Geschwindigkeit und/oder Duplexmode fest einstellbar sein.

4.2 Transparenz der Übertragungsstrecke

Für die „Ethernetverlängerung“ vom Gerät bis zur Zentrale (und zurück) gelten:

- Es werden Standleitungen verwendet, da mit Wählverbindungen (Dial on Demand Techniken) erfahrungsgemäß keine stabile Kommunikation möglich ist.
- Keine Verbindungen über das Internet (beachte untenstehenden Hinweis)
- Effektive Datenrate mind. wie bei OCIT-O über V.34 Leitungen (mind. 28800 Bit/s in jede Richtung)

Hinweis: Sollten Verbindungen über das Internet gefordert werden, so ist dies mit projektspezifischen Lösungen abzubilden. Der Errichter und der Betreiber der Datenstrecke zwischen den hier standardisierten Schnittstellen (nachfolgend Netzsegment genannt) hat zu gewährleisten, dass dem Stand der Technik und dem Gefährdungspotential⁵ entsprechende technische und organisatorische Sicherheitsmaßnahmen ergriffen und betrieben werden (u.a. VPN-Tunnel).

Dem Errichter oder Betreiber der OCIT-Zentrale oder des OCIT Feldgerätes sind auf Anfrage die geplanten oder betriebenen Sicherheitsmaßnahmen darzulegen, damit beurteilt werden kann, ob diese Maßnahmen für den Schutz der Zentrale oder des Feldgerätes ausreichend sind. Bedenken des Errichters wegen unzureichenden Schutz sind zu dokumentieren. Die Verantwortung für die Inbetriebnahme des Systems liegt als Letztentscheider beim Betreiber.

⁵ Internettechnologien sind unsicher in dem Sinne, dass bei fehlenden oder unzureichenden Schutzmaßnahmen Hacker bis in das Netz des Betreibers durchdringen können.

Eine Zustimmung zur Inbetriebnahme stellt keine Zertifizierung dar und entbindet daher den Errichter oder Betreiber des Netzsegmentes nicht von seiner Verantwortung für die installierte Technik und den sicheren Betrieb des Netzsegmentes.

4.3 Geswitchter Betrieb

Sind an einer Zentrale nicht mehr als 50 Geräte zu betreiben und herrscht in der Zentrale ein niedriges Broadcast-Aufkommen, so können die Geräte im geswitchten Betrieb angebunden werden (Layer 2 transparent). Damit wird ein Netz betrieben, das die Zentrale und die Feldgeräte in einer (DHCP-) Broadcastdomäne zusammenfasst. Hierbei ist ein DHCP-Relay und IP-Routing nicht erforderlich.

Zusätzlich zu den allgemeinen Transparenzanforderungen an die Übertragungsstrecke gelten bei geswitchtem Betrieb zwingend folgende Anforderungen:

- transparentes Bridging der MAC-Schicht nach IEEE 802.1d (in beiden Richtungen symmetrisches Verhalten)
- Dynamisches Lernen von Adressen (inkl. Aging)

Hinweis: Die Agingzeiten der verwendeten Komponenten sollten etwa 10 Minuten betragen. Sind die Zeiten höher, ist mit entsprechend länger anhaltenden Verbindungsproblemen nach dem Tausch von Hardwarekomponenten im Netzbereich (z.B. Netzwerkkarte an Feldgerät) zu rechnen.

4.4 Gerouteter Betrieb

Überschreitet die Anzahl der per Profil Ethernet anzubindenden Geräte ein Grenze von 50 oder wird im Zentralen-Netz ein Broadcast-Aufkommen erwartet oder beobachtet, dass mengenmäßig nicht sicher über die „Ethernetverlängerung“ transportiert werden kann, wird ein gerouteter Betrieb dringend empfohlen.

4.4.1 Einstellungen des Routings

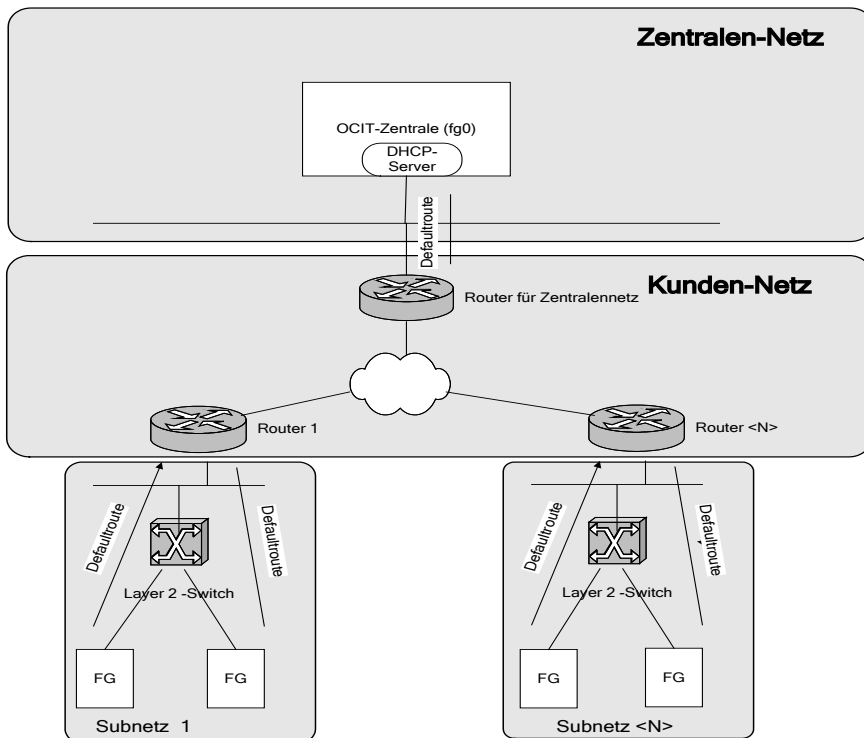


Abbildung 2: Routing über Kundennetz

Die per Ethernet angebotenen Feldgeräte (FG) setzen eine Default Route auf einen „Kundenrouter“ (Hier Router1 ... Router N).

Anmerkung: Die Adresse dieses Default Routers wird per dem Feldgerät DHCP von der OCIT-Zentrale vorgegeben (vgl. Option 3).

Die Router im „Kundennetz“ müssen nun so eingestellt werden, dass die FG-Netze vom Zentralen-Netz und umgekehrt erreicht werden können. Insbesondere **muss** dabei die OCIT-Zentrale (konkret fg0) erreichbar sein.

4.4.2 Einsatz eines DHCP Relay

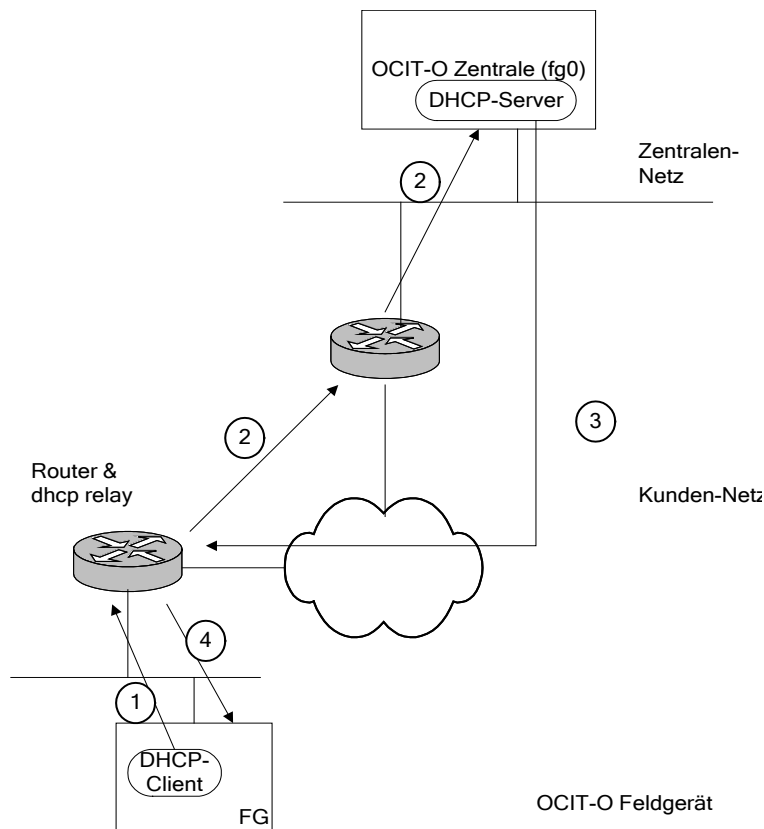


Abbildung 3: DHCP relay

Da die Zentrale und die Feldgeräte im gerouteten Fall nicht im selben LAN (genauer: Broadcast Domain) betrieben werden, **muss** das Kundennetz ein DHCP Relay gemäß RFC 3046 bereitstellen (siehe Abbildung 3). Diese Funktion **muss** zumindest auf dem Default Router des anzubindenden Feldgeräts aktiviert sein.

Hinweise: DHCP relays sind nicht zwingender Bestandteil einer OCIT-Zentrale
DHCP relays können auch kaskadiert betrieben werden.

Erläuterungen zum Ablauf:

1. DHCP Client im Feldgerät sendet DHCPREQUEST per **Broadcast**.
2. Der Router mit DHCP Relay empfängt den DHCPREQUEST und sendet ihn per Unicast Datagram an den DHCP Server der OCIT-Zentrale (eventuell über mehrere andere Router). Die IP Adresse des zugehörigen DHCP Servers wird beim Einrichten der Relay Funktion im Router hinterlegt.
3. Der DHCP Server antwortet dem DHCP Relay (im Router).
4. Das DHCP Relay sendet die Antwort per Broadcast an das Feldgerät.

4.4.3 Benötigte Dienste zwischen Zentrale und Feldgerät

Dienst	Von	Verbindungs- aufbau	Nach	Protokoll	Port(s)	Bemerkung
btppp	ZLAN	→ ←	FG	tcp, (udp)	2504, 3110, 5001	
dns	ZLAN	←	FG	udp	53	
ntp	ZLAN	←	FG	udp	123	
n.a.	ZLAN	→ ←	FG	icmp	n.a.	wegen "ping" für Diagno- sezwecke
n.a.	ZLAN	←	FG	dhcp	n.a.	

ZLAN= Zentralen-LAN

Tabelle 1 Benötigte Dienste zwischen FG ↔ Zentrale

Ggf. wird die Weiterleitung weiterer herstellerspezifischer Protokolle (z.B. secure shell, https) nötig, um die Feldgeräte im vollen (herstellerspezifischen) Leistungsumfang administrieren zu können.

A1 DHCP-Konfigurationen für Client und Server

Hinweis: Die hier aufgeführten Konfigurationen sind nicht getestet und nur als Beispiel für Entwickler gedacht!

Gültigkeit: ISC-Implementierungen von DHCP (entspricht der Referenzimplementierung des DHCP Protokolles)

A1.1 Client

sample_dhclient.conf

```
#####
# Suggested configurations for OCIT DHCP client (profile 3)
# for ISC implementation of DHCP only
#####
#
#

timeout 60;
retry 60;
reboot 10;
select-timeout 5;
initial-interval 2;

send dhcp-lease-time 3600;
option ocit-dhcp code 254 = boolean;

interface "eth0" {
    send dhcp-client-identifier "ocit-z11-fg1004";
    send host-name "fg1004";
    request subnet-mask, broadcast-address, routers, domain-name,
domain-name-servers, host-name, ocit-dhcp;
    require subnet-mask, domain-name, domain-name-servers, routers,
ocit-dhcp;
    script "/etc/ppp/dhclient-ocit";
}
```

A1.2 Server

sample_dhcpd.conf

```
# dhcpd.conf
#
# configuration template OCIT-O Profile 3 file for ISC dhcpd
#
allow unknown-clients;
deny duplicates;

# client identifier
option option-67 code 67 = text;
```

```

# marker option used by fielddevice clients to check
# that dhcp server is valid for OCIT
option ocit-dhcp code 254 = boolean;
option ocit-dhcp on;

default-lease-time 900;
max-lease-time 7200;

# global options
option domain-name "z11.beispielkunde.org";
option domain-name-servers 172.17.3.254,172.17.3.254;

shared-network OCIT-LAN {

    subnet 172.17.3.0 netmask 255.255.255.0 {
        option subnet-mask 255.255.255.0;
        option broadcast-address 172.17.3.255;
        option routers 172.17.3.254;
        default-lease-time 3600;
        max-lease-time 7200;

        # field device section
        class "ocit-z11-fg1004" {
            match pick-first-value (option dhcp-client-identifier, hardware);
        }
        subclass "ocit-z11-fg1004" "ocit-z11-fg1004";

        class "ocit-z11-fg1006" {
            match pick-first-value (option dhcp-client-identifier, hardware);
        }
        subclass "ocit-z11-fg1006" "ocit-z11-fg1006";

        pool {
            allow members of "ocit-z11-fg1004";
            range 172.17.3.1 172.17.3.1;
        }
        pool {
            allow members of "ocit-z11-fg1006";
            range 172.17.3.3 172.17.3.3;
        }
    }
}
# end of subnet
}
# end of shared-network OCIT-LAN

```

Glossar

ADSL	Asymmetric Digital Subscriber Line, Anschlusstechnik für Breitbandanschlüsse über die vorhandene Telefonanschlussleitung.
ATM	Asynchronous Transfer Mode, ist eine Technik der Datenübertragung, bei der der Datenverkehr in kleine Pakete codiert und über asynchrones Zeitmultiplexing übertragen wird.
BTPPL	Basis Transport Paket Protokoll Layer der OCIT-O Schnittstelle
DHCP	Dynamic Host Configuration Protocol, ermöglicht die automatische Zuweisung der Netzwerkkonfiguration an die im Netz angeschlossenen Geräte.
DNS	Domain Name System, eine verteilte Datenbank, die den Namensraum im Netzwerk verwaltet
Ethernet	Eine Datennetztechnik für lokale Datennetze (LANs).
IP	Internet Protocol
ISO / OSI	ISO/OSI-Basis-Referenzmodell (DIN-ISO 7498 v.1982, X.200 v. 1994) ISO: International Organization for Standardization OSI: Open Systems Interconnection
LAN	Local Area Network (Lokales Netzwerk in der Computertechnik)
LWL	Lichtwellenleiter
MAC-Adresse	Media-Access-Control-Adresse ist die Hardware-Adresse jedes einzelnen Netzwerkkadapters, die zur eindeutigen Identifizierung des Geräts in einem LAN dient.
PPP	Point to Point Protocol, ein Protokoll zum Verbindungsaufbau über Wählleitungen zum Internet Service Provider.
RFC	Request for Comment (= Arbeitspapiere, Protokoll-Spezifikationen oder Kommentare zu Netzwerk-Themen)
Router	Geräte die mehrere Rechnernetze verbinden. Dabei analysiert der Router die ankommenden Datenpakete nach ihrer Zieladresse und blockt diese oder leitet sie entsprechend weiter.
SDH	Synchronous Digital Hierarchy, eine der Multiplex-Techniken im Bereich der Telekommunikation, die das Zusammenfassen von niederratigen Datenströmen zu einem hochratigen Datenstrom erlaubt. Das gesamte Netz ist dabei synchron.
SHA-1	Secure Hash Algorithm, eine Gruppe standardisierter Funktionen, zur Berechnung eines eindeutigen Prüfwerts für beliebige Daten.
SHDSL	Symmetrical High-bit-rate Digital Subscriber Line, ermöglicht die permanente Anbindung an das Internet durch Bereitstellung einer Standleitung.
TCP	Transmission Control Protocol Eines der Internetprotokolle. Verbindungsorientiertes Transportprotokoll in Schicht 4 des ISO/OSI-Referenzmodells.

UDP	User Datagram Protocol Eines der Internetprotokolle. Verbindungsloses Protokoll in Schicht 4 des ISO/OSI-Referenzmodells.
V.xx	Standards der ITU-T (International Telecommunications Union), früher CCITT
XML	Extensible Markup Language Metasprache für das Definieren von Dokumenttypen. XML liefert die Regeln, die beim Definieren von Dokumenttypen angewendet werden.

OCIT-O-Profil_3_V1.0_A01

Copyright © 2009 ODG
