Sicherheitskonzept des öffentlicher Routingdienstes „SAVE“

1. Einleitung

Die Münchner InnoRoute GmbH baut in Deutschland ein eigenes Telekommunikationsnetz auf. Es basiert auf einem neuartigen Routingverfahren für IPv6, das eine hierarchisch strukturierte Topologie nutzt.

Das Ziel ist ein sicheres und stabiles Weitverkehrsnetz für Geschäfts- und Behördenkommunikation für IP-basierte Anwendungen. Insbesondere Anwendungen in den Bereichen Internet der Dinge (IoT) und Industrie 4.0 können von den Vorteilen des Netzes profitieren.

2. Inhaltsverzeichnis

Sicherheitskonzept des öffentlicher Routingdienstes „SAVE“ 1

Einleitung 1

Inhaltsverzeichnis 1

1. Rechtliche Einordnung 2
2. Routingrelevante Teile des Paketkopfes 3
3. Sicherstellung der Abhörsicherheit 4
4. Verifizierung des Absenderadresspräfix 5
5. Adressierung im 6Tree-Netz 7
6. 6Tree-Netzwerkstruktur 8
7. Routingalgorithmus 9
8. Routingalgorithmus bei redundantem Netz 10
9. Praktischer Aufbau des 6Tree-Netzes 10
10. Sicherer Zugang an das 6Tree-Netz 12
11. Anschluss eines mittelständischen SAVE-Teilnehmers 13
12. Anschlussarten 14
13. Router beim Teilnehmer 15
14. Globale 6Tree-Netze 17
15. Ausfallsicherheit 17
16. Netzmanagement 19
17. Standardisierung 19
18. Kundendaten 19
19. Terminologie 20

Umsetzungserklärung 21

3. Rechtliche Einordnung

Die Firma InnoRoute bietet den Routingdienst „SAVE“ an, der über das eigene Routingnetz „6Tree“ durchgeführt wird. Als IP-basierter Dienst ermöglicht SAVE die ganze Vielfalt an Anwendungen, die auf IP aufsetzen.

Im SAVE-Dienst existiert keine zentrale Namensauflösung (DNS). Die Adressen bekannter, autorisierter Kommunikationspartner werden lokal von den Teilnehmern verwaltet, was durch die einfache Adresspräfixgenerierung vereinfacht wird. SAVE ist daher nicht als Suchdienst geeignet, sondern primär für fest eingestellte, längerfristige Kommunikationsbeziehungen gedacht. Anwendungen finden sich in der Steuerung von Industrieanlagen, Standortvernetzung, Home Control, Homeoffice, Cloud Access etc.

Der SAVE-Dienst basiert auf dem Internet Protokoll (in Version 6) und ist ein Telekommunikationsdienst, kein Internet-Dienst, da die Weiterleitung der Nutzerdatenpakete im 6Tree-Netz nur anhand des IP6-Paketkopfs erfolgt und alle höheren Protokolle der ISO OSI-Schichten 4 und aufwärts nicht ausgewertet werden (siehe Abschnitt 4).

Der SAVE-Dienst ist ein reiner IPv6-Transportdienst, der die Bedingungen des Telekommunikationsgesetzes (TKG) erfüllt. Es werden (vorerst) keine Verbindungen unterstützt, sodass das 6Tree Netz zustandslos bleibt. In künftigen Ausbaustufen könnten Verbindungen zum Beispiel durch Software Defined Networking (SDN) angeboten werden.

SAVE unterstützt verschiedene Dienstgüteklassen (QoS Classes) innerhalb fest vorgegebener Ratenlimits. Auch eine TSN-Klasse mit minimaler Latenz und ohne Laufzeitvariation für industrielle Anwendungen ist vorgesehen. Dies ist in einem separaten Dokument beschrieben.

Die Nutzdaten der Datenpakete werden transparent weitergereicht, und gemäß §148 des TKG weder abgehört, ausgewertet, noch gespeichert. Daher übernimmt InnoRoute auch keinerlei Verantwortung über die Inhalte.

Missachtung des §148 TKG ist strafbewehrt. Somit liegt die permanente Sicherstellung dieser Eigenschaften im persönlichen Interesse des Geschäftsführers der InnoRoute GmbH, Andreas Foglar, den **Sicherheitsbeauftragten** für den SAVE Dienst. Als wichtige Maßnahme zur Verhinderung möglichen Abhörens sind die Router des 6Tree-Netzes so konstruiert, dass sie technisch nicht innerhalb eines sinnvollen ökonomischen Rahmens zum Abhören genutzt werden können (siehe Abschnitt 5).

InnoRoute wird keine Informationen zu den Kommunikationsbeziehungen bei der Nutzung des 6Tree-Netzes und des SAVE-Dienstes sammeln. InnoRoute wird nur die Auslastung des Netzes messen, um gegebenenfalls weitere Ressourcen aufzubauen.

InnoRoute transportiert Nutzerdatenpakete auf vordefiniertem Wege vom Sender zum Empfänger, der die Orte der Kommunikationsteilnehmer und der verwendeten Infrastruktur berücksichtigt, sodass örtlich kurze Wege automatisch bevorzugt werden. Das wird sichergestellt durch ein hierarchisches Netz, dessen nationaler Teil sich ausschließlich in Deutschland

befindet. Es ist analog zum Telefonnetz aufgebaut, wo bei einem Ortsgespräch die Vorwahlen weggelassen werden (siehe Abschnitt 7).

Das Vervielfachen von Nutzerdatenpaketen innerhalb des Netzes von einem Sender zu mehreren Empfängern (Multicasting) wird beim SAVE-Dienst nicht unterstützt, sodass Sender für diesen Anwendungsfall Pakete lokal replizieren und senden müssen.

Jeder Teilnehmer am SAVE-Dienst erhält einen eindeutigen IPv6-Adresspräfix, welcher die Telefonnummer des Teilnehmers enthält (siehe Abschnitt 7). Die Verwendung der Telefonnummer stellt sicher, dass (A) die Nummer eindeutig ist und (B) deutschlandweit (und sogar weltweit) jeder Festnetzanschluss und auch jedes Handy automatisch eine IPv6-Adresse zugeordnet bekommt.

Das Routingnetz von InnoRoute besteht nur innerhalb Deutschlands. Das Netzkonzept und die verwendete Adressvergabe sind im Prinzip weltweit verwendbar (siehe Abschnitt 16). Entsprechende Aktivitäten in den relevanten Standardisierungsgremien wurden bereits angestoßen (siehe Abschnitt 19).

InnoRoute fördert den Aufbau von 6Tree-Netzen und SAVE-Dienst in anderen Ländern, wobei auch dort die Eigenschaften zur Datensparsamkeit, Sicherheit und zum Routing über kurze Strecken eingehalten werden müssen.

4. Routingrelevante Teile des Paketkopfes

Die Router des 6Tree Netzes werten die in Tabelle 1 in Rot gedruckten Felder für die Paketverarbeitung in den Routern aus; die grauen Felder werden nicht genutzt.

06	Type of Service	Flow Label	
Payload Length		Next Header	Hop Limit
AF	Source Address Prefix		
Source Address Prefix			
Source Interface Identifier			
Source Interface Identifier			
AF	Destination Address Prefix		
Destination Address Prefix			
Destination Interface Identifier			
Destination Interface Identifier			

Tabelle 1: Der IPv6 Paketkopf und die vom 6Tree-Netz ausgewerteten Felder

Legende:

- Felder mit festen Werten: 06, AF, AF definieren ein Paket als SAVE-Datenpaket
- Type of Service: beeinflusst die Priorität des Paketes innerhalb eines jeden Routers; kann vom Netz modifiziert werden
- Flow Label: reserviert für SDN-Anwendungen
- Next Header: TCP, UDP (Werte 6, 17) beeinflusst Priorität, ICMP (Wert 58) für Pflichtfunktionen zum Netzwerkmanagement

- Hop Limit: wird zur Fehlerkontrolle innerhalb des Netzes gemäß Standard dekrementiert
- Source Address Prefix: Absenderverifizierung gemäß Abschnitt 6
- Destination Address Prefix: Routing gemäß Abschnitt 9.

5. Sicherstellung der Abhörsicherheit

1. Das Routingverfahren ist deterministisch. Die Weiterleitung erfolgt nach einem offengelegten Algorithmus (Abschnitt 9), der so einfach ist, dass er von einem zustandslosen Logikbaustein in extrem kurzer Zeit ausgeführt werden kann. Es findet kein durch Software gesteuerter Entscheidungsprozess statt, sodass der Weiterleitungsprozess auch nicht durch Manipulation von Software verändert werden kann. Dank des einfachen Weiterleitungsschemas kann die Weiterleitung so schnell erfolgen, dass Datenpakete bereits den Router verlassen, bevor sie zur Gänze eingelaufen sind. Dieses "Cut-Through" genannte Verfahren verzögert bei 1 Gb/s Bandbreite ein Datenpaket typischerweise nur um maximal drei Mikrosekunden und somit weit weniger als das üblicherweise angewandte Verfahren "Store-and-Forward".
2. Der in den 6Tree-Routern enthaltene Prozessor ist nicht an der Paketweiterleitung beteiligt, sondern erledigt ausschließlich Aufgaben wie die Konfiguration und Überwachung des Routers und des Netzes, z.B. für die Anomalie-Erkennung. Er kann keinen Einfluss auf die Wahl des Ausgangsports für weitergeleitete Pakete nehmen.
3. Die "TrustNode"-Router für das 6Tree-Netz wurden von InnoRoute selbst entwickelt, um volle Technologiebeherrschung zu erlangen, sodass Manipulationen durch nicht vertrauenswürdige, hinzugekaufte Funktionsblöcke ausgeschlossen sind. Die TrustNode-Router werden in Deutschland gefertigt und von InnoRoute vor Auslieferung eingehend getestet.
4. Es ist geplant, den Routing-Algorithmus durch vertrauenswürdige Einrichtungen (TÜV, BSI, ...) zertifizieren zu lassen.
5. Die extremkurze Weiterleitungszeit der Datenpakete ist ein weiteres Sicherheitsmerkmal. Ein Nutzer kann die Ende-zu-Ende Übertragungszeit mitprotokollieren; eine starke Abweichung während einer Sitzung kann auf einen Umleitungsversuch auf Layer 1 oder Layer 2 hinweisen, auf den entsprechend reagiert werden kann.
6. Die TrustNode-Router des 6Tree-Netzes sind in hochsicheren Co-Location-Standorten und Rechenzentren mit ISO 27001-Zertifizierung untergebracht. Zwischen diesen werden angemietete Glasfaserressourcen für den Transport genutzt, die exklusiv für den SAVE Dienst verwendet werden. Der Zugang zum 6Tree-Netz erfolgt durch sichere VPN-Tunnel oder dedizierte VLANs über bestehende Netzzugänge.
7. Die 6Tree-Netzstruktur ist für alle SAVE-Kunden offengelegt. Dies enthält sowohl Informationen über die Rechenzentren in denen Stellfläche durch Co-Location angemietet ist als auch die Übertragungsleitungen, deren jeweilige Verzögerungszeit von den Nutzern ebenfalls einsehbar sind. Jeder Nutzer kann also die Standort-zu-Standort-Verzögerungszeit für eine Datenverbindung bereits im Voraus ermitteln.
8. Das 6Tree-Netz ist hierarchisch aufgebaut. Das hat zur Konsequenz, dass Datenströme zwischen lokalen Endpunkten auch lokal bleiben, regionale Datenströme bleiben regional und deutschlandweite Datenströme bleiben in Deutschland.

9. Der SAVE-Dienst wird vom Internet-Dienst strikt getrennt. Der Internet-Dienst umfasst alle IP-basierte Kommunikation außerhalb des SAVE-Dienstes. Die Trennung geschieht entweder durch räumliche Trennung der Netzwerk-Abschlussbuchsen am Teilnehmer-Endgerät (der MaxBox, Abschnitt 15) oder durch eigene Glasfaserstrecken und damit getrennte Teilnehmer-Endgeräte, oder durch logische Trennung, zum Beispiel durch VPN-Tunnel oder eigene VLANs bei gemeinsam genutzten Übertragungsstrecken. Für die Integration auf VPN- oder VLAN-Ebene stellt InnoRoute Best Practice-Anleitungen bereit, um eine versehentliche Anbindung des SAVE-Dienstes an das Internet zu unterbinden.

Trotz aller beschriebenen Sicherheitsmaßnahmen kann InnoRoute nicht vollständig garantieren, dass Dritte über den SAVE-Dienst geleitete Datenströme nicht mitlesen können. Dies betrifft z.B. angemietete Übertragungsleitungen im Zugangsnetz zum 6Tree-Netzwerk. Es ist zum Beispiel technisch möglich Glasfaserstrecken anzuzapfen.

Wir empfehlen unseren Nutzern daher bei geheimen Informationen diese zusätzlich Ende-zu-Ende zu verschlüsseln.

6. Verifizierung des Absenderadresspräfix

In der Verantwortung der InnoRoute GmbH als Netzbetreiber liegt die Sicherstellung des korrekten Absenderadresspräfixes durch organisatorische und technische Maßnahmen. Zu den organisatorischen Maßnahmen gehört ein Prozess zur eingehenden Prüfung neuer Teilnehmer und eine Beratung zu geeigneten Netzwerk-Einstellungen für die komplexeren Fälle eines eigenen VLANs oder VPN-Tunnels im Zugangsnetz.

Die technischen Maßnahmen zur Sicherstellung des korrekten Absenderadresspräfixes sollen insbesondere robust, einfach zu prüfen und mit niedriger Latenz ausführbar sein. So wird in jedem einzelnen Router auf jeder Ebene der Hierarchie sichergestellt, dass alle Datenpakete im 6Tree-Netz auf derjenigen Hierarchieebene erwartbare Absenderadresspräfixe haben. Zudem wird beim Eingang in das 6Tree-Netz der Teilnehmer-Präfix durch geeignete Maßnahmen verifiziert. Bei unerwarteten oder an dieser Stelle nicht erlaubten Absenderadresspräfixen werden Pakete verworfen. Somit hat der Empfänger die Sicherheit, dass der Absender jedes Datenpaketes verifiziert ist und zu einem bekannten SAVE-Teilnehmer gehört und kann dann z.B. bei unerwünscht ankommenden Paketströmen den eindeutig identifizierbaren und lokalisierbaren Absender zur Unterlassung auffordern.

Erste Konsequenz der Absenderüberprüfung ist, dass im Fall eines Angriffes über den SAVE-Dienst kein anonymer Ausgangspunkt vorhanden ist, sondern sich die Quellen – einschließlich ihres Orts – eindeutig bestimmen lassen. Teilnehmer sind dafür zuständig ihre an den SAVE-Dienst angeschlossenen Geräte stets aktuell zu halten und durch geeignete Maßnahmen abzusichern um somit kein Mittler für einen Angriff zu werden, der eindeutig auf sie zurückfallen würde. Angriffe könnten vom Internet über einen sowohl an Internet als auch an SAVE angeschlossenes Gerät geschehen oder nach einem unbemerkten Angriff über SAVE weiter an andere SAVE-Endpunkte. Eine Trennung zwischen Geräten am vertrauenswürdigeren SAVE-Dienst und am nicht vertrauenswürdigen Internet ist daher äußerst wichtig. Wenn ein Chat- oder E-Mail-Dienst ausschließlich über 6Tree-Netz implementiert wird, können

durch geeignete Software zusätzliche Filter erstellt werden, um unerwünschte E-Mails oder unerwünschte Nachrichten aufgrund einfacher positiver Filterlisten herauszufiltern, bevor sie zum Nutzer gelangen, wie z.B. Fishing-Mails.

Die Absenderüberprüfung vereinfacht die Implementierung von Firewall-Regeln. Es können je nach Absender unterschiedliche Überprüfungen durchgeführt werden. Zum Beispiel können (Werbe-)Mails von unerwünschten Absendern bereits in der Firewall gelöscht werden.

Zudem können Fehlkonfigurationen durch das einfache Adressierungsschema einfach aufgedeckt werden, sodass unabsichtliche Einleitungen von externen Quellen in das SAVE-Netz schnell aufgedeckt und unterdrückt werden können.

Um die Überprüfung der Absenderadresspräfixe zu vereinfachen, wird im 6Tree Netz das 64-bit-Präfix der IPv6-basierten Adresse aus der Telefonnummer des jeweiligen Standorts gebildet (siehe Abschnitt 7). Diese Maßnahme erhöht nochmals die Sicherheit durch Vermeidung von manuellen Fehlkonfigurationen. Ein hoher Prozentsatz der Bevölkerung kennt die Struktur der internationalen Telefonnummern bestehend aus Ländervorwahl, Ortsnetzkennung und Anschlussnummer. Meist kennt jeder den Ländercode von Deutschland und Nachbarländern bzw. Urlaubsländern ebenso wie die Vorwahl des eigenen sowie anderer wichtiger Ortsnetze. Mit diesem Wissen kann bereits eine Firewall für das 6Tree-Netz konfiguriert werden – eine Aufgabe die sonst nur Experten vorbehalten ist. Diese Vereinfachung der Konfiguration ermöglicht eine schnellere, billigere und einfachere Überprüfung auf Korrektheit.

Die Überprüfung der korrekten Absenderadresspräfixe wird an Netzgrenzen vertraglich abgesichert. Dafür werden 3 Beispiele angeführt:

Beispiel 1: Teilnehmeranschluss

Ein Homeoffice Teilnehmer hat ein /64 Präfix. Teilnehmer mit großen Standorten und vielen Endgeräten erhalten von InnoRoute eine /60 (16 Subnetze) oder /56-Adresse (256 Subnetze) und sind dann für die Korrektheit der letzten 4 bzw. 8 Bit des Adresspräfixes verantwortlich. Analoges Beispiel dazu sind Nebenstellenanlagen im Telefonnetz.

Beispiel 2: Ländergrenzen

An Ländergrenzen wird InnoRoute vertraglich festlegen, dass der Partner im jeweiligen Land für die Korrektheit aller Senderadresspräfixe verantwortlich ist und dies stichprobenartig auditieren. Auch länderübergreifend ist die Prüfung durch das einfache Schema des 6Tree-Netzes sehr einfach und ohne aufwändige Erweiterungen durchführbar.

Beispiel 3: Zugangsnetze

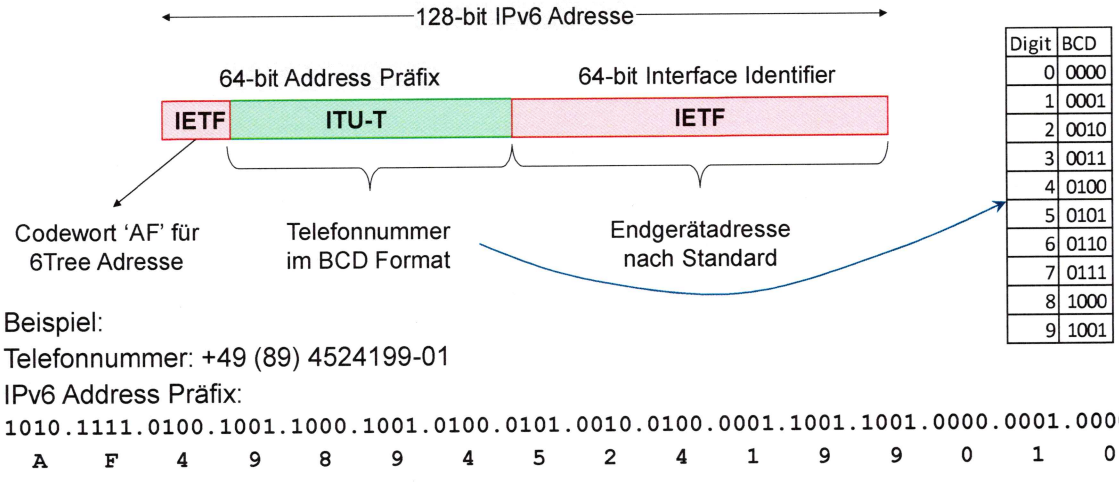
Ein Zugangsnetzbetreiber kann einen SAVE-Dienst anbieten und vom Internet-Dienst durch ein separates VLAN trennen. An der Grenze zu dem von InnoRoute betriebenen 6Tree Kernnetz wird ebenfalls die Pflicht zur Überprüfung der Teilnehmeradresspräfixe vertraglich festgelegt. Der Zugangsnetzbetreiber ist für die Korrektheit der Quelladressen seiner Kunden verantwortlich.

In allen Verträgen werden im Fall der Verletzung der Überprüfungspflicht abgestufte Maßnahmen, wie Warnhinweise bei Kommunikationspartnern bis hin zu zeitweisen Abschaltungen der Schnittstelle an der Netzgrenze festgelegt.

7. Adressierung im 6Tree-Netz

Die 128 Bit lange IPv6-Adresse ist in 2 Abschnitte zu je 64 Bit unterteilt (siehe Bild 1). Gemäß einem Vorschlag[1] der Telekommunikationsbehörde von Südkorea aus dem Jahr 1999 wird in das 64-bit Präfix die Telefonnummer des Anschlusses abgebildet. Der Wert 0xAF (hexadezimal) im obersten Byte der IPv6-Adresse kennzeichnet den 6Tree-Adressbereich. Die restlichen 14 Nibbles des IPv6-Präfixes werden für die Telefonnummer im BCD-Format (Binary Coded Decimal) genutzt. Diese verringerte Code-Dichte erlaubt eine bessere Fehlererkennung im 6Tree-Netz und erleichtert die Darstellung im Netzwerk-Engineering. Der untere 64-bit Teil der IPv6-Adresse wird IPv6-standardkonform mit dem Interface Identifier belegt, also beispielsweise einer modifizierte EUI-64 ID basierend auf der MAC-Adresse des Netzwerk-Adapters. Die Router im 6Tree-Netz nutzen diesen Teil der IPv6-Adresse nicht für die Weiterleitungsentscheidung, sondern nur die oberen 64 Bits.

Für die 6Tree-Adressierung sind zwei Standardisierungsgremien zuständig, die Internet Engineering Task Force (IETF) für Präfix und Interface Identifier und die International Telecommunication Union, Telecommunication Sector (ITU-T) für die Vergabe der Telefonnummern. Bei beiden Organisationen wurde das 6Tree-Konzept eingebracht (siehe Abschnitt 19).



Digit	BCD
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001

Bild 1: Struktur des IPv6-Adresspräfixes im 6Tree-Netz

In Bild 1 ist unten beispielhaft die Abbildung einer Münchner Telefonnummer auf das IPv6 Adresspräfix gezeigt. Die Codierung der 4-bit Felder (Nibbles) erfolgt nach der BCD-Tabelle rechts. Die Werte 10-15 (0xa bis 0xf) sind im Bereich der Telefonnummer illegal. In IPv6-Nomenklatur liest sich diese Adresse:

AF49:8945:2419:901::

[1] https://patents.google.com/patent/KR20010054226A/en

wobei für die 6Tree-Router der Interface Identifier hier auf null gesetzt wurde (reservierter Router-Anycast). Die Endgeräte im 6Tree-Netz eines Standorts unterscheiden sich mindestens durch die Interface Identifier. Adress-Kollisionen können mit Standard-IPv6-Mitteln erkannt und behoben werden.

Die 6Tree-Adressierung wird nicht nur für Endgeräte, sondern auch für die 6Tree-Router selbst verwendet. Zum Beispiel:

- Welt-Top Router Anycast: AF::
- Deutschland-Top Router Anycast: AF49::
- Berlin-Top Router Anycast: AF4930::

Die Verwendung von Router-Anycasts erlaubt Redundanz und steigert damit die Verfügbarkeit des Netzes. Um einen konkreten Router zu adressieren werden manuell zugewiesene Interface Identifier genutzt.

8. 6Tree-Netzwerkstruktur

Das Prinzip des hierarchischen Routingnetzes zeigt Bild 2. Die Routing-Knoten sind hier vereinfacht mit einem Uplink und 3 Downlinks dargestellt, wobei ersterer mit Routern der höheren Hierarchieebene verbindet und letztere zu Routern oder Endgeräten mit den niedrigeren Hierarchieebene.

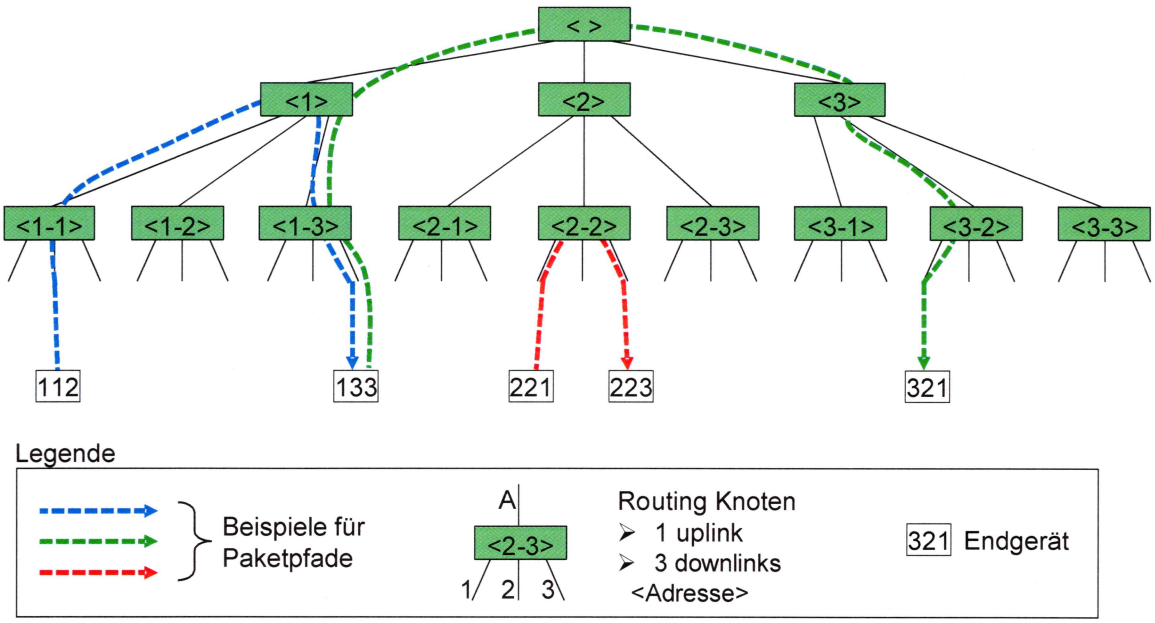


Bild 2: Prinzipielle Struktur des 6Tree-Netzes

Die drei beispielhaft eingezeichneten Paketpfade zeigen, dass Pakete immer über möglichst wenige Hierarchiestufen weitergeleitet werden.

9. Routingalgorithmus

Der Entscheidungen eines 6Tree-Routing-Knotens aus Bild 2 sind in Bild 3 dargestellt. Es zeigt oben den Uplink-Port A, unten die Downlink-Ports 1, 2 und 3. Die Entscheidungswege sind für jede Richtung dargestellt.

Bei Paketen, die von den Downlinks kommen wird zuerst die Quelladresse (IP Source Address) überprüft. Das geschieht für jeden Downlink-Port getrennt, da jeder auch seine eigene Portnummer prüft. Zum Beispiel prüft der Routing-Knoten <1-3> nicht nur seine eigene Adresse; für Datenpakete, die an Port 3 empfangen werden, muss das Absenderadresspräfix 133 lauten. Ansonsten werden die Datenpakete verworfen. Zusätzlich wird die Zieladresse geprüft. Sie darf in diesem Fall nicht das Präfix 133 haben.

Im nächsten Schritt wird für alle vom Downlink erhaltenen Pakete geprüft, ob die Zieladresse (IP Destination Address, siehe Tabelle 1) im durch den Router nach unten aufgespannten Adressbereich liegt. Ist das der Fall, wird zum entsprechenden Downlink-Port weitergeleitet, ansonsten zur nächsthöheren Hierarchieebene[2]. Bei vom Uplink erhaltenen Paketen wird für alle bisher nicht verworfenen Pakete nur geprüft, an welchen Downlink-Port weitergeleitet werden muss.

Zusammengefasst ist das Downstream-Routing eines 6Tree-Routing-Knotens:

- Ist das Paket an meine Hierarchie adressiert?
- Wenn ja, dann richtigen Downlink auswählen, sonst nach oben weiterreichen.

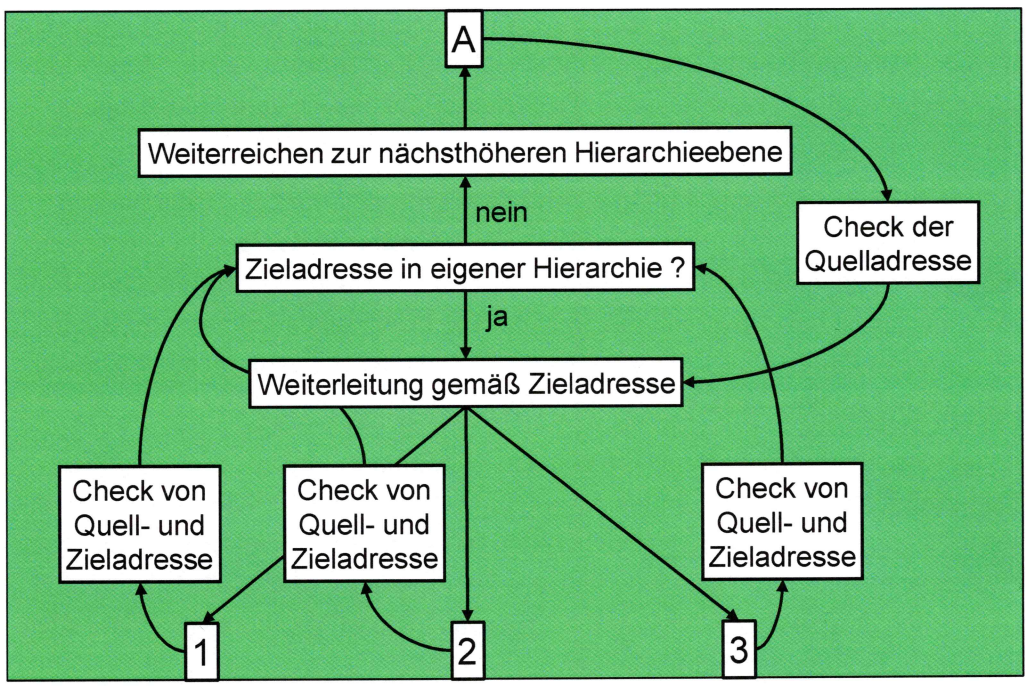


Bild 3: Entscheidungsbaum eines Routing Knotens

[2] Siehe https://datatracker.ietf.org/doc/draft-foglar-ipv6-ull-routing/

Im Fall eines redundanten Knotens mit mehr als einem Uplink kommt eine weitere Entscheidungsebene hinzu, wie im nächsten Abschnitt ausgeführt.

Eine potenzielle Schwachstelle ist im 6Tree-Netz die Einspeisung beliebiger Pakete durch einen Angreifer in Downstream-Richtung, da in Downstream-Richtung nicht in der gleichen Tiefe geprüft werden kann wie in Upstream-Richtung. Um diese Schwachstelle zu verhindern werden die Kernrouter durch InnoRoute in besonders gesicherten Räumen in hochsicheren Rechenzentren untergebracht, wobei die Sicherheitsmaßnahmen umso höher sind je höher die Hierarchieebene der Router ist.

10. Routingalgorithmus bei redundantem Netz

Das 6Tree-Netz kann ganz oder teilweise redundant aufgebaut werden, oder auch mehrfachredundant. Dafür hat der 6Tree-Router neben den Downlink-Ports 0 bis 9 und dem bisher erwähnten Uplink-Port A einen zweiten Uplink: Port B. Dann ist in Upstream-Richtung eine erweiterte Entscheidungsfindung notwendig: das Upstream-Routing.

Auch diese Entscheidungsfindung wird bei 6Tree Netzen autark vom Router selbst getroffen, ohne die Notwendigkeit der üblichen, komplexen Routingprotokolle.

Jeder Router erstellt eine interne Tabelle, in der Absenderpräfixe eingetragen werden. Für jeden Eintrag gibt es nur zwei binäre Informationen, ob vom jeweiligen Uplink ein Präfix erhalten wurde oder nicht. Im Umkehrschluss wird angenommen, dass Zieladressen mit dem jeweiligen Präfix erreicht werden können.

Die Redundanz führt nicht nur zu einer größeren Ausfallsicherheit, sondern auch zu größerem Durchsatz im Netz. Bei Ausfall eines Routers erhöht sich die Last auf den verbleibenden Leitungen und somit nehmen die Paketverluste zu. Das Dienstgütekonzept stellt jedoch sicher, dass wichtige Daten nicht betroffen sind.

Durch die einfache Netzstruktur kann auf ein passives Monitoring zurückgegriffen werden. Die Idee ist, dass Kommunikation bidirektional ist, Endpunkte also in der Regel Datenpakete in beide Richtungen senden und somit eine implizite ständige Verbindungsprüfung läuft. Eine Mitlaufüberwachung speist bei Abwesenheit von Nutzverkehr im Sekundentakt sogenannte Heartbeat oder auch Continuity Check Pakete ein, die wie Nutzpakete weitergeleitet werden, sodass der Ausfall einer Leitung nach 2-3 Sekunden festgestellt werden kann.

Das Erlernen von Absenderpräfixen ist als unveränderliche Einheit implementiert und kann nicht durch manipulierte Software korrumpiert werden. Dadurch, dass berücksichtigte Absenderpräfixe in sehr begrenztem Rahmen gespeichert und basierend auf der lokal konfigurierten Router-Adresse bekannt sind, muss kein Überlauf wie bei Ethernet-Switch-CAMs befürchtet werden. Die Absenderadresspräfixe aller Pakete werden verifiziert (Abschnitt 6), sodass auch der Lernvorgang nicht manipuliert werden kann.

11. Praktischer Aufbau des 6Tree-Netzes

Das 6Tree-Netz besteht aus dem Kernnetz und den Zugangsnetzen.

Das initiale 6Tree-Kernnetz in Deutschland wird mit 9 Standorten in deutschen Großstädten bzw. Metropolregionen realisiert, wie in Bild 4 gezeigt. Der zentrale Standort ist Leipzig aufgrund der geografischen Lage und der Anbindung an die deutschen Glasfasernetze.

Die Reihenfolge der Anschaltung der initialen Metropolregionen wird je nach Kundenanfrage festgelegt. Ebenso die Anschaltung weiterer Metropolregionen.

Die Standorte des 6Tree-Kernnetzes sind Rechenzentren, die Colocation-Dienst anbieten. Dazu gehört die Anmietung von Stellfläche, Racks mit Stromversorgung, Kühlung etc. und auch die Anbindung an Glasfasernetze. Für 6Tree-Netze werden hochsichere, nach ISO 27001 zertifizierte Rechenzentren ausgewählt.

Die Verbindungen zwischen den Standorten werden durch angemietete, dedizierte Glasfasern bzw. Wellenlängen oder Farben (DWDM) realisiert.

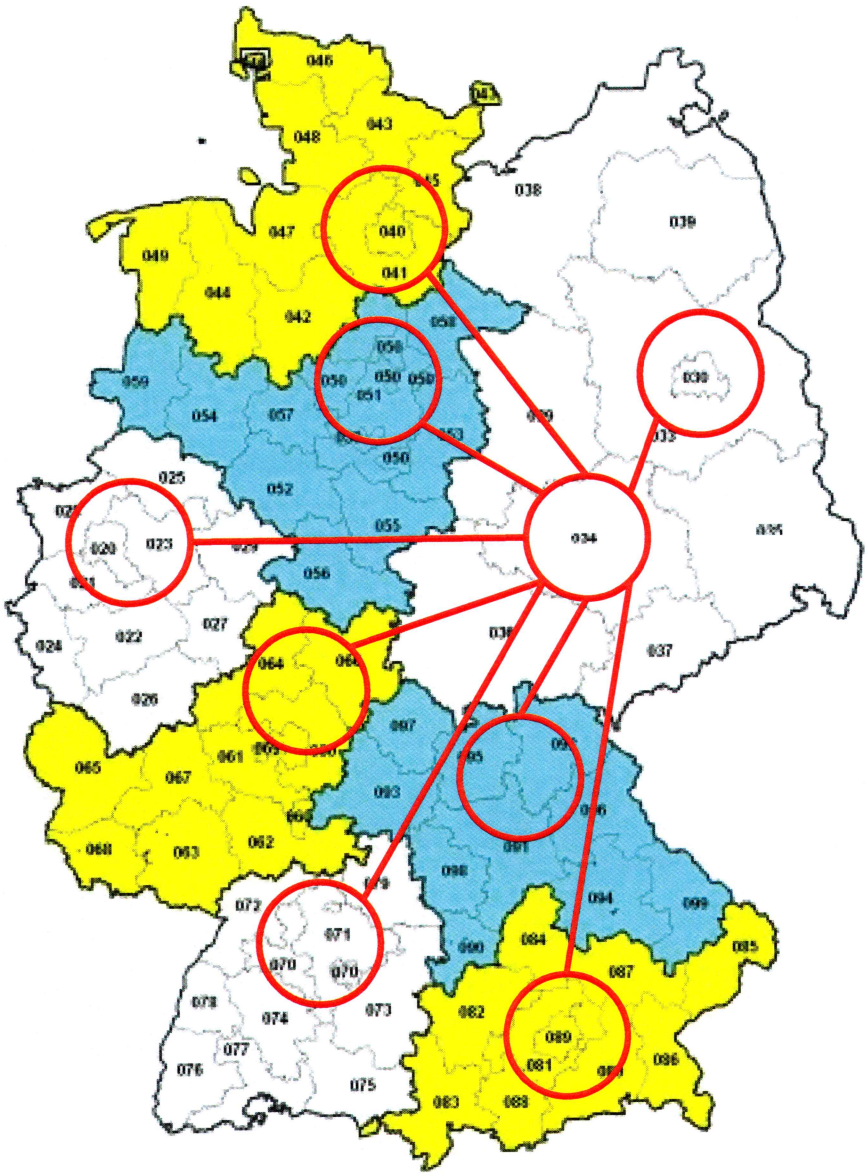


Bild 4: Geplantes 6Tree-Netz in Deutschland

Teilnehmer mit Glasfaseranbindung und/oder Präsenz in Rechenzentren werden direkt an das 6Tree-Kernnetz angeschlossen (Abschnitt 13). Teilnehmer mit DSL-, Kabel- oder PoN-Zugangstechnologie werden zunächst an die nächstgelegene Metropolregion mittels VPN und später über VLAN zugeführt (siehe Abschnitt 14).

Da die Router eine Grundlatenz von nur wenigen Mikrosekunden haben, ist im 6Tree-Kernnetz die minimale Laufzeit der Pakete praktisch nur durch die Ausbreitungsgeschwindigkeit in den Glasfaserleitungen (ca. 5 µs/km) bestimmt. Bei der Metropolregion ist die typische einfache Distanz ca. 100 km (0,5 ms), bei einer nationalen Verbindung ist mit typischerweise ca. 500 km (2,5 ms) zu rechnen. Die Antwortzeiten (Round Trip Times, RTT) sind entsprechend 1 ms bzw. 5 ms.

Die Grundlatenz der Router trifft dann zu, wenn es zu keinen Kollisionen von Paketen an einem Ausgang kommt. Sonst gibt es Wartezeiten, die durch Priorisierung von Paketen minimiert und in der TSN-Klasse sogar ganz vermieden werden können.

12. Sicherer Zugang an das 6Tree-Netz

Der SAVE-Dienst ist wie auch der Internet-Dienst IP-basiert. Das hat den Vorteil, dass alle IP-basierten Anwendungen über die Transportprotokolle (TCP, UDP, …) auch über SAVE funktionieren. Der Anwender kann beide Dienste gleichzeitig nutzen; die Auswahl von SAVE geschieht lediglich durch Verwendung der speziellen IPv6-Adresse, die mit 0xAF beginnen.

Unterschiedlich ist die Adressfindung, die im Internet bei der Verwendung von global gültigen Domainnamen über DNS (Domain Name Service) erfolgt, im SAVE-Netz durch lokal gepflegte Kommunikationspartner-Listen entsprechend einem persönlichen Telefonbuch.

Die Trennung von SAVE-Datenpaketen und Internet-Datenpaketen erfolgt beim Teilnehmer in der MaxBox, (Bild 5), die jeweils eigene RJ-45 Buchsen für SAVE- und Internet-Dienst bietet (Bild 8).

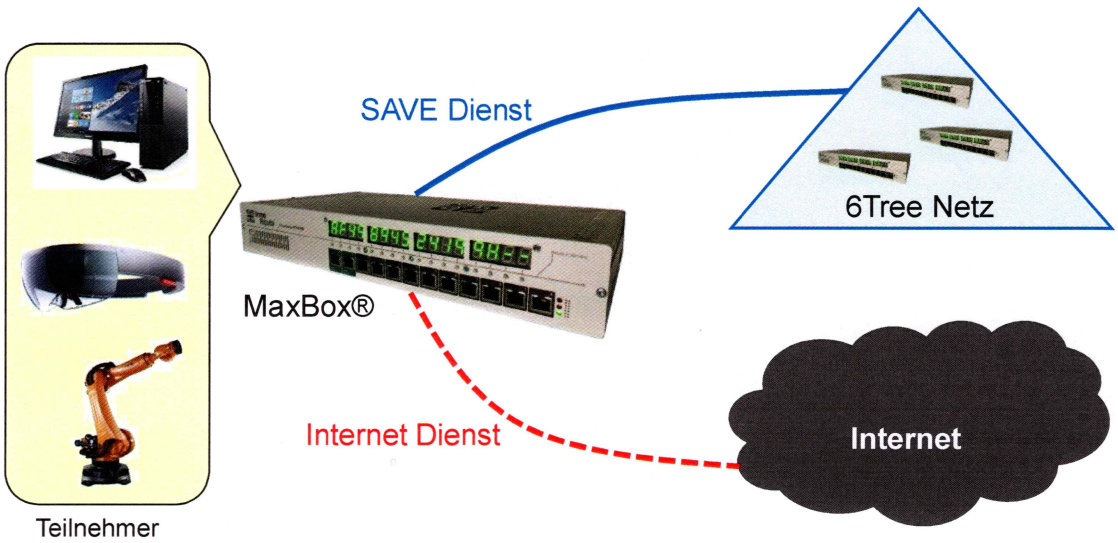


Bild 5: Trennung von SAVE-Dienst und Internet

Die Trennung von SAVE-Datenpaketen und Internet-Datenpaketen erfolgt beim Teilnehmer in der MaxBox, (Bild 5), die jeweils eigene RJ-45 Buchsen für SAVE- und Internet-Dienst bietet (Bild 8).

13. Anschluss eines mittelständischen SAVE-Teilnehmers

Die Konfiguration anhand eines mittelständischen SAVE-Teilnehmers ist in Bild 6 dargestellt. Das mittelständische Unternehmen hat bestenfalls bereits ein Rack in einem Rechenzentrum untergebracht, in dem auch ein 6Tree-Rack von InnoRoute steht. Das Unternehmen mietet einen Gigabit-Port an einem 6Tree-Router entsprechend seiner Telefonnummer an. Die beiden Racks werden mit einem sogenannten Cross-Connect Kabel verbunden, auf dem ein VLAN für den SAVE-Traffic eingerichtet ist. Dieses VLAN endet im Hauptstandort des Kunden, wo ein MaxBox-Router den SAVE-Dienst vom Internet-Dienst trennt (siehe Bild 5).

Beim Zugang des Kunden zum Rechenzentrum handelt es sich meistens um einen Ethernet-basierten Anschluss, wie zum Beispiel den EthernetConnect-Service der Deutschen Telekom oder den Connect-LAN-Service von M-Net o.ä. Für die SAVE-Datenpakete wird ein eigenes VLAN eingerichtet, um diese Datenpakete vom Internet-Dienst zu trennen. Für das VLAN können Service Level Agreements festgelegt werden, um die SAVE-Anbindung hochqualitativ durchzuführen. Die Datenpakete des SAVE-VLANs werden über das Cross-Connect Kabel zum 6Tree-Router weitergeleitet.

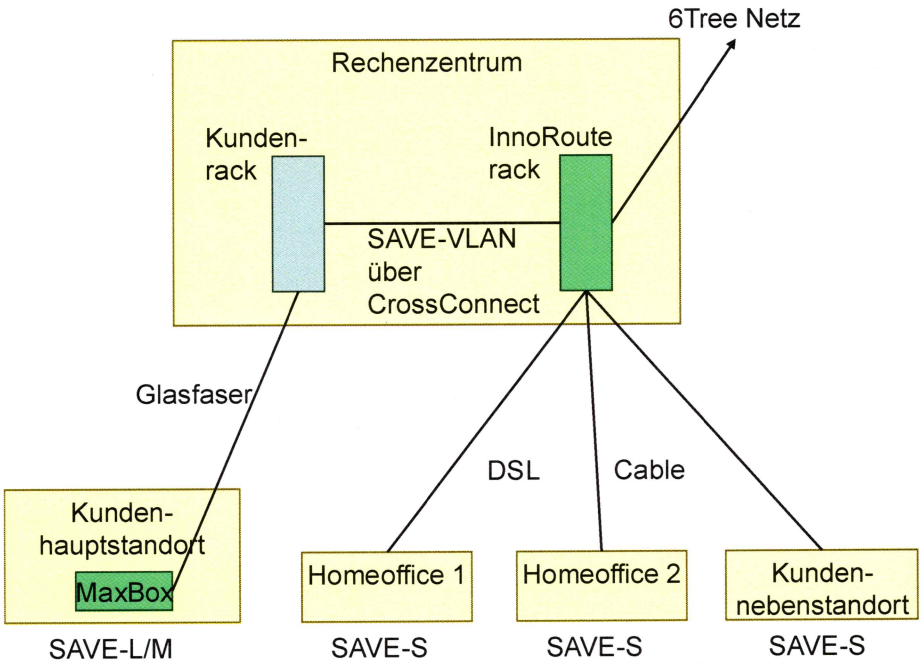


Bild 6: Anschluss eines mittelständischen Unternehmens an den SAVE-Dienst

In Bild 6 sind neben dem Hauptstandort des Kunden noch ein Nebenstandort und zwei Homeoffices eingezeichnet, die alle im Telefonnummernbereich des Hauptstandorts liegen. Sie verwenden statt der MaxBox z.B. eine Fritz!Box der Fa. AVM o.ä. zur Trennung der Dienste. Dazu erhalten diese eine spezielle Firmware, die den SAVE-Dienst am LAN-Port 3 ausgibt.

Alternativ könnte auch eine „AdapterBox“ von InnoRoute zum Einsatz kommen, die einen sicheren VPN Tunnel aufbaut. Diese „kleinen“ Zugänge werden als SAVE-S bezeichnet.

14. Anschlussarten

Tabelle 2 gibt eine Übersicht über die Anschlussoptionen.

Anschlusstyp	Anschluss an	Technologie	Latenz	Medium	Verfügbarkeit
SAVE-L / M	6Tree Kernnetz	VLAN	gering	Glasfaser	sofort
SAVE-S	Zugangsnetz	VPN	hoch	Kupfer/ Kabel	sofort
		VLAN	mittel		2022
SAVE-T	LTE	-	-	Funk	2023

Tabelle 2: 6Tree-Netzzugangs-Optionen

SAVE-L und SAVE-M werden mit einer **MaxBox** realisiert, SAVE-S mit einer Fritz!Box o.ä. mit spezieller Firmware oder AdapterBox.

In Bild 7 sind alle aktuell berücksichtigten Zugangsarten eingeführt; für SAVE-S die beiden Optionen VPN-Tunnel oder VLAN.

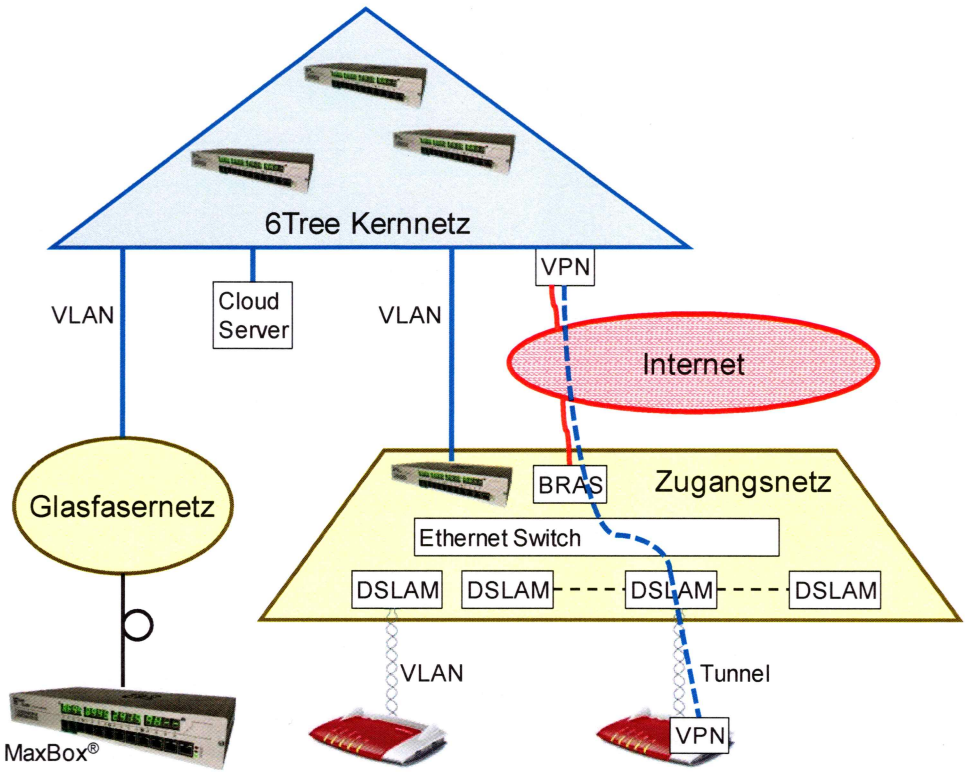


Bild 7: 6Tree Netzzugang

Der Zugang an das 6Tree-Netz über **DSL**, **Koaxialkabel** oder auch **PON** (SAVE-S) ist vorerst nur über das Internet möglich. Der heutige Stand der Technik für den DSL-Fall ist in Bild 7 beispielhaft mit der Fritz!Box rechts gezeigt: die Zugangsmultiplexer (DSLAM) sind über eine Ethernet-Switch-Funktion mit dem BRAS-Router verbunden, der den Übergang zum Internet bildet. Für die Anbindung eines Teilnehmers an das 6Tree-Kernnetz wird ein VPN-Tunnel vom Home-Router über das Internet bis zur VPN-Terminierung am 6Tree-Kernnetz eingerichtet. Letztere wird netzseitig durch vertrauenswürdige und leistungsfähige **VPN**-Router (beispielsweise der Fa. LANCOM) realisiert.

Die technisch bessere Lösung für Zugangsnetze ist in Bild 7 an der linken Fritz!Box (rotes Endgerät in der Mitte) gezeigt. Im Zugangsnetz wird ein spezieller TrustNode platziert, der den Anschluss an das 6Tree-Kernnetz sicherstellt. Im Zugangsnetz wird ein eigenes **Service-VLAN** eingerichtet; jeder Teilnehmer, der daran teilnehmen möchte und eine entsprechendes Telefon-Präfix hat, wird für dieses VLAN freigeschaltet. Mit dieser Lösung ist der Tunnel über das Internet nicht mehr notwendig, und Latenz und Jitter sinken signifikant ab. Referenzwerte werden im Betrieb von InnoRoute gesammelt und als Erwartungswerte für die Kunden bereitgestellt werden. Bei DSL bleibt als wesentliche Verzögerung jedoch noch das DSL-Interleave-Delay von ca. 10 ms pro Richtung.

Der Zugang über Mobilfunknetze (SAVE-T) wird zu einem späteren Zeitpunkt angeboten.

In Bild 7 ist auch ein **Cloud-Server** eingezeichnet, der am Kernnetz angeschlossen ist. Es bietet sich an, dedizierte Cloud-Server direkt an das 6Tree-Netz anzuschließen, um kurze Latenzzeiten und hohe Datensicherheit zu erzielen. Diese Cloud-Server erhalten ebenso 6Tree-Adressen die entsprechend gefiltert werden können. Der Cloud Server kann von InnoRoute betrieben werden, vom Rechenzentrum oder auch von existierenden Cloud-Anbietern.

Bei der Verwendung von Cloud-Servern werden die Telefonnummern der entsprechenden Rechenzentren genutzt.

15. Router beim Teilnehmer

Die Anschaltung an das 6Tree-Netz erfolgt in den Optionen SAVE-L und SAVE-M über die MaxBox von InnoRoute, ein um zusätzliche Funktionen erweiterter 6Tree-Router für den Einsatz am Rand des Zugangsnetzes.

Die **MaxBox** wird z.B. wie in Bild 8 gezeigt zwischen Modem und existierender Infrastruktur (z.B. Firewall) geschaltet, sodass Port A mit dem Modem verbunden wird, Port B mit der Firewall. Die MaxBox leitet alle bisherigen Datenströme von Port A zu Port B und umgekehrt, sodass existierende Dienste unverändert weiterlaufen. Dieses Verhalten ist grundlegend anders als bei den oben beschriebenen 6Tree-Routern in Weitverkehrsnetzen, die Port B zu Redundanzzwecken nutzen und somit eine andere Logik enthalten.

Die **MaxBox** ist mit nur ca. 3 µs Grundlatenz zwischen zwei Ports extremschnell, sodass das Einfügen in den vorhandenen Netzzugang keine wesentliche Auswirkung auf die Ende-zu-Ende-Latenz hat. An den sicheren Ports 0…9 werden SAVE-Pakete ausgekoppelt. Hier können Server und PCs Zugang an das 6Tree-Netz erhalten.

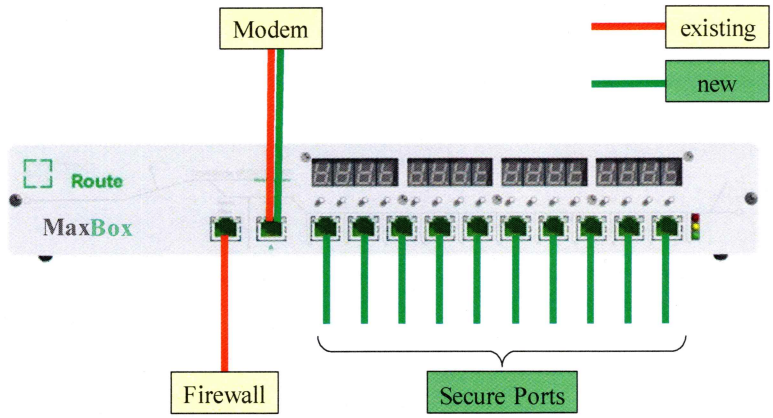


Bild 8: MaxBox-Ports

Um die Konfiguration zu vereinfachen konfiguriert sich die **MaxBox** nach Anbindung an das 6Tree-Netz automatisch selbst und zeigt die Router-Adresse am eingebauten Display an. Beim Anschluss ist das Router-Adresspräfix durch den SAVE-Kunden gegen die eigene Telefonnummer zu prüfen und notwendigenfalls manuell zu korrigieren. Dies gelingt, da das Router-Adresspräfix aus der Telefonnummer abgeleitet ist. Hat zum Beispiel der Telefonanschluss der Firma die Nummer +49-89-4524199-0 und ist SAVE-L gewählt, so lautet die korrekt angezeigte Router-Adresse AF49.8945.2419.90H-. Das ‚H' (Hierarchie) bezeichnet die von der **MaxBox** ausgewertete Stelle. An den Ports 0…9 angeschlossene Geräte erhalten (über DHCPv6 und Prefix Delegation) die Adresspräfixe

AF49.8945.2419.9000 bis AF49.8945.2419.9090

zugewiesen. An jedem Downlink könnte wieder eine MaxBox angeschlossen werden, um bis zu 100 Ethernet-Subnetze anzubieten. Hierbei wäre Port B der angeschlossenen MaxBoxen jeweils nicht nutzbar.

Im Falle eines SAVE-M Anschlusses würde die MaxBox-Adresse

AF49.8945.2419.900H

konfiguriert und angezeigt. Hier können 10 Ethernet-Subnetze generiert werden.

Von außen kann man in beiden Fällen direkt mit allen Endgeräten des Teilnehmernetzes kommuniziert werden, sofern dies in der **MaxBox** für den jeweiligen Teilnehmer erlaubt ist.

In der **MaxBox** wird die Firewall über eine Konfigurationsschnittstelle für jeden Port konfiguriert, wobei für verschiedene Absenderadressen Durchlassfilter und/oder Sperrfilter (Positiv- oder Negativfilter) einstellbar sind, um die Zugriffsrechte auf die gewünschten Partner einzugrenzen. So kann man sicherstellen, dass z.B. die Entwickler eines anderen Standortes auf die Produktivserver zugreifen können, die Vertriebsmitarbeiter auf die Marketingserver usw., sie jedoch nicht untereinander Ressourcen nutzen dürfen. Das gilt entsprechend auch für Mitarbeiter im Homeoffice. Auch Kunden und Geschäftspartnern kann (zeitweise) Zugriff auf bestimmte Ressourcen freigeschaltet werden. Auch globale Filter können konfiguriert werden, zum Beispiel um nur Partnern aus Deutschland oder aus der Region den Zugriff zu erlauben.

Bei der SAVE-S Option erfolgt die Anschaltung über eine von InnoRoute speziell konfigurierte Fritz!Box (o.Ä.) oder die AdapterBox von InnoRoute. Bei SAVE-S wird ein /64 Präfix zugewiesen, das die Telefonnummer enthält und ggf. mit Nullen aufgefüllt wird.

16. Globale 6Tree-Netze

Die Adressierung der 6Tree-Router und -Endgeräte ist dank der Verwendung der Telefonnummer weltweit möglich. Man kann sich das weltweite 6Tree-Netz wie eine Pyramide vorstellen (Bild 9). Die Dreiecke innerhalb des globalen 6Tree Netz sind ausgebaute Bereiche, wie zum Beispiel das von InnoRoute betriebene Kernnetz Deutschland, das globale Kernnetz, ein Zugangsnetz in Deutschland – zum Beispiel von einem Stadtwerk betrieben, sowie Firmennetze im In- und Ausland – hier beispielhaft China. In verschiedenen Grautönen sind die redundanten Ebenen eingezeichnet.

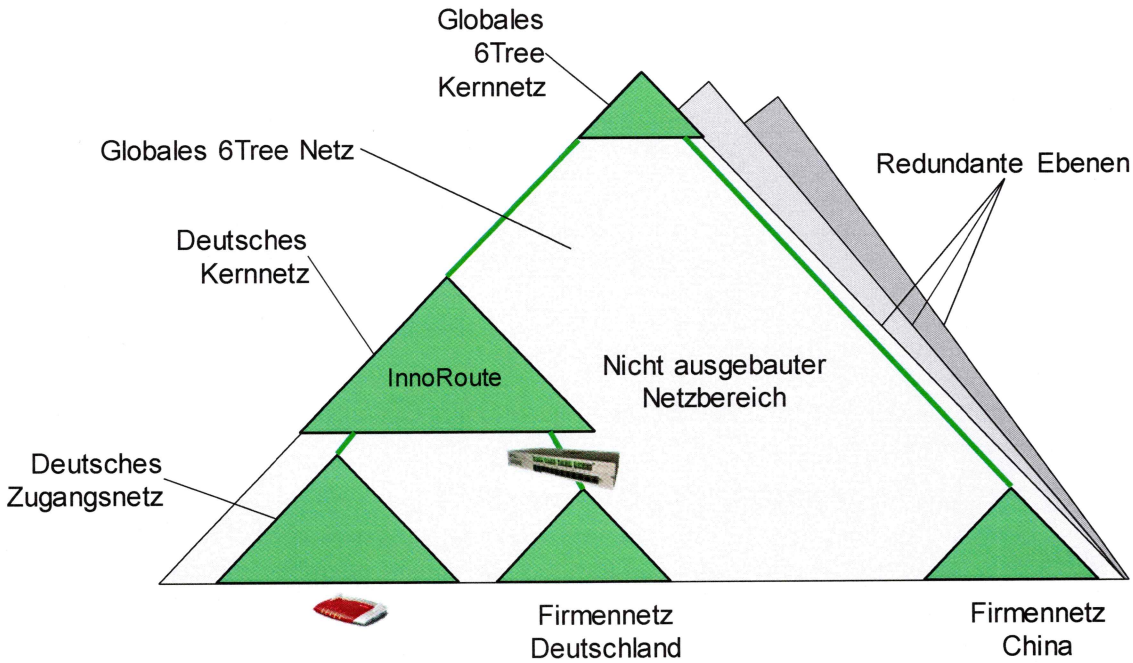


Bild 9: Globales 6Tree-Netz im Teilausbau

Zwischen den von verschiedenen Betreibern betriebenen Teilbereichen sind Übergabeschnittstellen, an denen die 6Tree-Regeln eingehalten und auditiert werden müssen. Am Übergang zwischen InnoRoute und der Firma, die ein lokales 6Tree-Netz betreibt ist in Bild 9 eine Max-Box eingezeichnet, der Teilnehmer am deutschen Zugangsnetz hat eine spezielle Fritz!Box (vgl. Bild 7).

17. Ausfallsicherheit

InnoRoute platziert Reservegeräte an jedem Colocation Standort. Der Austausch eines defekten Routers gegen bereitstehende Backup-Systeme kann vom lokalen Bedienpersonal durchgeführt werden, ein Service der von den meisten Rechenzentren unter dem Begriff „Remote Hands“ rund um die Uhr angeboten wird.

Möglich ist dies durch die automatische Konfiguration der 6Tree-Router von InnoRoute. Die Anreise eines InnoRoute-Experten ist nicht erforderlich, und die maximale Ausfallzeit reduziert sich von ca. 1 Tag auf ca. 1 Stunde.

Bei der Auswahl der Colocation-Standorte achtet InnoRoute auf diese Punkte:

- Netzanbindung mit ISO-OSI Layer 1 oder 2
- ISO 27001[3]-Zertifizierung
    - Garantiert bestmöglichen Schutz vor Störungen, technischen Fehlern, Spionage und Informationsmissbrauch. Erfüllt Sicherheitsanforderungen nach §11 des Bundesdatenschutzgesetzes, der die Erhebung, Verarbeitung und Nutzung personenbezogener Daten regelt.
- Ausfallsicherheit: mindestens Tier 2

Verfügbarkeits-klasse	Redundanz	Verfügbarkeit	Kumulierte Ausfall-Wahrscheinlichkeit pro Jahr
Tier 1	N* keine Redundanz	99,67 %	28,8 Stunden
Tier 2	N+1	99,75 %	22,0 Stunden
Tier 3	2 N System	99,98 %	1,6 Stunden
Tier 4/ Tier 3+	2 (N+1)	99,99 %	0,8 Stunden

Tabelle 3: Verfügbarkeitsklassen von Rechenzentren

- Mindestens mit 3 DCSA Sternen zertifiziertes Data Center nach „eco Datacenter Star Audit[4]“
    - Ein mit 3 Sternen zertifiziertes Data Center eines Betreibers bietet bereits eine ausreichende Sicherheit und Verfügbarkeit an. Ein erster Fehlerfall ist abgedeckt, bei einem Stromausfall steht eine Netzersatzanlage (NEA) zur Verfügung.
- Eco: ein TrustNode benötigt typischerweise bei Volllast 25W; bei 20 Geräten pro Rack: 500W; die ist viel weniger als die 2 kW, die üblicherweise zur Verfügung gestellt werden.

Durch redundanten Netzaufbau kann auch bei Unterbringung der 6Tree-Router in verschiedenen Tier-2-Rechenzentren eine Tier-4-Verfügbarkeit erzielt werden.

Innerhalb eines Rechenzentrums stellt InnoRoute sicher, dass redundante Router an unabhängigen Stromversorgungen (Sicherungen) angeschlossen werden.

[3] https://www.tuev-sued.de/management-systeme/it-dienstleistungen/iso-27001/white-paper-iso-27001
[4] https://www.eco.de/themen/datacenter/dcaudit/ueber-dcsa/

18. Netzmanagement

InnoRoute verwaltet das 6Tree-Netz und stellt den aktuellen Netzzustand allen SAVE-Kunden kontinuierlich zur Verfügung. Diese können den aktuellen Netzausbau, die Netztopologie, die Router und ihren jeweiligen Standort, die Übertragungsstrecken zwischen den Routern und ihre Eigenschaften jederzeit einsehen. InnoRoute ermittelt mit speziellen ICMP-Nachrichten permanent den Zustand der Router und die Laufzeiten zwischen den Routern und stellt die daraus gewonnen Ergebnisse den SAVE-Kunden zur Verfügung.

Das Netzwerkmanagement ist in einem separaten Dokument beschrieben.

19. Standardisierung

InnoRoute hat 6Tree/SAVE bei den 2 relevanten Standardisierungsgremien eingebracht:

- Die IETF (Internet Engineering Task Force) ist für das Präfix AF (o.Ä.) zuständig. Dort wurde ein Internet Draft eingereicht: https://datatracker.ietf.org/doc/draft-foglar-ipv6-ull-routing/
- Die ITU-T Study Group 2 ist für die Standardisierung von Telefonnummern zuständig.

Beide Organisationen waren interessiert und offen für Neuerungen. Beide empfahlen erst dann konkrete Vorschläge einzubringen, wenn es praktische Ergebnisse gibt.

InnoRoute plant daher eine temporäre Zuordnung des Präfixes AF49/16 bei RIPE/ IETF zu beantragen, sobald das nationale 6Tree-Netz einige Teilnehmer unterstützt. Falls später das 6Tree-Netz z.B. auf Österreich erweitert wird, sollten die Partner dort das Präfix AF43/16 beantragen; analog dazu kann in jedem weiteren Land ein Präfix mit der Länderkennzeichnung beantragt werden.

Im Fall, dass der 6Tree-Code ‚AF' durch die Standardisierung verändert wird, können die 6Tree-Router entsprechend angepasst werden.

20. Kundendaten

InnoRoute nutzt seit der Gründung einen in Deutschland befindlichen Datenspeicher bei STRATO in Berlin. Dieser wurde immer wieder um weitere Bereiche vergrößert. Insbesondere Kundendaten wurden von Beginn an dort abgelegt. Für die gewerblichen (B2B) Kunden des SAVE-Dienstes wird ein neuer, eigens verschlüsselter Bereich angelegt und der Zugriff auf die unbedingt notwendigen Mitarbeiter und Prozesse beschränkt und protokolliert werden. Die Inhalte werden regelmäßig auf ihre Aktualität und weiterhin gültige Gründe für ihre Speicherung geprüft werden. Nicht mehr für den ursprünglichen Zweck erhobene Daten werden dann sofort gelöscht.

Für den Fall künftiger Erweiterung auf Privatkunden (B2C) wird InnoRoute die Zusammenarbeit mit Partnerfirmen anstreben, die auf die Verwaltung großer Kundenzahlen spezialisiert sind um den Anforderungen an Datensicherheit, Datenschutz und Kundenservice Sorge zu tragen.

21. Terminologie

- **SAVE (Source Address Verification)** ist die ein Routing-Dienst, der über das 6Tree-Routingnetz abgewickelt wird.
- **6Tree** ist ein Konzept für ein hierarchisch aufgebautes Routing-Netz, basierend auf IPv6 mit einer speziellen Adressierung.
- **Colocation** ist ein Service, den viele Netzbetreiber und Data-Center anbieten. Fremdanbieter können Stellplatz, Strom und Übertragungskapazität anmieten, um eigene Geräte aufzustellen. Es wird hohe Sicherheit geboten: Zutrittskontrolle, Fernüberwachung, Notstromversorgung, Brandschutz, Klimaanlage etc.
- **Tier 1...4** sind standardisierte Verfügbarkeitsstufen für Rechenzentren
- **CPE (Customer Premises Equipment)** sind Geräte, die beim Teilnehmer installiert sind, wie beispielsweise Fritz!Box, MaxBox, Modem und AdapterBox.
- **CO (Central Office)** ist auf Deutsch das Vermittlungsamt. Gemeint sind hier Installationen im Weitverkehrsnetz, wie die 6Tree-Router in öffentlichen Colocation-Racks und Datacenter-Racks.
- **MaxBox®** ist ein CPE-Router der InnoRoute GmbH.
- **TrustNode®** ist ein CO-Router der InnoRoute GmbH.
- **MPLS (Multi-Protocol Label Switching)** ist eine Technologie, um feste Verbindungen z.B. über Internet-Router einzurichten. Dafür wird zwischen zwei Endpunkten ein vordefinierter Pfad (in der praktischen Umsetzung meist manuell) eingerichtet, der auch reservierte Bandbreite haben kann.
- **VLAN (Virtual LAN)** erlaubt ein physikalisches Ethernet-Netzwerk in mehrere, logisch unabhängige Netze aufzuteilen. Zum Beispiel kann ein Firmennetz mehrere VLANs haben, für Entwicklung, Vertrieb, Administration usw.
- **VPN (Virtual Private Network)** beinhaltet Tunneltechnologien, um z.B. einen PC von außen über das Internet an ein Firmennetz anzubinden. Hier werden VPN-Tunnel eingesetzt, um einen SAVE-Teilnehmer über das Internet mit dem IPv6-basierten 6Tree-Netz zu verbinden. Ein VPN-Tunnel kann optional verschlüsselt werden.
- **IPv6-Adresspräfix** bezeichnet den oberen Teil der IPv6 Adresse, maximal 64 Bits. Für SAVE wird ein spezielles Mapping verwendet. Der zweite, 64-bit lange untere Teil der IPv6 Adresse, der Interface Identifier, ist davon unbeeinflusst.
- **Zugangsnetz (Access Network)** ist das öffentliche Netz, an dem Internet-Teilnehmer angebunden sind. Meist nutzen sie DSL-Technologien oder Cable Modems, vermehrt auch Glasfaser.
- **BRAS (Broadband Remote Access Server)** ist ein Router, der das Zugangsnetz abschließt und mit dem öffentlichen IP Kernnetz (auch IP-Backbone genannt) verbindet.
- **TSN (Time Sensitive Networking)** ist eine Netzwerktechnologie bei der Datenpakete mit konstanten, kleinen Latenzzeiten transportiert werden.

Im Text werden beispielhaft einige Produkt- und Firmennamen erwähnt, an denen InnoRoute keinerlei Rechte hält, wie z.B. AVM, Fritz!Box, LANCOM und STRATO.

Umsetzungserklärung

Hiermit erkläre ich als Sicherheitsbeauftragter der InnoRoute GmbH, dass die in diesem Dokument beschriebenen Maßnahmen im Rahmen eines einjährigen Testbetriebes umgesetzt werden. In dem Testbetrieb nehmen nur Pilotkunden teil, die auf diesen Umstand hingewiesen werden.

München, 30. September 2020 Unterschrift und Firmenstempel

A. Foglar

InnoRoute GmbH
Marsstraße 14a, 80335 München
www.innoroute.de

Andreas Foglar

Geschäftsführer und Sicherheitsbeauftragter

InnoRoute GmbH