

Häufige gestellte Fragen ("FAQ") bei IP-Übertragungsgeräten und NGN

Im BHE-Fachausschuss für Übertragungs- und Netzwerktechnik wurden die "häufig gestellten Fragen" der Hersteller-Hotlines zum Thema IP-Übertragungsgeräte bzw. NGN (Next-Generation-Network) zusammengetragen und durch Experten beantwortet. Gerne werden in diesem Zusammenhang weitere Fragestellungen aufgenommen, deren Beantwortung dann bei einer Überarbeitung des Papiers ergänzt werden kann.

Übersicht über die Fragen:

1. [Welche Hersteller sind bei einer IP-Aufschaltung untereinander kompatibel?](#)
2. [Welche NSL sind gemäß VdS für den Empfang von IP zugelassen?](#)
3. [Warum kann das ISDN-Datenprotokoll nicht über IP geroutet/getunnelt werden?](#)
4. [In welchen Zeitabständen muss bei einer verschlüsselten Verbindung der Schlüssel geändert werden?](#)
5. [Wie viele Objekte können bei der NSL denselben Schlüssel für die verschlüsselte Verbindung nutzen?](#)
6. [Wie erkennt man, ob der Kunde einen NGN oder einen klassischen Telekommunikationsanschluss hat?](#)
7. [Wie realisiert man die Notstromversorgung des Routers?](#)
8. [Sind die Übertragungseinrichtungen \(ÜE\) gegen einen Angriff aus dem Internet sicher?](#)
9. [Was geschieht während bzw. nach der Zwangstrennung des DSL-Anschlusses?](#)
10. [Wie kommt man von außen auf die ÜE?](#)
11. [Kommt man von außen über GPRS auf die ÜE?](#)
12. [Einstellungen im Router?](#)
13. [Was muss bei einer Firewall beachtet werden?](#)
14. [Wie kann bei verschlüsselten Verbindungen der Schlüssel abgeholt oder gewechselt werden?](#)
15. [Welche Lösung ist VdS konform?](#)
16. [Wie und wann läuft die Umstellung auf NGN?](#)
17. [Wie kann man testen, ob der Port gesperrt ist \(Lokal oder auf Zielseite\)?](#)
18. [Was ist ein lokaler Port und ein Zielport bzw. was sind Ports überhaupt?](#)
19. [Wie kann man testen, ob z.B. durch eine Firewall Sperrungen vorhanden sind?](#)
20. [Was ist der Gateway und braucht man den unbedingt?](#)
21. [Was muss in der Netzmaske stehen?](#)
22. [Was ist ein DNS und was muss hierbei eingetragen werden?](#)
23. [Wie finde ich die MAC – Adresse heraus?](#)
24. [Welche Möglichkeiten der Protokollierung gibt es?](#)
25. [Wie kann ich sporadische TCP – Ausfälle über längere Zeit \(mehrere Tage\) protokollieren?](#)

26. [Wie funktioniert der Schlüsselwechsel?](#)
27. [Welches Protokoll wird über TCP/ IP übertragen?](#)
28. [Warum dauert die Meldungsübertragung bei einer verschlüsselten Verbindung so lange?](#)
29. [Welche Bandbreite benötigt man für eine stehende TCP/IP Verbindung? \(Datenmenge\)](#)
30. [Kann ein IP-ÜG auch über W-LAN angeschlossen werden?](#)

1. *Welche Hersteller sind bei einer IP-Aufschaltung untereinander kompatibel?*

Alle Hersteller, die nach dem Protokoll VdS 2465-S2 arbeiten und die im Verzeichnis VdS 2471 A.13 „Schnittstelle S2/S3 zur Anschaltung an IP-Netze unter Verwendung des TCP-Protokolls“ beschriebenen Anforderungen einhalten.

2. *Welche NSL sind gemäß VdS für den Empfang von IP zugelassen?*

Die NSL muss im Verzeichnis "VdS-anerkannte Wach- und Sicherheitsunternehmen WUS" (VdS 2136) aufgeführt sein und die Anforderungen nach VdS 2471 A.13 einhalten.

Bei Aufschaltung auf die NSL eines VdS-anerkannten WuS sind die Interventionsmaßnahmen zwischen diesem und dem Betreiber der EMA – ggf. in Abstimmung mit dem Versicherer – zu vereinbaren und mit dem Alarmdienst- und Interventionsattest, VdS 2529 vom WuS zu dokumentieren. Das WuS ist von der Errichterfirma darüber zu informieren, dass es sich bei der Aufschaltung um eine VdS-anerkannte EMA handelt.

Hinweis: Inzwischen wurden alle drei Teile der europäischen Norm DIN 50518 für Alarmempfangsstellen in Deutschland durch das DIN veröffentlicht. Im dritten Teil der Normenreihe wird die jährliche Überprüfung zum Nachweis der Einhaltung der Normanforderungen anhand eines jährlichen Audits gefordert. Ein Verzeichnis der VdS-Zertifizierten Alarmempfangsstellen gemäß DIN EN 50518 – VdS 3139 finden Sie unter http://www.vds.de/fileadmin/fachbereiche/vds_3139_3.pdf

In der VdS 2311 Planung/Einbau EMA wird derzeit noch nicht auf die DIN EN 5018 verwiesen.

3. *Warum kann das ISDN-Datenprotokoll nicht über IP geroutet/getunnelt werden?*

Das dafür notwendige HDLC over IP (High-Level Data Link Control über das IP-Netz) wird nicht oder nur selten unterstützt.

4. *In welchen Zeitabständen muss bei einer verschlüsselten Verbindung der Schlüssel geändert werden?*

Der VdS schreibt hierzu keine Zeitabstände vor. Bei Anlagen nach BSI-Standard (Bundesamt für Sicherheit in der Informationstechnologie) muss dies jährlich erfolgen.

5. *Wie viele Objekte können bei der NSL denselben Schlüssel für die verschlüsselte Verbindung nutzen?*

Jedes Objekt **muss** seinen eigenen Schlüssel besitzen.

6. *Wie erkennt man, ob der Kunde einen NGN oder einen klassischen Telekommunikations- Anschluss hat?*

Wenn auf der Sendeseite die analoge- oder ISDN-Telefonleitung durch ein IAD-Gerät (IAD = Integrated Access Device, z.B. Fritz-Box) bereitgestellt wird, handelt es sich um einen NGN-Anschluss. Bitte beachten Sie hierzu auch das Papier "BHE-Hinweise zu Alarm-Übertragungsgeräten an sogenannten NGN-Anschlüssen".

Link: http://www.bhe.de/direkt/UNT-FAQ-Papier/BHE-Hinweise_zu_Alarmuebertragungsgeraeten_05_2009.pdf

7. *Wie realisiert man die Notstromversorgung des Routers?*

Gemäß VdS ist nicht gefordert, da Router und NTBA Kommunikationsgeräte sind, die bereits zum Netz gehören. Das ist einer der Gründe, warum ein Ersatzweg notwendig ist (welcher sich nicht aus dem für den Hauptübertragungsweg genutzten IP-Netz bildet).

8. *Sind die Übertragungseinrichtungen (ÜE) gegen einen Angriff aus dem Internet sicher?*

Die ÜE arbeitet abgehend als Client und nicht als Server, somit werden keine ankommenden Verbindungen angenommen. Falls im ÜE ein Fernzugang über IP eingerichtet ist, so wird dieser ebenfalls AES-verschlüsselt (AES = Advanced Encryption Standard, ein Verschlüsselungsstandard, der als sehr sicher gilt) und ankommende Verbindungen können durch IP-Adressenvergleich geblockt werden (Firewall-Funktionalität in der ÜE).

9. *Was geschieht während bzw. nach der Zwangstrennung des DSL-Anschlusses?*

Die ÜE nimmt einen automatischen Wiederaufbau vor (Dauer ca. < 20s).

10. *Wie kommt man von außen auf die ÜE?*

Entweder hat der Anschluss eine feste IP-Adresse oder es muss ein DynDNS-Server (s.a. Frage: "Einstellungen im Router") eingerichtet werden. Zusätzlich ist eine entsprechende Portregel auf die IP-Adresse der ÜE im Router erforderlich.

11. *Kommt man von außen über GPRS auf die ÜE?*

Normalerweise nicht bzw. nur, wenn spezielle Providerdienste genutzt werden.

12. *Einstellungen im Router?*

DynDNS-Anbieter ist z.B. DynDNS.org. Dieser Anbieter stellt die Möglichkeit bereit, dass man unter einer festen Adresse, z.B. Firmenname.dyndns.org erreichbar ist, da der Name auf die sich ändernde IP-Adresse des Gerätes verweist.

Domainname (Hostname):

Der Domainname ist die eindeutige Bezeichnung für einen Zusammenschluss von mehreren Rechnern zu einem Netzwerk.

Der **Hostname** (auch **Sitenname**) ist die eindeutige Bezeichnung eines Rechners in einem Netzwerk.

Port-Nummer:

Anhand der Port-Nummer kann festgelegt werden, an welchen Port der IP-Adresse das IP-Paket gesendet werden soll.

13. *Was muss bei einer Firewall beachtet werden?*

Die verwendeten Zielports müssen in der Firewall freigegeben sein (für abgehende Verbindung).

14. *Wie kann bei verschlüsselten Verbindungen der Schlüssel abgeholt oder gewechselt werden?*

vgl. hierzu VdS 2311 (9.4.7.6 Verschlüsselung)

... Verschlüsselung, Schlüsselvergabe und Schlüsselaustausch sind in der ÜE realisiert, wenn diese für IP-Alarmübertragung VdS-anerkannt ist. ...

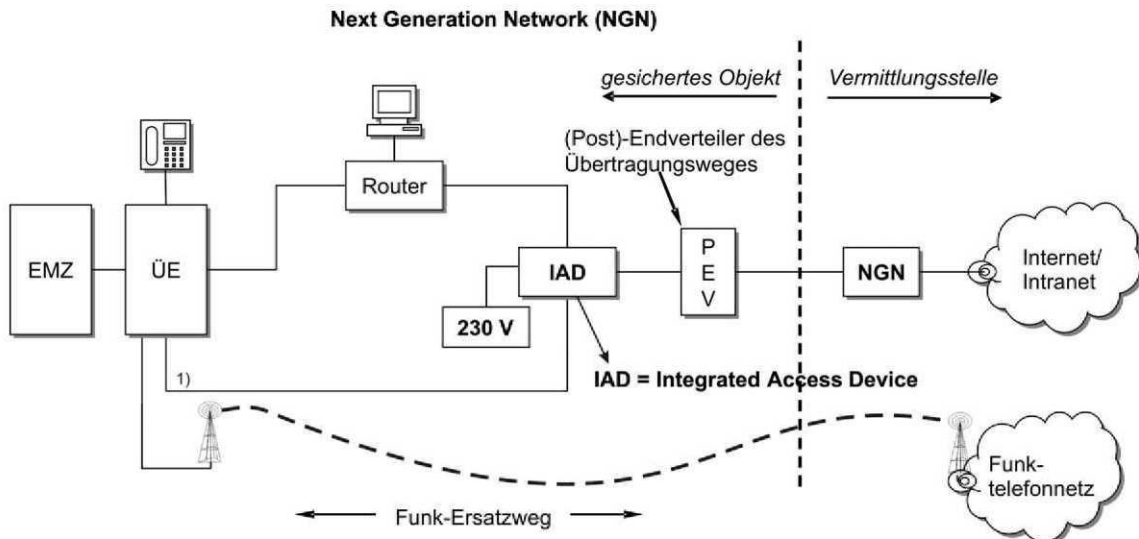
Hinweis 1: Eine unverschlüsselte (ungesicherte) Übertragung ist nur in einem Intranet zulässig, bei dem sichergestellt ist, dass kein unerlaubter Zugang über Fremdnetze zum Übertragungsweg möglich ist. Dies muss vom Netzbetreiber schriftlich bestätigt werden.

Hinweis 2: Die Übertragung des Schlüssels muss immer über den zweiten Übertragungsweg (z.B. ISDN-Netz-B-Kanal oder Funknetz) erfolgen. Eine Übertragung von Schlüsseln über die aktuelle IP-Verbindung ist nicht zulässig.

Hinweis 3: In Einzelfällen (z.B. bei der Erstinbetriebnahme oder bei behördlichen Anforderungen) kann die Schlüsselvergabe auch durch eine manuelle Eingabe vor Ort oder per Datenträger, auf dem der Schlüssel verschlüsselt oder unverschlüsselt gespeichert ist, erfolgen.

15. Welche Lösung ist VdS konform?

→ Auszug VdS 2311: Erfolgt der Anschluss der ÜE an das IP-Netz des Betreibers über eine integrierte Anschlusseinheit (IAD; Integrated Access Device) mit 230 V Netzstromversorgung, bei der DSL-Modem und NTBA in einem Gerät integriert sind (so genanntes „Next Generation Network - NGN“), **muss** der Ersatzweg über eine separate Trasse (z.B. Funk-Netz) geführt werden (siehe Bild 9.05).



1) Beim „NGN“ darf die drahtgebundene Telefonie **nicht** als Ersatzweg genutzt werden, da sie bei Ausfall des Internets/Intranets ebenfalls nicht mehr verfügbar ist.

Bild 9.05: IP-Übertragung mit Ersatzweg über separate (Funk-)Trasse bei zukünftigen Telefonsystemen („Next Generation Network – NGN“)

16. Wie und wann läuft die Umstellung auf NGN?

Die Umstellung läuft bereits testweise. Die Deutsche Telekom plant vorerst, keine neuen ISDN-Verträge offensiv anzubieten. Die Abschaltung von Vermittlungsstellen soll erfolgen, wenn nur noch ein kleiner Teil von ISDN Anschlüssen aktiv ist. Genau Zahlen sind hier nicht bekannt.

17. Wie kann man testen, ob der Port gesperrt ist (Lokal oder auf Zielseite)?

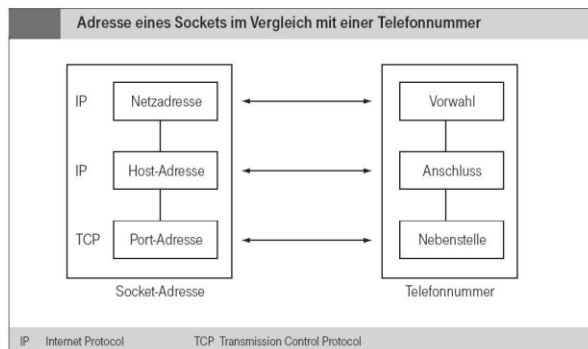
Durch Verwendung von Netzwerkanalyse-Tools wie z.B. nmap (<http://nmap.org/man/de/>)

18. Was ist ein lokaler Port und ein Zielport bzw. was sind Ports überhaupt?

Ein **Port** ist ein Teil einer Adresse. Bestimmte Applikationen verwenden Portnummern, die ihnen von der IANA fest zugeordnet und allgemein bekannt sind. Sie liegen üblicherweise von 0 bis 1023. Anwendungshersteller können bei Bedarf Ports für eigene Protokolle registrieren lassen. Die Portnummer 49152 bis 65535 sind so genannte *Dynamic* und/oder *Private Ports*. Diese lassen sich variabel einsetzen.

Eine TCP-Verbindung ist abhängig von 4 Parametern:

- Quell IP-Adresse (von Client)
- Quell Port (von Client)
- Ziel IP-Adresse (von Server)
- Ziel Port (von Server)



19. *Wie kann man testen, ob z.B. durch eine Firewall Sperrungen vorhanden sind?*

Durch Netzwerkanalyse mit z.B. Wireshark, nmap oder traceroute.

20. *Was ist der Gateway und braucht man den unbedingt?*

Teilweise wird ein Kombinationsgerät aus DSL-Router und DSL-Modem als Internet-Gateway bezeichnet. Diese Geräte vereinen - vereinfacht ausgedrückt - die Funktion, Netzwerke miteinander zu verbinden (Routing), mit der Fähigkeit, hierfür unterschiedliche Protokolle zu benutzen (Gateway). So werden IP-Pakete aus dem Anwendernetzwerk bei DSL-Verwendung zumeist über das PPPoE-Protokoll in das Netz des Providers übersandt. Ein Gateway ist nur notwendig, wenn die Ziel-Adresse außerhalb des lokalen Netzwerks liegt.

21. *Was muss in der Netzmaske stehen?*

In Verbindung mit der IP-Adresse eines Gerätes legt die Netzmaske fest, welche IP-Adressen dieses Gerät im eigenen Netz sucht und welche es über Router in anderen Netzen erreichen könnte. Sie trennt also die IP-Adresse in einen Netzwerkteil (Netzpräfix) und einen Geräteteil. Der Netzwerkteil muss bei allen Geräten des jeweiligen Netzes gleich, der Geräteteil bei jedem Gerät innerhalb des Netzes unterschiedlich sein. Die Netzmasken aller an einem IP-Netz beteiligten Rechner sollten somit gleich konfiguriert sein. Vergleichen sie hierzu auch unser Papier „Netzwerktechnische Grundlagen“.

Link: http://www.bhe.de/direkt/UNT-FAQ-Papier/Netzwerktechnische_Grundlagen.pdf

22. *Was ist ein DNS und was muss hierbei eingetragen werden?*

Das Domain Name System (DNS) ist einer der wichtigsten Dienste im Netzwerk. Seine Hauptaufgabe ist die Beantwortung von Anfragen zur Namensauflösung. In Analogie zu einer Telefonauskunft soll das DNS bei Anfrage mit einem Hostnamen (dem für Menschen merkbaren Namen eines Rechners im Internet) als Antwort die zugehörige IP-Adresse (die „Anschlussnummer“ im Internet) benennen.

Beispiel: Der Hostname `www.example.org` wird in eine IPv4-Adresse (z.B. `192.0.2.42`) bzw. in eine IPv6-Adresse (z.B. `2001:db8:85a3:8d3:1319:8a2e:370:7347`) umbenannt.

23. *Wie finde ich die MAC – Adresse heraus?*

Die MAC-Adresse der ÜE kann i.d.R. aus der Parametrierung entnommen werden.

Die MAC-Adresse (Media-Access-Control-Adresse) ist die Hardware-Adresse jedes einzelnen Netzwerkadapters, die zur eindeutigen Identifizierung des Geräts in einem Rechnernetz dient.

Je nach Betriebssystem sind hierzu verschiedene Befehle in der Kommandozeile oder über die grafische Benutzeroberfläche nötig. Es gibt aber auch diverse zusätzliche Programme, die diese Aufgaben vereinfachen können. In Windows XP, Vista, 7 folgendes Vorgehen:

Startmenü/Ausführen: Eingabe des Befehls „cmd“, im schwarzen Fenster, das sich öffnet, Eingabe des Befehls `ipconfig /all`; die gesuchte Kennung ist dann in der Zeile „Physikalische Adresse“ zu finden.

24. *Welche Möglichkeiten der Protokollierung gibt es?*

Sniffer-Tools wie z.B. Wireshark, „bessere“ Router protokollieren den Datenverkehr mit.

Bitte beachten Sie, dass der Einsatz von Wireshark ggf. nicht zulässig ist und der Einsatz mit den Kunden abgestimmt werden muss. Die Serviceprogramme der Hersteller bieten zudem in vielen Fällen die Möglichkeit, auf mehreren Ebenen mit zu protokollieren.

25. *Wie kann ich sporadische TCP – Ausfälle über längere Zeit (mehrere Tage) protokollieren?*

Mit verschiedenen Programmen, z.B. Wireshark (vgl. Anmerkungen unter 24).

26. *Wie funktioniert der Schlüsselwechsel?*

vgl. VdS-2465-S2, Abschnitt 10: "Die ÜE erhält von der AE eine Aufforderung zum Schlüsselwechsel. Daraufhin stellt die ÜE eine Verbindung über den sicheren Zweitweg zur AE her und fordert einen neuen Schlüssel an. Die ÜE identifiziert sich hierbei über ihre Identnummer. Als Antwort erhält die ÜE von der AE den neuen Schlüssel mit zugehöriger Schlüsselnummer. Sobald die ÜE der AE den Empfang des neuen Schlüssels bestätigt hat, dürfen AE und ÜE auf der gesicherten TCP/IP-Verbindung nur noch den neuen Schlüssel bzw. die neue Schlüsselnummer verwenden."

27. *Welches Protokoll wird über TCP/ IP übertragen?*

Es handelt sich hierbei um ein eigenständiges Protokoll, siehe Protokollbeschreibung VdS 2465-S2. Der Unterschied zwischen TCP und UDP besteht darin, dass für TCP Verbindungen immer ein Handshake, also eine Bestätigung des Erhalts eines Datenpaketes gesendet wird. Bei UDP Verbindungen, werden die Datenpakete nacheinander gesendet, ohne für jedes Datenpaket eine Empfangsbestätigung zu verlangen.

28. *Warum dauert die Meldungsübertragung bei einer verschlüsselten Verbindung so lange?*

Bei stehenden verschlüsselten Verbindungen werden alle 3 bis 8 Sekunden Datenpakete von der AE zu dem IP-ÜG gesendet. Dieses Polling darf nicht verkürzt werden, damit eventuelle Angreifer nicht Rückschlüsse ziehen können, wann Meldungen übertragen werden. Deswegen kann nur bei jedem Poll eine Meldung übertragen werden.

29. *Welche Bandbreite benötigt man für eine stehende TCP/IP Verbindung? (Datenmenge)*

Bandbreite < 0,5 kbit/s, Datenvolumen: < 150 MB/Monat (bei 4s Poll)

30. *Kann ein IP-ÜG auch über W-LAN angeschlossen werden?*

Dies ist gemäß den VdS-Regularien nicht zulässig.

Als weiterführende Informationsquelle empfehlen wir Ihnen das BHE-Papier „Übertragung von Alarmmeldungen“ **Link:** http://www.bhe.de/direkt/UNT-FAQ-Papier/Uebertragung_von_Alarmmeldungen_01_2010.pdf

BHE e.V.	Feldstr. 28 66904 Brücken	Telefon: 0 63 86/92 14-0 Telefax: 0 63 86/92 14-99	Internet: www.bhe.de E-Mail: info@bhe.de
-----------------	--	---	---