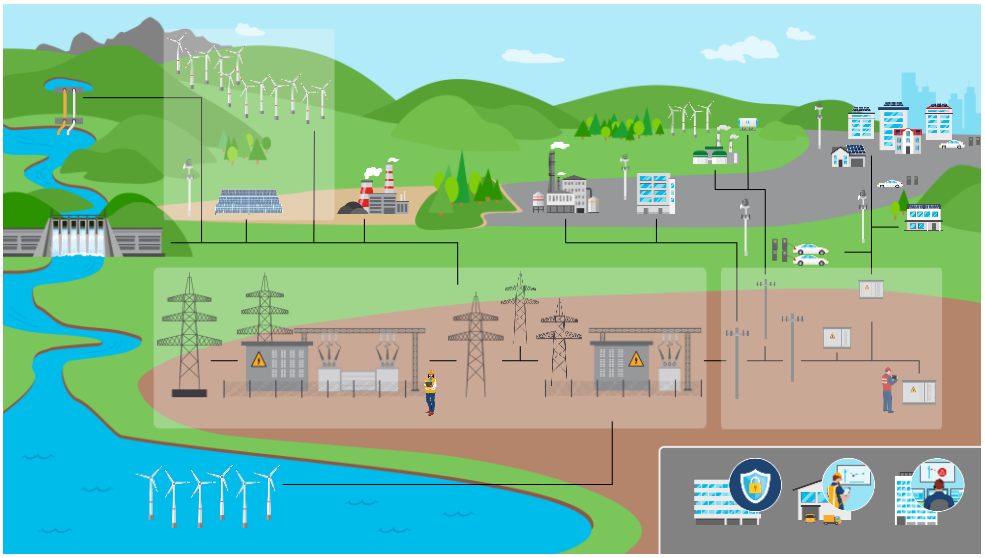
Cisco Digital Utilities: Weitverkehrsnetze für Energienetzbetreiber

Weitverkehrsnetze für Energienetzbetreiber



Energiewende und Telekommunikation

Die Steuerung elektrischer Stromnetze baut insbesondere in Zeiten der Energiewende auf Kommunikationsnetzen auf. Während sich die Weitverkehrsnetze im Bereich der Höchst- und Hochspannung meist auf eigene Kabelnetze stützen, sind Netzwerkinfrastrukturen in der Mittel- und Niederspannung oftmals über funkbasierte Technologien, DSL oder Powerline realisiert. Je nach Situation kommen Leistungsangebote öffentlicher Provider im Mobilfunk oder DSL-Bereich zum Einsatz.

In diesem Dokument wird der Bereich der Höchst-, Hoch- und Mittelspannung mit eigenen Kabelnetzen betrachtet. Lösungskonzepte im Bereich der Niederspannung oder im Umfeld funkbasierter Technologien sind in einem separaten Dokument beschrieben.

Moderne Weitverkehrsnetze, die die Kommunikation zwischen den Anlagen sowie von den Anlagen zu den zentralen Leitstellen herstellen, müssen unterschiedlichen Anforderungen genügen. Neben der Übertragung vieler historisch etablierter Kommunikationsarten müssen auch Anforderungen für den mittel- bis langfristigen Einsatz beachtet werden. Technologieentscheidungen sind hierbei für Zeiträume von mehr als einer Dekade zu treffen und sollten auch über längere Zeit Zukunftssicherheit gewährleisten.

Ähnlich wie bei der Entscheidung für PDH- und SDH-Systeme (Plesiochrone und Synchrone Digitale Hierarchie) in der Vergangenheit, sind auch heute moderne Carrier-Infrastrukturen ein Leitbild für Auswahl und Fokussierung der Weitverkehrsinfrastruktur eines Energienetzbetreibers. Technologische Grundlagen und Protokolle im Carrier-Umfeld stellen hier die Basis für eine zukunftssichere Entscheidung dar. Unbedingt erforderlich ist die Anpassung der Kommunikationsnetze an die Anforderungen eines Energienetzbetreibers, als ein wichtiger Grundbaustein für die Bereitstellung der notwendigen Kommunikationsdienste.

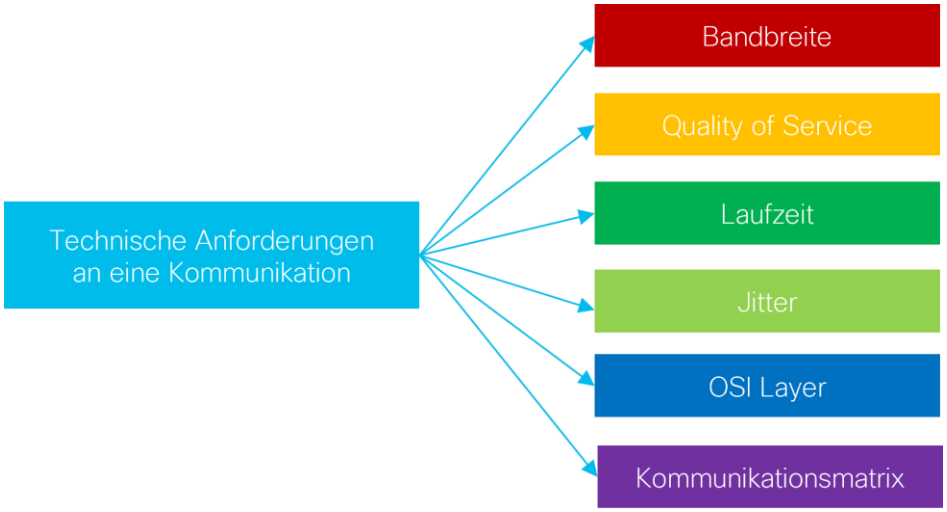
Im Folgenden stellen wir verschiedene Gedankengänge zur Herleitung von Lösungskonzepten dar. Zu Beginn ist es erforderlich, die notwendigen Funktionen oder auch Fähigkeiten zum Transport der Anwendung zu definieren. Sie stellen die Grundlage für die Technologieauswahl dar. Nach der Beschreibung der Fähigkeiten möchten wir einen Überblick über die Technologie geben und heutige Umsetzungen bzw. zukünftige Trends im Ausblick darstellen. Die Anforderungen aus Sicht der Security, aber auch die operationellen Aspekte, sind ebenfalls in einem Kapitel dargestellt.

Fähigkeiten und Anforderungen

Die notwendigen Fähigkeiten, die eine Kommunikationsinfrastruktur zur Verfügung stellen muss, lassen sich in zwei Anforderungsbereiche differenzieren.

- Die erste Gruppe beinhaltet alle Anforderungen, die spezifisch aus dem Betrieb eines Energienetzes heraus entstehen. Sie sind im Allgemeinen wenig vergleichbar mit Ansätzen aus anderen Industriezweigen. Beispiele wären hier die Kommunikation gemäß IEC 60870-5-104 oder der Austausch zwischen Schutzgeräten zur Absicherung der Netzwerkinfrastruktur, z.B. Kabel, Freileitungen und Transformatoren.
- Die zweite Gruppe beinhaltet Anforderungen, die in dieser Form allgemeingültiger als Gruppe eins sind und auch in anderen Industriezweigen oder im Bereich der Bürokommunikation vorkommen. Beispiele in diesem Umfeld sind Sprach- und Videokommunikation oder Fernwartung.

Betrachtet man die Übertragung von Daten in modernen Kommunikationsnetzen, so sind unterschiedliche Fähigkeiten und Anforderungen zu spezifizieren. Ähnlich wie in den aktuell noch genutzten SDH- und PDH-Netzen, sind viele bisherige Anforderungen auch weiterhin relevant und müssen technisch erfüllt werden. Die Technologieentwicklungen ermöglichen zudem weiterführende Funktionalitäten, z.B. im Layer 3, die eine höhere Integration und Flexibilität von Diensten erlauben. Die folgende Liste gibt einen Überblick über mögliche Eigenschaften, die durch moderne Kommunikationsnetze realisiert werden.



- Bandbreite

  Die Bandbreite stellt die Anforderung an die Übertragungskapazität dar und muss dynamisch oder absolut im Netzwerk reserviert werden können. Die dynamische Reservierung erlaubt im Vergleich zu SDH- oder PDH-Netzen eine sehr viel effizientere Nutzung von Ressourcen.

- Quality of Service (QoS)

  Die Bevorrechtigung von bestimmten Daten in ihrer Übertragung vor anderen Datenströmen (Klassifizierung, Queueing, Policy Priorisierung) ist erforderlich, um trotz dynamischer Bandbreitenvergabe eine sichere Übertragung zu gewährleisten. Die Einstufung von Daten in die QoS-Klassen stellt im Grunde nur eine Differenzierung zwischen echtzeitfähigem, bevorrechtigtem und normalem Verkehr dar. Je nach Anforderung wird in den drei Bereichen noch weiter unterteilt oder eine minimale oder maximale Bandbreite festgelegt.

- Laufzeit

Die Laufzeit einer Kommunikation ist die absolute Zeit, die für den Transport eines Datenpaketes von Endpunkt A nach Endpunkt B erforderlich ist. Bei einer automatischen Wegewahl ergibt sich diese Zeit durch die dynamische Führung im Netz. Je nach Wegewahl können sich auf diese Weise unterschiedliche Laufzeiten ergeben. Alternativ sind aber auch Mechanismen vorhanden, die einen vordefinierten identischen Hin- und Rückweg und damit eine konstante Laufzeit in beide Richtungen ermöglichen. Hinzu kommen immer die physikalisch unabdingbaren Laufzeiten der Kabellängen und die Bearbeitungszeiten der Komponenten.

- Jitter

  Der Jitter einer Verbindung beschreibt die Schwankung der Laufzeit zwischen den Endpunkten A und B für eine Kommunikationsverbindung. Viele Anwendungen sind hier sehr tolerant, während andere Anwendungen, wie z.B. Differenzialschutz, sehr empfindlich auf zu hohe Schwankungen der Laufzeiten reagieren.

- OSI Layer (Open Systems Interconnection)

  Der Begriff Layer ist aus dem OSI-Modell übernommen und unterscheidet zwei mögliche Varianten. In der Layer-2-Variante wird das Datenpaket direkt als Paket übernommen und transparent zwischen den Endpunkten A und B übertragen. Bei den Layer-2-Verbindungen kann es sich um Ethernet oder auch serielle Daten (E1, V.24, X.21) handeln. In der Layer-3-Variante werden Datenpakete zwischen den beteiligten Endpunkten über das Netz geroutet. So können auch unterschiedliche IP-Netze verbunden werden.

- Kommunikationsmatrix

  Es werden drei grundsätzliche Kommunikationsarten unterschieden. Die einfachste Form ist die Punkt-zu-Punkt-Kommunikation zwischen zwei beteiligten Endpunkten. Eine weitere Option stellt die Punkt-zur-Mehrpunkt-Kommunikation in Form eines Baums dar, in der alle Endpunkte mit der Wurzel des Baums, aber nicht untereinander kommunizieren können. Die dritte Option ist eine Kommunikation zwischen beliebigen Endpunkten.

  Wurzel des Baums, aber nicht untereinander kommunizieren können. Die dritte Option ist eine Kommunikation zwischen beliebigen Endpunkten.

Nach einer technischen Betrachtung von Anforderungen an die Fähigkeiten einer Kommunikation, müssen diese Aspekte auch auf die unterschiedlichen Anforderungen zum Betrieb eines Energienetzes in den Zusammenhang gebracht werden.

- IEC 60870-5-104 oder IEC 61850 MMS

  Anwendungen aus diesem Bereich nutzen TCP/IP als Kommunikationsprotokoll und sind auf Layer-3-Verbindungen (in unterschiedlichen oder im selben Subnetz) angewiesen. Spezielle Anforderungen an Bandbreite, Latenz oder Jitter sind nicht vorhanden. Allerdings ist eine recht hohe QoS-Klasse von Interesse, um die Kommunikation immer bevorrechtigt durchführen zu können. Die Kommunikation erfolgt typischerweise zwischen Station und Leitstelle.

- Schutzkommunikation

  Bei der Schutzkommunikation und speziell bei der Differenzialschutz-Kommunikation bestehen hohe Anforderungen an die Qualität der Übertragung. Um Paketverluste absolut zu vermeiden, muss eine zugesicherte Bandbreite vorhanden sein. Die Latenzen dürfen sich durch dynamische Vorgänge im Netzwerk nicht verändern, Hin- und Rückweg müssen gleich sein. Ebenso muss der Jitter unterhalb einer kritischen Toleranzgrenze liegen. Der Verkehr der Differenzialschutz-Relais ist oft eine eingepackte E1-Schnittstelle oder bei neueren Versionen ein direkter Datenaustausch über Ethernet. Etwas zeitlich unkritischer ist die Distanzschutz-Kommunikation, da hier oftmals nur ein Schaltzustand übertragen wird. Aber auch diese Kommunikation muss gesichert und priorisiert realisiert werden.

- IEC 61850 SV oder Goose im Weitverkehr

  Die Protokollelemente Sampled Values (SV) oder Goose der IEC-61850-Familie bestehen aus Multicast-Paketen mit Layer-2-Aufbau und können ebenfalls im Weitverkehr übertragen werden. Neben der Layer-2-Variante für Goose- und Sampled-Value-Kommunikation ist ebenfalls eine Variante mit Layer 3 definiert. Die notwendige Bandbreite muss vom Netzwerk gewährleistet werden, Paketverluste sind hier zwingend zu vermeiden. Ebenfalls müssen Parameter wie Jitter möglichst niedrig und die Latenz möglichst konstant gehalten werden. Neben diesen Werten ist auch der Austausch der Zeitinformation wichtig, da Sampled Values von der erzeugenden Einheit mit Zeitstempel verschickt werden, die von der empfangenden Einheit mit lokalen Daten in Bezug gesetzt werden.

- Precision Time Protocol (PTP)

  Das Precision Time Protocol wird benötigt, um eine Zeitinformation, z.B. für Sampled Values oder andere Elemente der IEC-61850-Familie, im Netzwerk zu verteilen. Während das Network Time Protocol (NTP) eine Genauigkeit von 1 Millisekunde erreicht, ist beim PTP eine Genauigkeit von 1 Mikrosekunde notwendig. Der Dienst PTP ist durch den Einsatz moderner Infrastruktur leicht realisierbar. Wichtig dabei ist, dass die Anzahl der zu querenden Netzelemente möglichst niedrig gehalten wird. Jede Komponente im Datenstrom erzeugt eine weitere Variation der Paketlaufzeit und damit eine Zeitungenauigkeit für den PTP-Dienst. Neben dem generellen Support der PTP-Funktion sind auch QoS, Latenz und Jitter Anforderungen an die Netzwerkinfrastruktur. PTP-Kommunikation im Weitverkehr auf Basis der Carrier-nahen Implementierungen muss konform zum Powerprofil in die Leitstellenkommunikations-Station übersetzt werden.

- Synchrophasor-Anwendungen

  Es empfiehlt sich die Nutzung von Synchrophasor-Messgeräten (basierend auf IEC 61850-90-5) für die Anwendungsfälle. In diesen werden exakt der Netzzustand erfasst, der Status bewertet und Daten archiviert, basierend auf der Kommunikation zwischen Sensoren und Auswertungskomponenten. Die entstehenden Daten werden dabei oftmals von einem Erzeuger an mehrere Empfänger zur Bearbeitung weitergeleitet. Die Basis hierfür stellen IP-basierte Multicast-Protokolle dar. Alle beteiligten Komponenten müssen dabei über eine präzise Zeitsynchronisierung, z.B. mit Hilfe von PTP, verfügen. Bei den Controls Special Protection Schemes (SPS), Predictive Dynamic Stability Maintaining System und Wide Area

Monitoring Protection and Control (WAMPAC) sind Latenzzeiten je nach Anwendungsfall in einem Bereich von 20ms bis 5s einzuhalten.

- Kollaboration

  Die MitarbeiterInnen im Betrieb eines Energienetzes nutzen intensiv Funktionalitäten aus dem Kollaborationsbereich. Neben Grundfunktionen wie der reinen Sprachkommunikation sind auch erweiterte Funktionen wie Video, Konferenzen, Chat und Sharing wichtige Bausteine für den Austausch zwischen Leitstellen, TechnikerInnen, Krisenräumen und Betriebsstandorten. Das Weitverkehrsnetz muss diesbezüglich, in Abstufung zu den Steuerungsfunktionen des Energienetzes, Bandbreite, QoS sowie Latenzanforderungen erfüllen. Ein weiterer wesentlicher Bestandteil ist die vollständige Vermaschung der TeilnehmerInnen und die Kommunikation im Layer-3-Umfeld, um jede denkbare Verbindung effektiv nutzen zu können.

- Fernwartung

  Fernwartung ist eine Funktion, die generell den Betrieb und die Überwachung der Feldleitgeräte vereinfachen soll. Im Umfeld der Fernwartung sind Funktionen wie Logging, Remote-Auswertung, Softwarewartung, Parametrierung zu benennen. Neben den zu beachtenden sicherheitstechnischen Aspekten solcher Lösungen, sind Layer-3-Netze mit mehreren Teilnehmern die Basis für die technische Umsetzung. Im Umfeld QoS, Latenz und Jitter liegen dazu keine besonderen Anforderungen vor. Auch der Bandbreitenbedarf kann den anderen Diensten untergeordnet werden.

- Anlagen-zu-Anlagen-Kommunikation

  In den heutigen etablierten Abläufen zum Betrieb eines Energienetzes sind die Anlagen mit Punkt-zu-Punkt-Verbindungen an das Netzleitsystem angebunden. Direkte Kommunikation zwischen Umspann- und Schaltanlagen, z.B. mit IEC-104-Protokollen, ist nicht notwendig. Mögliche Erweiterungen von Funktionalitäten zur direkten Kommunikation einiger Umspannanlagen miteinander sind zukünftig denkbar. Diese würden Layer-3-Mehrpunktverbindungen erfordern. Je nach Anforderung sind die entsprechenden Parameter QoS, Bandbreite sowie Jitter auszuführen. In verschiedenen Musteranlagen werden als Beispiel erweiterte Regelkreise zur Spannungshaltung im Mittelspannungsnetz eingesetzt.

- Dienste auf Multicast-Basis

  Der Einsatz von Multicast kann notwendig werden, wenn mehrere Teilnehmer gleichzeitig Daten eines weiteren Teilnehmers benötigen. So wie Sampled Values die Daten als Layer-2-Multicast ausführen, sind ähnliche Funktionen auch im Layer 3 realisierbar. Die dazu notwendigen Protokolle sind im Carrier-Umfeld seit längerer Zeit Standard und werden z.B. im Finanzsektor oder beim Videostreaming eingesetzt. Die Umsetzung in WAN-Netzwerken auf Layer-3-Basis erfordert dynamische Strukturen, die während der Nutzung aufgebaut und erhalten werden. Empfänger und Sender können hierbei an vielen Stellen gleichzeitig vorhanden sein. Die Nutzung von Synchrophasor-Anwendungen baut auf einer Multicast-Infrastruktur auf.

Die hier dargestellten Funktionsanforderungen aus der Sicht eines Energienetzes stellen lediglich eine Auswahl dar. Schon dadurch wird deutlich, dass eine heutige Kommunikationsinfrastruktur für ein Energienetz wesentlich mehr Aspekte erfüllen muss, als es in der Vergangenheit mit reinen leitungsbasierten Systemen notwendig war.

Technologien

Nach Auflistung der Fähigkeiten und Anforderungen an eine moderne Kommunikationsinfrastruktur für Energienetze und der Definition der technologischen Möglichkeiten sind einzelne Technologien zu betrachten, die in der Lage sind, die aktuellen und zukünftigen Anforderungen zu erfüllen.

Im Carrier-Umfeld werden unterschiedliche **Technologien und Begrifflichkeiten** diskutiert und positioniert.

- MPLS (Multiprotocol Label Switching)

  Eine wesentliche technologische Grundlage in Carrier-Netzen stellt die MPLS-Technologie dar. MPLS wurde Mitte der 1990er Jahre eingeführt und ist über die Zeit die Basis für Carrier-Netze geworden. Der Grundgedanke hinter MPLS ist, jedem Datenpaket ein Label zu geben, auf dessen Basis eine Weiterleitung in einem Netzwerk durchgeführt wird. Bei der eigentlichen Realisierung werden zwei Varianten unterschieden, MPLS-TP und MPLS-IP. Beide unterscheiden sich in wesentlichen Details. Spricht man von MPLS, ist im Allgemeinen die MPLS-IP-Variante gemeint.

- MPLS-TP (Multiprotocol Label Switching-Transport Profile)

  Die Technologie MPLS-TP ist in ihrer Ausführung sehr nah an die Betriebsweise eines SDH-Netzes angelehnt. Alle Dienste und Verbindungen werden durch ein zentrales Managementsystem provisioniert. Dynamische Services in Layer-3-VPN oder z.B. ein dynamisch erstellter Ersatzweg im Fehlerfall sind jedoch nicht möglich. Redundanzen werden vom Managementsystem vorab implementiert und dann bei Bedarf genutzt. Durch den eher statischen Ansatz findet diese Technologie wenig bis keine Anwendung in Carrier-Infrastrukturen.

- MPLS-IP (Multiprotocol Label Switching-Internet Protocol)

  Bei MPLS-IP werden alle Wege, Dienste und Ressourcen durch dynamische Protokolle realisiert. Die Netzinfrastruktur kann damit sehr einfach und schnell auf Fehler, Topologie-Veränderungen oder neue Anforderungen reagieren. Zusätzlich zu dem dynamischen Verhalten können in Koexistenz auch festgelegte Wege (Traffic Engineering) realisiert werden, die dem Verhalten im SDH sehr ähnlich sind. MPLS-IP stellt damit – insbesondere im direkten Vergleich mit MPLS-TP – eine sehr effiziente Struktur zur Verfügung, die auch Anwendungen wie Layer-3-VPN, Multicast oder Segment Routing beachtet.

- SR (Segment Routing)

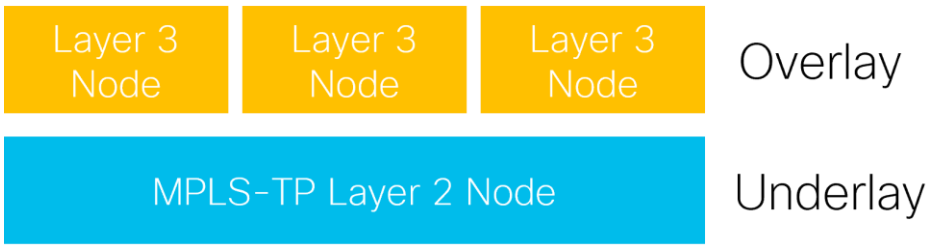
  Segment Routing ist eine technologische Weiterentwicklung im Umfeld MPLS-IP, welche die dynamische Nutzung von Ressourcen weiter optimiert und neben MPLS auch IPV6 unabhängig als Basis nutzen kann. Viele Carrier setzen heute einen kombinierten Ansatz der MPLS-IP- und Segment-Routing-Technologien zur Abbildung der Kundenanforderungen ein. Segment Routing ist die aktuelle Zielarchitektur vieler Carrier.

- SDN (Software-Defined Network)

  Software-Defined Network ist eine Herangehensweise an Netzwerkinfrastrukturen, die sowohl durch den Einsatz von zentralen Bausteinen (Controllern) als auch durch die Umsetzung im Management eines Netzwerkes realisiert werden kann. Oftmals werden viele dezentrale Entscheidungen bewusst der Dynamik des Netzwerkes überlassen, während die Rahmenparameter über Controller zur Verfügung gestellt werden. Ein standardisierter Ansatz für SDN von den Normungsgremien ist im Carrier-Bereich, wie auch in den meisten anderen Anwendungsbereichen, nicht vorhanden.

Die Bewertung der einzelnen Technologien unter Betrachtung der Anforderungen des Energieversorgers ergibt wichtige Aspekte für **Auswahl und Einsatz**.

Eine große Herausforderung der MPLS-TP-Ansätze liegt im Bereich Skalierbarkeit, vor allem bei Services mit einer Vielzahl von Kommunikationsverbindungen. Bei MPLS-TP fehlt außerdem die Funktion, dynamische Verbindungen aufzubauen, z.B. in der Nutzung von Multicast oder der Realisierung von Redundanzen. Oftmals versucht man, diese Probleme durch die Teilung in ein Layer-2-Underlay und ein Layer-3-Overlay mit getrennter Hardware zu lösen.



Bei dem Overlay-Underlay-Ansatz entstehen mehrere Verantwortlichkeiten in Unternehmen mit der Herausforderung, die Fähigkeiten der beiden Schichten aufeinander abzustimmen. Es wäre z.B. sinnvoll, wenn Layer-3- oder Multicast-Strukturen eine entsprechende Abbildung im Layer 2 haben, um unnötige Weiterleitungen zu vermeiden.

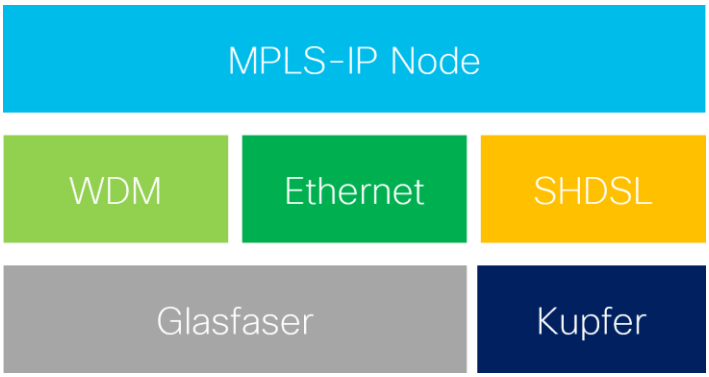
Einschränkungen des PTP im Bereich der Zeitverteilung ergeben sich durch die Erhöhung der Anzahl der Komponenten im Kommunikationsweg. Müssen bei der PTP-Planung im Layer 3 die Knoten im Layer 2 addiert werden, so halbiert sich die mögliche Knotenanzahl im Layer 3 und damit die Ausdehnung der PTP-Struktur bis zur nächsten Aufbereitung des Zeitsignals. Auf diese Weise entsteht eine Zeitungenauigkeit im Netzwerk, die es zu vermeiden gilt.

SDNs adressieren heute sehr stark Anforderungen aus dem betrieblichen Bereich im Umfeld eines Carriers. Sie verbinden geschäftliche Anforderungen direkt mit technischen Umsetzungen. Zielsetzungen im SDN-Umfeld sind oft Rollouts im großen Umfang: wiederkehrende Tätigkeiten automatisieren, den Lifecycle von Services unterstützen, aber auch Fehler in Abläufen minimieren oder sogar vermeiden. Dadurch sind hohe Qualitätsstandards in Betrieb und Diensten zu erreichen. Vor allem die Integration in Automationssysteme für Business-Prozesse ermöglichen viele Mehrwerte im Carrier-Umfeld. Diese Mehrwerte sind vom einzelnen Energienetzbetreiber gezielt zu prüfen und abzuwägen.

Beim Einsatz von MPLS-IP können viele Vorteile durch das dynamische Verhalten im Fehlerfall oder die flexible Ergänzung von Services erreicht werden. Die meisten Dienste wie IEC 60870-5-104, IEC 61850 MMS, Kollaboration und Fernwartung können diese Vorteile sehr effizient nutzen.

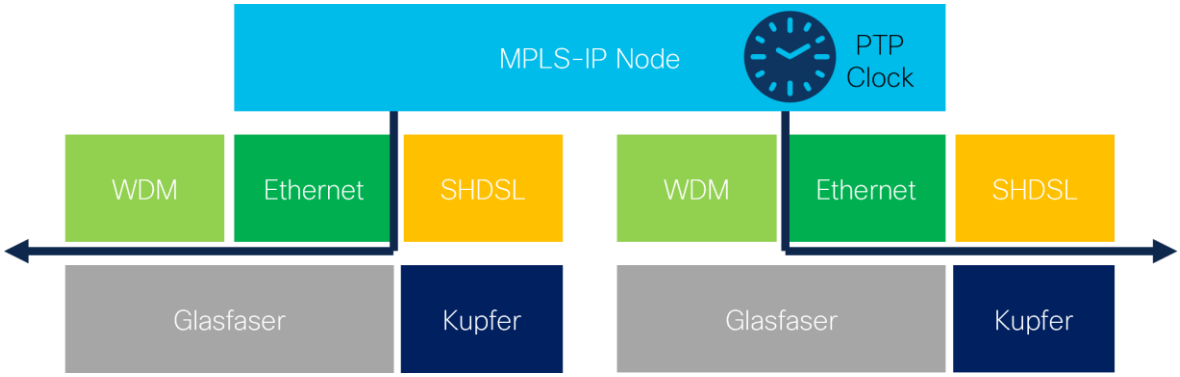
Um auch Dienste wie Schutzkommunikation mit speziellen Anforderungen in Übertragungszeit, Bandbreite oder Jitter umsetzen zu können, werden zusätzlich zu dem dynamischen Verhalten festgelegte Wege (Traffic Engineering) implementiert. Traffic Engineering stellt Funktionen zur Verfügung, die mit dem dynamischen Verhalten koexistieren können.

Am meisten verbreitet bei großen und umfangreichen Installationen von Carriern sind MPLS-IP-Netze mit einer Vorbereitung für die Optionen des Segment Routing. Die Basis der weiteren Betrachtung ist daher eine MPLS-IP-basierte Infrastruktur, die auf die vorhandenen Kabelnetze aufsetzt. Neben der direkten Schaltung einer Ethernet-Schnittstelle auf eine optische Faser können auch optische WDM-Systeme oder WDM-Interfaces als Grundlage genutzt werden. Dieser Technologie-Layer wird eingesetzt, um die Distanzen zwischen Standorten und auch die Koexistenz mit anderen Diensten auf der gleichen optischen Faser zu ermöglichen. Oftmals werden bereits auf diesem Layer auch Redundanzen zur Verfügung gestellt.



Da die Kabelinfrastrukturen zu einem großen Teil aus Glasfasernetzen bestehen, sind direkte Anschaltungen mit Ethernet-Schnittstellen möglich. Bei der Überschreitung von Distanzgrenzen oder bei Bedarf von hohen Bandbreiten ab ca. 100Gbit/s kommen zwingend WDM-Systeme oder kohärente Optiken zum Einsatz. Sollen Kupferkabel die Grundlage darstellen, so sind Interfaces aus dem DSL-Bereich „back to back“ einzusetzen. Aus Sicht des MPLS-IP Nodes handelt es sich jeweils um das gleiche logische Interface, das in der gleichen Betriebsart genutzt wird. Der Betrieb wird auf diese Weise stark vereinfacht. Selbstverständlich sind spezifische Parameter wie die verfügbare Bandbreite zu beachten.

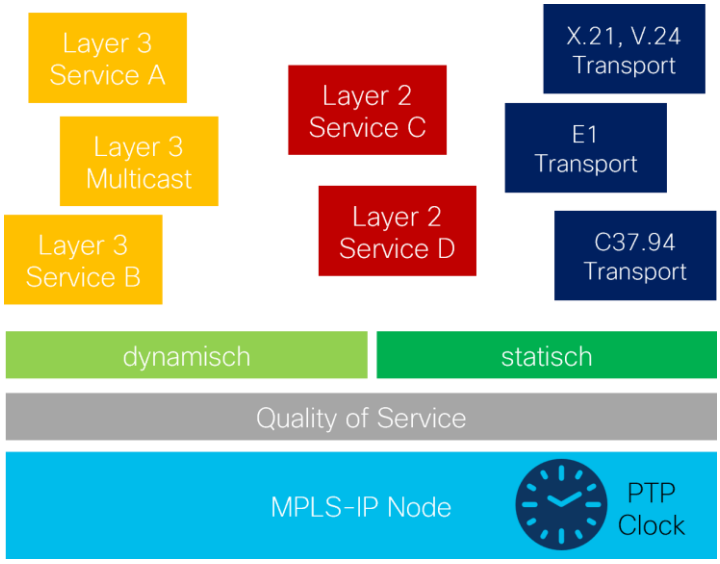
Beim Einsatz von PTP stellt der MPLS-IP Node eine PTP Clock dar und kommuniziert über die unterliegenden Medien mit den Nachbarstandorten. Die Verteilung der Zeit über PTP ist Bestandteil der Netzwerkplanung. Die PTP-Systeme werden zentral über eine hochpräzise Cesium Clock (Atomuhr) mit einer Zeit versorgt. Auf Basis der PTP-Planung sind eventuell weitere Zeitnormale erforderlich.



In der nächsten Schicht werden in den MPLS-IP Nodes die notwendigen Protokolle für die Basis von MPLS-IP eingerichtet. Der MPLS-IP Node stellt die folgenden Funktionen zur Verfügung.

- Aufbau der logischen Topologie zwischen den beteiligten Knoten: MPLS-IP kann hier vollkommen dynamisch mit Hilfe der Routingprotokolle Wege zwischen Endpunkten erstellen. Wege können im Fehlerfall aber auch vorbereitend automatisch neu berechnet werden, um die Kommunikation wieder zur Verfügung zu stellen. Die Vorbereitung der Wege wird systematisch für das Gesamtsystem realisiert und nicht pro Service.
- Ergänzung der Traffic-Engineering-Funktionen, um parallel zu dem dynamischen Verhalten auch feste und eindeutig definierte Wege zu realisieren: Im MPLS-IP können dadurch die Eigenschaften einer Wegeauswahl in Abhängigkeit des Service definiert und realisiert werden.
- Quality of Service und Bandbreiten können je Interface nach Bedarf der einzelnen Anwendungen eingerichtet werden. Hierbei werden die Anwendungen nach Kritikalität und Anforderungen parametriert. Im QoS-Bereich werden auch die notwendigen Bandbreiten beschrieben und von den Systemen zur Verfügung gestellt.

- Um Anwendungen aus dem Bereich der Schutzkommunikation zu realisieren, werden festgelegte Kommunikationswege (Traffic Engineering) definiert und aus dem dynamischen Routing ausgeschlossen. Der Service, z.B. für Differenzialschutz, wird mit den Eigenschaften Bandbreite, geringster Jitter und einer konstanten Latenz eingerichtet.
- Schnittstellen aus dem seriellen Bereich wie C37.94, E1 usw. werden als Interface angenommen und in MPLS-Pakete eingepackt. Die Weiterleitung kann nach Definition per Traffic Engineering z.B. für E1- und dynamisch z.B. für V.24-Kommunikation erfolgen.
- Protokolle wie die IEC-Kommunikation (IEC 60870-5-104 oder IEC 61850-MMS) können als dynamischer Layer-3-Service implementiert werden. Kommunikationsmuster wie eine volle Vermaschung oder Baumstrukturen können einfach und flexibel per Konfiguration erreicht werden.
- Services wie z.B. Kollaboration, Fernwartung usw. können direkt als dynamischer Layer-3-Service eingerichtet und einfach an jedem MPLS-IP-System nach Bedarf zur Verfügung gestellt werden. Hierbei sind ebenfalls Kommunikationsmuster wie eine volle Vermaschung für Kollaboration und eine Baumstruktur für Fernwartung Attribute des Layer-3-Dienstes.
- Multicast-Dienste lassen sich einfach in eine MPLS-IP-Infrastruktur integrieren. Anwendungen, die direkt mit Multicast-Protokollen interagieren, können in der Infrastruktur einfach implementiert werden.



Security im Weitverkehrsnetz

Ein ganzheitliches Sicherheitskonzept muss das Weitverkehrsnetz umfassend schützen. Umgekehrt benötigt das Sicherheitskonzept Daten aus der Infrastruktur des Weitverkehrsnetzes, damit es in diesem anspruchsvollen Umfeld stabil und richtig funktionieren kann. Betrachtet man die Sicherheit mit Fokus auf die Infrastruktur, so müssen unterschiedliche Aspekte beachtet werden.

- Security-Funktionalitäten zum Aufbau und Betrieb der MPLS-IP-Funktionen: In diesen Bereich fallen notwendige Funktionen wie die Identität und Verschlüsselung in Routingprotokollen, die Security-Elemente im Management – wie SNMP-V3 oder SSH – oder auch signierte Betriebssysteme und Hardwareelemente. Bei vielen der Protokolle ist die Identität der beteiligten Komponenten und Systeme relevant.
- Bei der reinen Weiterleitung von Daten über WAN-Schnittstellen sind zum Erreichen der Schutzziele auch Verschlüsselungsoptionen möglich. Insbesondere müssen hier die MACsec-Umsetzungen betrachtet werden, da sie keine Nachteile (Fehlerkorrekturfunktionen in MACsec beachten) für die PTP und die sensitive Kommunikation im Bereich Latenz und Jitter darstellen. Bei MACsec wird die Verschlüsselung auf Layer-2- realisiert.

- MPLS-IP ist vom Grunddesign mandantenfähig ausgelegt und definiert. Eine Grundfunktion der Mandantenfähigkeit ist die strikte Isolation der einzelnen Mandanten voneinander. Mit dieser Funktion lässt sich beispielsweise IEC-Kommunikation einfach von Fernwartungsdiensten im Netz trennen.
- In den einzelnen Mandaten können Kommunikationseigenschaften wie eine Baumstruktur, zentrale Servicebereiche oder eine Vollvermaschung als unabhängige Parameter implementiert werden.
- Neben der klaren Definition von Kommunikationsbeziehungen können auch kontinuierlich Informationen über die aktuelle Kommunikation an zentrale Auswertungssysteme, beispielsweise für das Prozessnetz-Monitoring, weitergeleitet werden. Zu diesem Zweck sind Netflow-Spezifikationen oder Spiegel-Ports umsetzbar.

Betrieb und Netzwerkmanagement

Eine Weitverkehrsinfrastruktur geht nach der Planung und dem Aufbau in eine langjährige Betriebsphase über. In der Planung und Auslegung sind zentrale Managementsysteme zu definieren, die die einzelnen Tätigkeiten während des Betriebs unterstützen. Die Basis hierzu stellen die fünf grundlegenden Anforderungen FCAPS (Fault, Configuration, Accounting, Performance, Security) dar. Die FCAPS-Funktionen sind verantwortlich für ein oft Geräte-zentriertes Management und stellen sowohl im Rollout als auch in der Fehlerüberwachung und im Betrieb die erforderlichen Funktionen zur Verfügung.

Managementsysteme sollten aber auch zusätzliche Funktionen übernehmen können, um wertvolle Hilfestellung im Betrieb zu leisten.

- Service Provisioning

  Services wie vordefinierte Wege, Layer-3-VPN oder Layer-2-Punkt-zu-Punkt-Verbindungen nutzen Funktionen von etlichen Komponenten im Netzwerk. Das zentrale Management muss bei der Provisionierung der Services unterstützen und die notwendigen Anpassungen und Konfigurationen auf allen beteiligten Komponenten durchführen. Die dazu notwendigen Ressourcen und Parameter sind netzübergreifend in einer zentralen Datenbank zu pflegen.

- Service Monitoring

  Im Netzwerk konfigurierte Services müssen vom Netzwerkmanagement zentral auf ihre Funktion und Verfügbarkeit hin überwacht werden. Viele Attribute sind bereits in den Services nativ vorhanden oder können durch ergänzende Mechanismen wie Y.1731 (ITU, OAM functions and mechanisms for Ethernet based networks) konfiguriert und überwacht werden.

- Root Cause Analyse & Service-Ausfall

  Bei einer Störung, z.B. dem Ausfall einer Leitung, werden oft viele Fehlermeldungen gleichzeitig erzeugt, aber ganzheitliche Zusammenhänge trotzdem nicht dargestellt. Für MitarbeiterInnen im Operation Center ist ein schnelles Identifizieren der eigentlichen Ursache und der betroffenen Services wichtig, um weitere Arbeiten vornehmen zu können und betroffene Abteilungen zu informieren.

- Kapazitätsplanung

  Infrastrukturen werden im Laufe der Betriebszeit mit Services ausgelastet. Eine Betrachtung der Entwicklung über die Zeit ist eine der Hauptfunktionen der Kapazitätsplanung. Dadurch lassen sich Engpässe frühzeitig erkennen und Services oder auch damit verbundene Investitionen gezielt vorbereiten.

- Kritikalitätsüberwachung

  In Energieversorger-Infrastrukturen sind viele Kommunikationsdienste für den sicheren Betrieb notwendig. Eine schnelle Bewertung, ob eine Planung von Services oder eine vorhandene Störung zu einem Single

Point of Failure führen wird, fundiert Entscheidungen für weitere Vorgehensweisen. Die Kritikalitätsüberwachung ist für die kontinuierliche Bewertung der vorhandenen Redundanzen notwendig.

- Wartungsplanung

  In Infrastrukturen werden Komponenten oder Leitungen in regelmäßigen Abständen gewartet. Geplante Arbeiten müssen gegen den aktuellen Betriebszustand des Netzes geprüft und „Was ist, wenn...?"-Analysen durchgeführt werden. Dieser Vorgang ermöglicht eine stetige Bewertung der Redundanz.

- Betriebssysteme und Software

  Beim Einsatz von Software kann nie eine vollständige Fehlerfreiheit erreicht werden. Das Managementsystem und der Support müssen daher in der Lage sein, bekannte Fehler und Security-Risiken zu erkennen und daraus Handlungsempfehlungen abzuleiten.

- API und Schnittstellen

  Für den Betrieb sind API-Integrationen mit weiteren Managementsystemen, z.B. mit Ticketverwaltungssystemen, Asset-Management-Systemen oder Business-Prozess-Automation, oftmals interessant. Eine hohe Automation und damit Reduktion manueller Fehler und Konfigurationen sind hier wichtige Ziele.

Zusammenfassung

Eine moderne Weitverkehrsinfrastruktur für Energienetzbetreiber muss unterschiedliche Anforderungen erfüllen und über bestimmte Fähigkeiten bzw. Funktionen verfügen. Neben dem Support von konventionellen Schnittstellen und der Umsetzung von kritischen Services des Energienetzes ist auch die Bewertung der Zukunftssicherheit Bestandteil der zu betrachtenden Aspekte. Eine MPLS-IP-Infrastruktur ermöglicht eine flexible Umsetzung der aktuellen und zukünftigen Anforderungen. Betriebliche Aspekte lassen sich auf diese Weise sehr umfangreich und detailliert betrachten und auch wichtige Sicherheitsanforderungen werden direkt erfüllt. MPLS-IP stellt einen konkreten Weg für eine mittelfristige Migration zu aktuellen Carrier-Technologien dar. Damit sind sowohl die geforderte technische Leistungsfähigkeit als auch die Zukunftssicherheit für getätigte Investitionen gewährleistet.