Nokia Validated Design

Teleprotection Services with Active Multipath

3HE-26647-AAAA-TQZZA
Issue 1
March 2026

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

Contents

List of figures

List of tables

1 Terminology

Table 1 **List of terms**

Term	Definition
A/S-PW	Active/standby pseudo wire
ADC	Asymmetrical delay control
AMP	Active multipath Active/active multipath
CEM	Circuit emulation
CES	Circuit emulation service
CESoPSN	Circuit emulation service over Packet Switched Network
CESoPSN-CAS	Circuit Emulation Services over Packet Switched Network with Channel Associated Signaling
DTT	Direct transfer trip
ESMC	Ethernet Synchronization Message Channel
FRR	Fast reroute
GMC	Grandmaster clock
IBSF	intent-based service fulfilment
IP/MPLS	Internet protocol/multi-protocol label switching
JB	Jitter buffer
LCD	Line current differential
LSP	Label switching path
MB	Magnetic blow-out (relay)
MKA	IEEE 802.1X - *MACsec Key Agreement protocol*
MPLS	RFC 3031 - *Multiprotocol Label Switching Architecture*
NGE	Network group encryption
NSP	Network Services Platform
NVD	Nokia validated design
PAC	Protection and control
PDV	Packet delay variation
PE	Provider edge router
POTT	Permissive overreaching transfer trip
PTP	Precision time protocol
QoS	Quality of service
RSVP	Resource reservation protocol
SAK	Secure association key (used in MACsec)
SAToP	Structure agnostic transport over packet
SDP	Service distribution point
SF	Service fulfilment
SGT QoS	Security group tag quality of service

Term	Definition
SSM	Synchronization status message
SyncE	Synchronous Ethernet
TDM	Time division multiplexing
TPR	Teleprotection relay
VCI	Virtual circuit identifier
VLL	virtual leased line
VPLS	virtual private LAN service

2 Executive summary

Nokia validated designs (NVDs) provide finely tailored validated recommendations for applying Nokia's portfolio to specific consumer market segments.

An NVD solution is based on detailed requirements analysis from many customers, along with extensive research into the most current technological developments in the industry segment. After a design is compiled, Nokia applies an intense array of hardware, software, traffic, and failure tests to form the NVD. The resultant design and collateral provide a blueprint that consumers in the industry segment can use with confidence to deploy the NVD solution with their own environment and applications.

This NVD focuses on the approach and methods for deploying services and circuits for teleprotection relay (TPR) systems across an IP/MPLS network. Power utilities put systems in place that continuously monitor the electrical infrastructure and provide real-time information about the state of the power grid at key points in the network. These TPR systems are designed to help protect the power grid against failures and avoid cascading problems through the grid.

Using this NVD, utility operators can be certain that the IP/MPLS network meets or exceeds the requirements of their TPR applications.

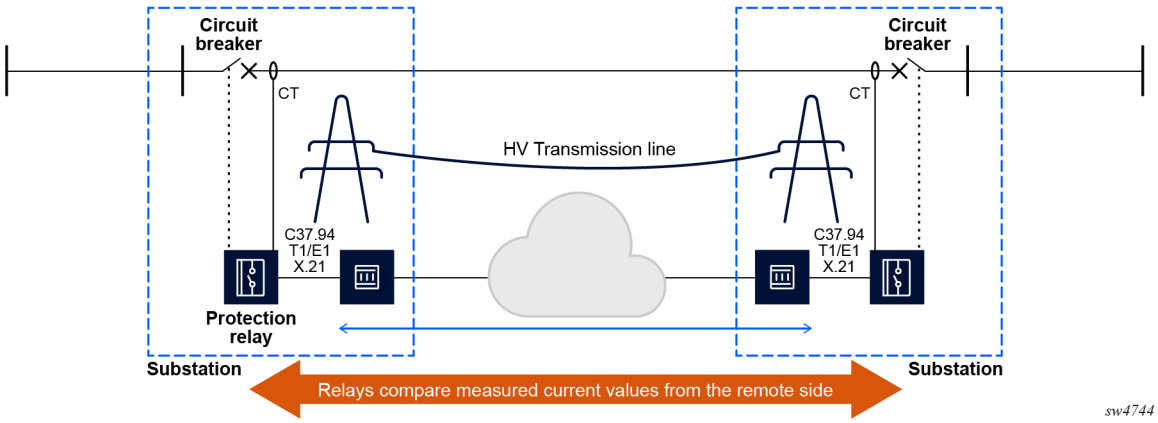
3 Teleprotection fundamentals

3.1 Current differential fault detection

Operating an electric grid requires provisioning safeguards for detecting faults and taking subsequent corrective action on the grid transmission lines. Teleprotection systems are used to detect faults in the power grid and activate circuit breakers or reclosers to prevent faults from rippling through the network, and to restore power to a part of the grid after an outage. Teleprotection is an essential requirement for operating and maintaining a reliable, robust and safe electric grid.

A current differential teleprotection system is an important pilot-based system for mission critical utility deployments. This type of system relies on a communications channel between adjacent nodes along the transmission line. The main principle for operating a current differential protection system is based on Kirchoff's fundamental rule of electrical systems, which says that the sum of the currents flowing into a point is always identical to the sum of the currents flowing out of the same point. If there is any difference, there is a fault. The following figure shows this functionality.

Figure 1 **Current differential protection**



Line current differential (LCD) relays continuously send sample values to each other to compare the current values that they see. The relays rely on a fixed latency time to transmit and receive data, because they need to compare real-time sample values using a fixed offset to compensate for the communications latency. This requires accurate timing on the transport network, low latency with minimal variation, and symmetric transmission delay for the paths between the relay devices.

The importance of this functionality is magnified when smart grid deployments include increasingly diverse sources of electric power that are combined and channeled to increasingly diverse consumers of electric power.

Note: This section focuses on LCD relay systems, which are the most modern systems with the strictest latency and jitter requirements. However, the transport solution described in this document applies for other relay types, for example, mirrored bits, direct transfer trip (DTT), permissive overreaching transfer trip (POTT), and so on.

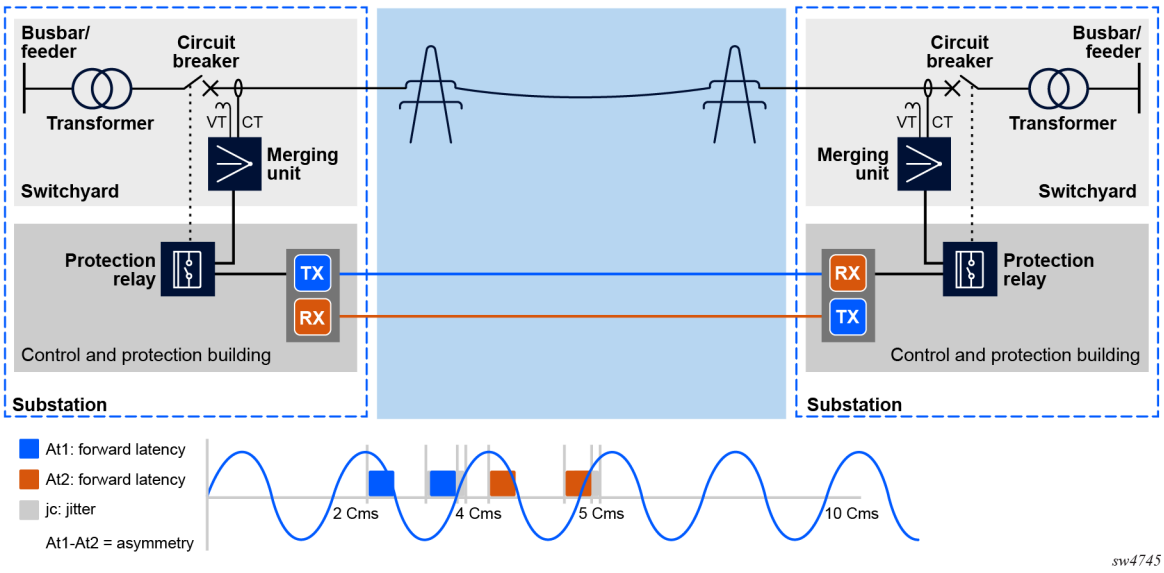
3.2 Critical performance requirements

A failure such as a short circuit in a high voltage power system can cause major damage leading to an avalanche effect on the entire power system of a city, region, or country. It is therefore essential that failures are detected rapidly and protection systems are engaged immediately.

Older teleprotection systems that use analog (voice band) communication interfaces may be allowed a total acceptable network delay of up to 15, 20, and even 40 ms in some cases. However, today the network must support the stricter latency requirements required by current-differential relays. Today teleprotection applications are typically developed using a total fault-clearing time of five to seven cycles of the AC electrical system. The AC electricity cycle rate is 50 Hz (20 ms per cycle) in most parts of the world, and typically 60 Hz (16.66 ms per cycle) in the Americas. If the fault inception and the resolution delay take between one and three-to-five cycles respectively, this leaves one cycle, or 16.6 ms (20 ms in a 50 Hz grid), for the total end-to-end delay comprised of TPR equipment delay, network delay, and transport propagation delay. If the TPR delay is found to be around 3 ms at each terminal, this leaves approximately 10 ms for an acceptable total telecom network delay. This 10 ms maximum latency for digital systems is defined in the IEC 834-1 standard.

The following figure shows the time constraints of the TPR delay.

Figure 2 **Time constraints of the TPR system (50 Hz)**



Latency is not the only constraint to which a teleprotection application is subjected. The variation of the latency, also called jitter, (even within the 10 ms limit) is an important factor. Pilot-based teleprotection systems rely on a communications channel to send and receive information. This means that information is transmitted in both directions along the protected line, creating two communication paths: one forward and one reverse. For teleprotection to work properly, the latency must be the same for both the forward and reverse paths. The difference must be less than 2 ms, and be constant (within the jitter tolerance). This is often referred to as path asymmetry, or the difference between the forward and reverse path.

IEEE 1646 is an additional standard that defines delivery times for power substation applications. It generally defines latency for protection applications between 8 to 16 ms (one way).

3.3 Evolution from legacy to packet networks

Older generation teleprotection equipment used analog voice interfaces. The teleprotection equipment sent audio tones across a communications link that could be as basic as copper wires. Different frequencies are used for the guard tone (to signal that the TPR is operational) and for the command channels. These frequencies are all within the audible spectrum from 1100 Hz up to 4000 Hz. The frequencies and modulation schemes are defined by ITU-T standards. Commands are typically sent at very low speed (200 baud or lower) using frequency modulation. The physical interface used by analog teleprotection equipment is most commonly a 4-wire interface.

More recent teleprotection equipment now uses digital interfaces, which has evolved over the past 20 years or so. The most common digital interfaces found on TPR systems are RS-232, X.21, G.703, IEEE C37.94, and most recently, Ethernet interfaces.

TPR systems rely on a stable, symmetric, constant delay telecom network. Traditional telecom networks utilize TDM transmission architectures based on PDH/SDH/SONET to provide the communication channel between relays. The circuit switched nature with fixed frame lengths provides some guarantee of delay limit, delay stability, and transmission symmetry. Existing PDH/SDH/SONET networks are well suited to supporting current differential protection, which demands performance on the communications networks.

Over the past several years, there has been a growing demand for more Ethernet and IP based services for power substations. Engineers expect to be able to connect to their corporate intranet from within the substation. Analog telephones have been replaced by voice over IP (VoIP) models and CCTV cameras are moving to IP and multicast-based solutions. But perhaps the most important driver towards Ethernet and IP in the substation is the deployment of IEC 61850 based automation systems for the substation. These require Ethernet connectivity, which means more Ethernet switches and routers are being deployed in the power utilities communications networks.

While recent SDH/SONET equipment provides Ethernet connectivity, it is not well equipped to deal with the scale and complexity of Ethernet and IP services for large power utility networks. The non-MPLS IP routing and Ethernet switching technologies are not well suited to handling real-time data from applications such as SCADA and teleprotection, so other solutions must be considered.

In addition to the limitations of the existing power utility communications networks, several other business-related factors are driving the need for change. For example, power utilities must reduce costs and maintain or increase performance while making a transition to a smart-grid enabled status. This is driving power utilities to transform their telecom and corporate information and communication technology (ICT) department into integrated operations and ICT organizations.

The organizational transformation facing power utilities poses challenges for the network infrastructure because the operational telecoms applications are mission critical and have fundamentally different requirements for bandwidth, end-to-end delay, and jitter compared to corporate ICT applications. The latter have been deployed on Ethernet and IP networks for a few decades, while power utilities have relied on more conventional TDM technologies.

Bringing these two worlds together onto a common telecommunications infrastructure is a challenging task. However, the transformation is necessary because service providers are increasingly terminating support for legacy circuit transport such as 4W, DS1/E1, and so on.

3.4 Addressing the challenges with IP/MPLS

3.4.1 IP/MPLS overview

With the advent of IP and Ethernet devices in the power systems, many utilities are migrating their telecom networks to IP/MPLS to support next-generation interfaces and achieve a converged network infrastructure for existing applications, as well as for new smart grid applications. To meet teleprotection requirements, the network must maintain high-quality connectivity between relays, with QoS defined by limits on delay, delay variation, and asymmetry. Nokia's IP/MPLS network is a robust solution, offering the following features to address the challenges of teleprotection requirements for utilities:

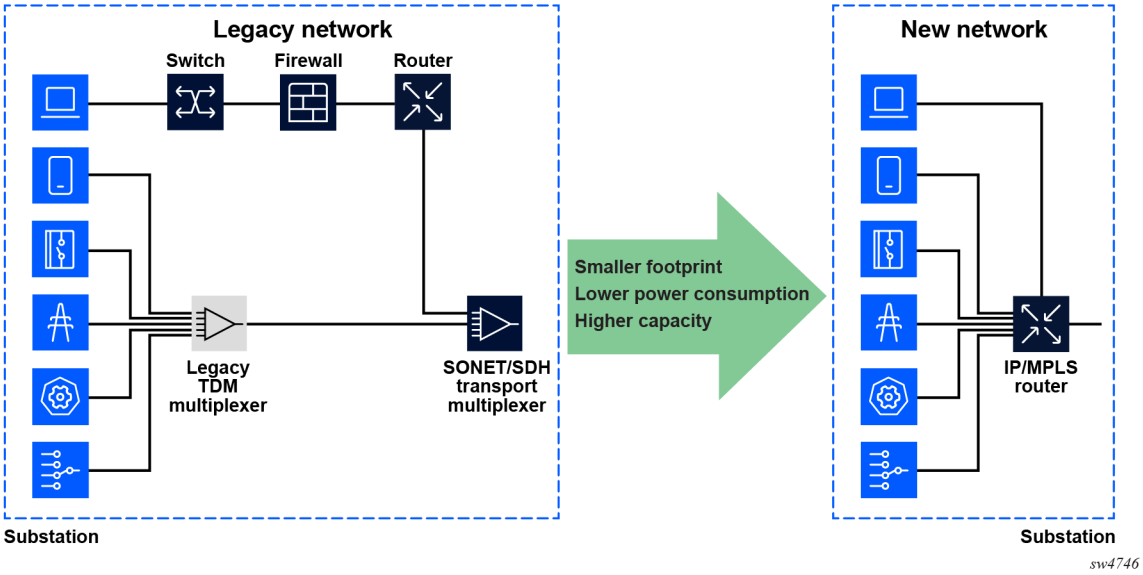
- interface support – natively supports common legacy teleprotection interfaces (4W/E&M, RS-232, X.21, G.703, C37.94) via circuit emulation services over packet switched network, structure-agnostic transport over packet (CESoPSN, SAToP), and next-generation Ethernet interfaces
- asymmetry control – actively manages jitter buffer depth to ensure symmetrical paths and prevent false trips using Nokia's patented asymmetrical delay control (ADC)
- synchronization – supports both synchronous Ethernet (Sync-E) for frequency and IEEE 1588v2 precision time protocol (PTP), including the power utility profile (IEC 61850-9-3), crucial for accurate timestamping and operation
- resilience – offers multilevel resilience including redundant links, diverse paths, resilient synchronization, node-level redundancy, and advanced application-level schemes such as active/active (1+1 or 1+3) hitless failover
- guaranteed QoS – uses label switched paths (LSP) for strict paths, high priority for teleprotection packets, and traffic engineering to meet latency and jitter targets

3.4.2 Latency and jitter considerations

A concern for utilities is whether the IP/MPLS network can meet the strict latency and jitter requirements for protection signals between transmission substations, in particular the ability to guarantee low-latency service. IP/MPLS is sometimes incorrectly perceived as connection-less IP technology that can only provide data transport with a “best-effort” QoS. However, MPLS provides a connection-oriented solution capable of multiple guaranteed QoS levels, and supports strict prioritization of latency-critical applications over other types of traffic.

The following figure shows the implementation of an IP/MPLS network for the utility transmission.

Figure 3 **IP/MPLS network for power utilities**



Another concern about IP/MPLS networks for teleprotection schemes is the idea that the statistical nature of packet networks impacts the performance of TPR systems. This has been disproved through extensive testing and implementation, and is not applicable if the utility takes suitable care in the engineering and provisioning of the private network based on IP/MPLS.

SDH/SONET networks can be provisioned to provide alternate routes for mission-critical traffic such as that between TPR systems. When operating correctly, the network provides less than 50 ms switchover time. This 50 ms time is the resiliency “reference” for any new telecom technology. IP/MPLS network technology provides several different fully standardized resiliency mechanisms to provide a switchover time of less than 50 ms. These include end-to-end alternate paths and MPLS fast reroute (FRR). MPLS FRR provides many pre-calculated alternate paths that can overcome any failure scenario in less than 50 ms.

The Nokia IP/MPLS network supports teleprotection including the following features:

- Label switched paths (LSP)

  LSP ensures all packets associated with a particular service, such as teleprotection, follow the same path. This is often referred to as strict paths and ensures that predetermined latency and symmetry targets are always met.

- Prioritization

  The packets associated with teleprotection communication can be assigned as high priority, to meet critical teleprotection requirements and assure reduced packet-delay variation through the network.

- Multiple synchronization options

  Several features ensure that the network is properly synchronized. The IP/MPLS routers are synchronized, which means they can provide a reference clock to the

relays that are connected using serial interfaces, using the network clock to generate the service clock. Next generation relays connected using Ethernet can also be synchronized because the Nokia IP/MPLS routers support ITU-T Sync-E and IEEE 1588v2 precision time protocol (PTP). See Synchronization and Synchronization design for more information.

- Interface support

  Nokia routers natively support commonly used teleprotection interfaces including E&M, RS-232, X.21, G703 and IEEE C37.94. Ethernet is also supported for the next generation, Ethernet-based relays. To reduce latency, it is advantageous to support a direct interface from the TPR to the IP/MPLS routers. This eliminates the need for a channel bank as well as additional latency and maintenance costs.

3.4.3 Emulating TDM functionality with IP/MPLS

An IP/MPLS network supports traditional relays using the circuit emulation service (CES).

The key design consideration for teleprotection over a packet network is how to minimize latency, jitter, and asymmetry. For an IP/ MPLS network, the telecom network latency for TDM traffic over IP/MPLS consists of packetization delay, network transport delay, and jitter buffer depacketization delay.

Packetization delay relates to the process of transforming TDM traffic into packet data that is directly proportional to the packet size and inversely proportional to the TDM interface speed used to fill the packet. For network delay, there is a fixed delay based on the physical-link speed and distances involved, and a variable delay depending on the number of hops (nodes) in between. Each node thereby adds transit equipment latency. Delay caused by jitter buffer and depacketization relates to the time required for a data packet to move out of the jitter buffer and be depacketized into a TDM stream connecting to the TPR system.

Most telecom network delays occur at the edge, where low speeds are present. Latency in the core depends on the number of nodes traversed. The use of link coloring and strict paths can be used to engineer the network to avoid path divergence and asymmetrical delays.

In addition, the IP/MPLS router or a GPS clock can provide a real-time clock pulse that timestamp the relay data, thus ensuring accurate data comparison and processing.

Packetization delay is also imposed at ingress, as the TDM data is packetized. Smaller payload sizes with a higher number of packets per second result in lower packetization delay and lower one-way delay. Larger payload sizes with a lower number of packets per second result in higher packetization delay and higher one-way delay. The packet payload size is configurable.

Nokia also provides non-stop service (NSS) capability to the applications riding over the IP/MPLS network. NSS means there is no impact to services carried on the device when there is a failure in a redundant component (for example, control, fabric, or power).

Network transport delay in the core depends on the number of nodes, the distance, and the communications medium, but results mainly from transmission delays. With IP/MPLS traffic

engineering, a service such as teleprotection follows a predetermined path through the network that meets the strict latency requirements.

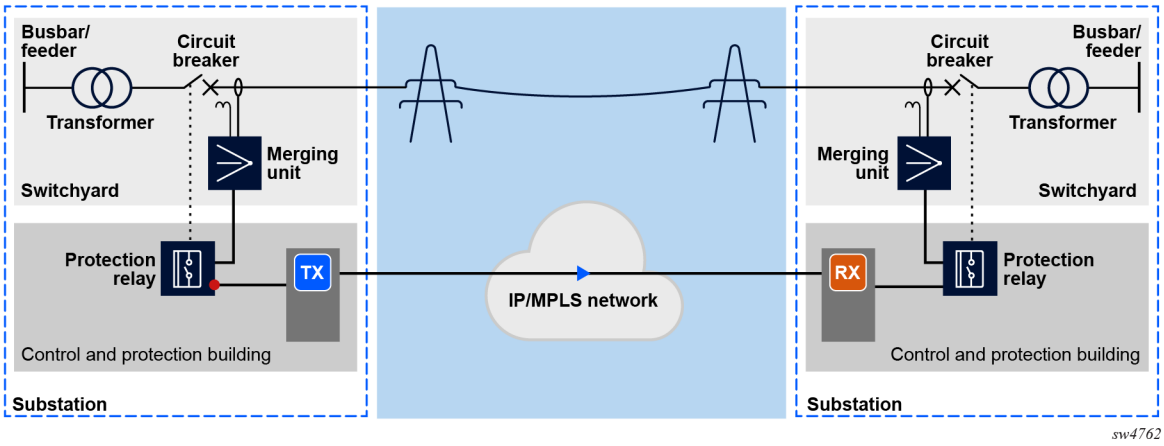
On play out, a CES uses a jitter buffer to ensure that received packets are tolerant to packet delay variation (PDV). This ensures the payload depacketization back into the TDM stream is successful, as is required for communication with the TPR. The smaller the jitter buffer, the less delay is imposed. However, the jitter buffer must also be large enough to ensure that jitter does not cause a communications failure on the TPR system. When selecting the jitter-buffer size, the user must consider the size of the TDM-encapsulated packets. Larger payloads require larger jitter-buffer sizes. A properly configured jitter buffer provides continuous playout, thereby avoiding discards caused by overruns and underruns. The principle of packetization and jitter buffer must be implemented in both directions between the protection devices. It is therefore important to ensure that the jitter buffer is aligned in both directions to avoid asymmetry, as described in the following section.

3.4.4 Synchronization

Network timing or synchronization is a key element that assures the correct functioning of TDM applications over a packet network. Over the past few years, several techniques have been developed to provide high-precision timing over packet networks. Sync-E and IEEE 1588v2 are the most important techniques to consider for use in MPLS networks that carry teleprotection applications.

Both technologies scale well in large networks and provide timing precision that is appropriate for the teleprotection systems. However, Sync-E has advantages because it is a Layer 1 synchronization solution that is totally immune to packet-delay variation. Sync-E also interworks well with SDH/SONET network synchronization, which is important in migration scenarios. Nokia IP/MPLS routers support both Sync-E and IEEE 1588v2, thus allowing complete flexibility in designing network synchronization.

Figure 4 **Data packetization across MPLS tunnel with jitter-buffer support**



Next generation relays now utilize Ethernet interfaces. Point-to-point relay communication is supported with an IP/MPLS network using Ethernet virtual leased line (VLL) services. Multipoint communication such as IEC 61850 GOOSE messaging is supported using virtual private LAN service (VPLS), ideally synchronized with the PTP power utility profile for synchronization.

3.4.5 Managing an IP/MPLS network for power utility applications

Although IP/MPLS can handling teleprotection traffic in a utility network, power utility operators have expressed concern about the complexity of managing an IP/MPLS network, including provisioning services and managing alarms. To address this concern, Nokia simplifies the management of IP/MPLS networks using a suite of network and service-management products that leverages many years of experience with PDH, SDH/SONET, and ATM networks. One main component of this suite of management products is Nokia's Network Services Platform (NSP).

A utility operator can use the Nokia NSP to manage thousands of nodes from a centralized user interface (UI). The NSP provides intuitive alarm management and inventory, and supports intent-based networking capabilities that continuously monitor and provide notifications about the configurations on every node in the network. The NSP provides visual analysis of all the paths and the services in the network, and raises an alarm if a path is rerouted and falls outside the limits set by the service SLA policy. The NSP also provides an easy re-alignment of the network, simplifying lifecycle management for busy utility organizations.

It is important to have the tools to manage the elements, services, and protocols, and it is equally important to be able to plan. For this reason, the NSP also provides the path computation element (PCE). PCE incorporates a real-time simulator to perform network simulations. This enables users to look at different possible scenarios if link or node failures occur.

3.4.6 Bandwidth and latency considerations

As described in Emulating TDM functionality with IP/MPLS, there are underlying principles of the packetization technique used to send data from a TDM I interface (for example, RS-232) or a 64 kb service (for example, T1/E1, G.703CoDir, and C37.94), across an IP/MPLS network. In most cases, an optical fiber offering plenty of bandwidth is available, which means there is no immediate need to focus on the bandwidth consumption impact of packetization. However, there are other cases where no fiber optic network is available, for example, when using microwave radio links or low bandwidth leased Ethernet circuits. In these cases, it is important to know in more detail how the parameter settings used to configure the packetization system impact the bandwidth requirements.

Packetization is the process that occurs when legacy interface data (serial data or data coming from DS0 channels in a T1/E1) is presented to a router's ingress port. The router must put a series of bytes into packets (encapsulation) at a certain constant rate, and route them to their destination. This is done according to a standard mechanism as defined in the CESoPSN standard (RFC 5086). An alternative mechanism to transport TDM over a packet network is to structure agnostic

transport over packet (SAToP) as standardized in RFC 4553. This method does not take the DS0 channels into consideration and basically transports the complete E1 or T1 transparently.

The jitter buffer assures a smooth play-out of the serial data on the egress port and compensates for packet-delay variations that may occur during transit of the packet through the network and intermediate network nodes.

When a CESoPSN or SAToP circuit is provisioned on IP/ MPLS routers it is important to define the payload size (in bytes) at the ingress port and the jitter buffer depth (in ms) at the egress port.

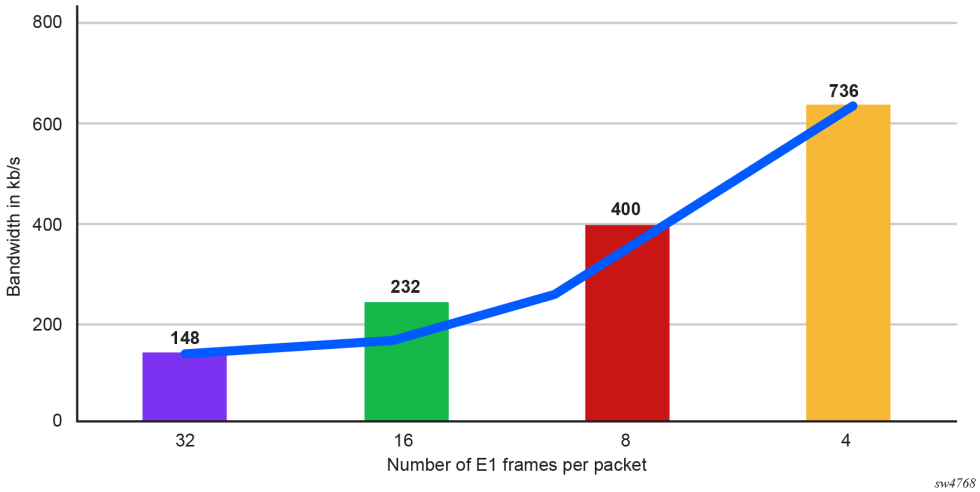
3.4.6.1 The impact of payload and jitter buffer

The configuration of the payload size has an immediate impact on the number of packets that are generated and the bandwidth consumed on the network ports. The payload size is directly proportional to the packetization delay and inversely proportional to the bandwidth used, so there is a tradeoff. However, given the strict latency requirements for TPR circuits, small payload sizes are required. See the *Nokia Teleprotection over packet networks eBook* for more information about calculating payload sizes.

Careful calculations are required when transporting TDM traffic over packet networks. For instance, when available bandwidth is constrained over copper lines or microwave links, attention must be paid to the configuration parameters used for the packetization of the data. It is important to understand the boundaries of the application in terms of maximum latency, apply a margin to it, and work the numbers to find the right balance for the end-to-end latency and bandwidth requirements. In networks where the links are built with fiber-optic connections, bandwidth is less of an issue, and it is acceptable to tune the parameters for the lowest possible latency.

The following figure shows a sample graph of how the number of E1 frames put into a single packet impacts the bandwidth utilization.

Figure 5 **Sample of packetization bandwidth**



3.4.7 Asymmetry control

Current differential fault protection, distance and current differential protection, and their principles of operation are described, in Current differential fault detection. This includes how current differential protection systems exchange information about currents they are measuring at regular intervals.

In an AC system, voltage and current alternate at almost constant frequency, which means it is important for the current differential protection system to know the time when samples are created and sent from a remote protection system.

To ensure the receiving protection system knows the time, an accurate source of time is required. One of the most common ways of providing time is to connect a GPS receiver to the protection device. While using GPS receivers is relatively common in some power utilities, it is often considered to be a cause of concern because GPS satellite signal reception can be easily jammed. Antennas can be subject to bad weather conditions and in some situations the precision of the civil GPS data can be altered, thus impacting the operation of the protection systems.

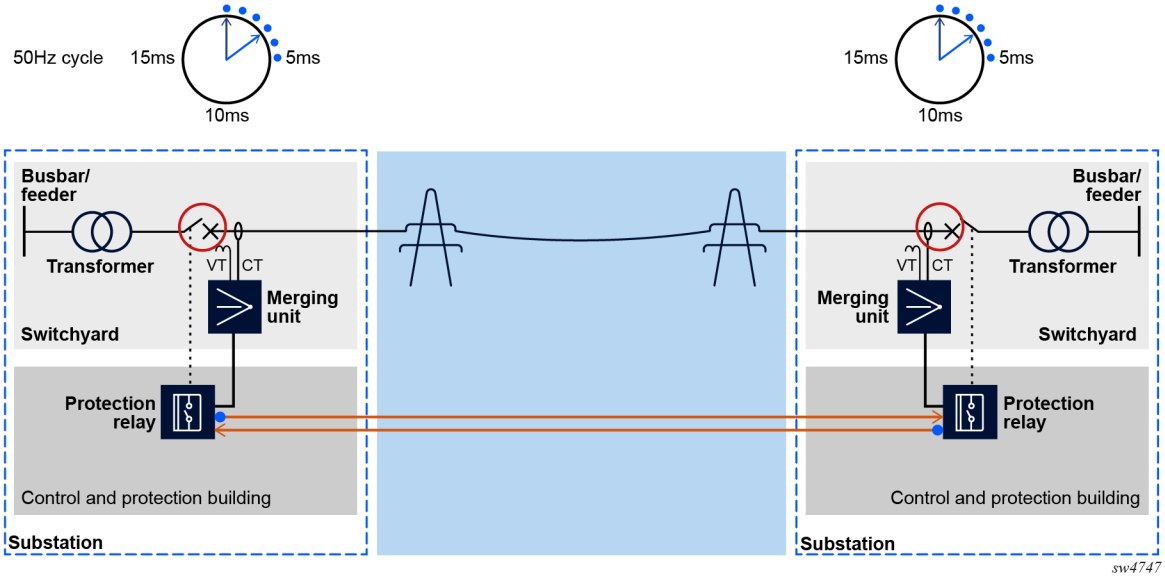
For these reasons, most power utilities implement other means of distributing time information in their networks. In this regard, the importance of synchronization is an underlying principle; see Synchronization design for more information.

In many cases, current differential protection systems use time stamps when sending their phasor data to the remote system, using their internal clock as a time reference to compare their locally-measured data with the data they receive from the remote end. However, unless they are connected to a GPS receiver or another time source, the internal clocks are not kept in sync. They can obtain frequency synchronization from the telecom network they are attached to, and in the best case they can get a pulse-per-second signal if the telecom network is capable of providing this service.

The protection systems are engineered to protect a high voltage power line and the attached electrical infrastructure. They are configured as a function of the level of voltage and the current the line carries, as well as the length of the line. These parameters are static and because the length of the power line doesn’t change, the protection systems often take a fixed amount of propagation delay into consideration. They derive the fixed latency from the exchange of data with the remote protection system. This is how a protection system that receives phasor data from the remote end can compare the data with the values measured at the local end, using the propagation delay offset. The difference should be close to zero but can be several hundreds of microseconds.

The following figure shows the principle of operation.

Figure 6 **Fixed latency offset principle of operation**



When circuit switched technology is used, dedicated fibers or other dedicated point-to-point connections are used between the protection relays. The delay or latency between the two end points remains fixed.

While both protection systems on either side of the line calculate the latency between them through the exchange of time-stamped data, it is assumed that the latency is the same in both directions. There is a certain tolerance towards the asymmetry between forward and reverse latency because there is always some amount of buffering occurring in any telecommunication system. This may be several bits, bytes, or packets.

The tolerated asymmetry that is normally configured in any differential protection system can vary greatly from one implementation to the other. If a condition occurs where the latency in either direction changes, the protection system interprets this as a fault on the line. This is because the asymmetry affects the run-time latency calculation in the protection system, which in turn compensates the received phasor data with the wrong amount. This causes the system to trip the circuit breaker if the error exceeds the tolerance. This is referred to as a “false trip” and must be avoided.

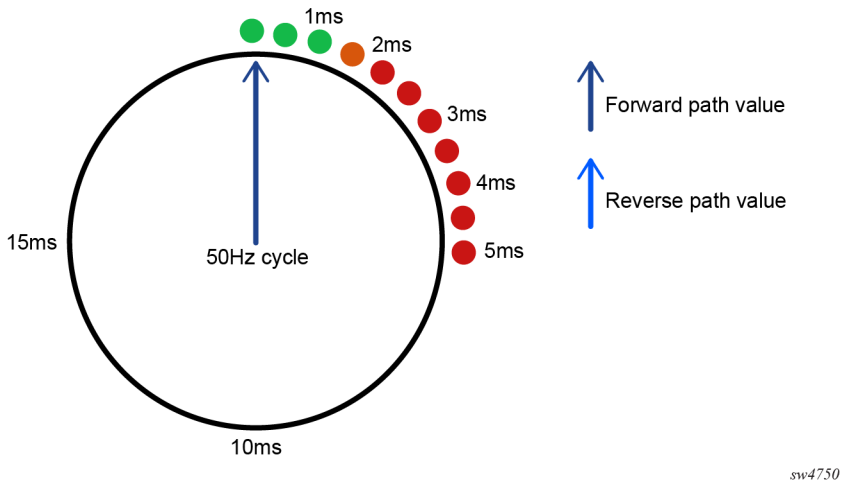
The asymmetry tolerance is primarily tied to the following aspects:

- voltage level of the protected line
- the margin the power utility allows for the difference in the current measured at both ends of the line

Nokia has observed large differences in how power utilities have configured their current differential protection systems. At the ultimate limit, protection systems were tolerating up to 2 ms of asymmetry. In other cases, the protection systems were configured for asymmetry tolerances in the range of 500 microseconds.

The following figure shows a phasor cycle at 50 Hz and provides an indication of the angle difference for increments of 500 microseconds up to 5 ms.

Figure 7 **50 Hz cycle and symmetry tolerance**



Differential protection systems are sensitive to end-to-end latencies but often allow up to 10 ms or more. However, the difference between the forward and reverse latency must be much less, typically well below 2 ms. This has been observed when analyzing the behavior of protection systems connected to a test network, where different impairments are introduced such as symmetrical latency increases, asymmetry conditions, and packet loss as possible causes of asymmetry.

Asymmetry can be caused by several things. The path length in the telecommunication system could be different between the forward and reverse direction because of a mistake in the configuration of the circuits. With Nokia's NSP, these human-error path-divergent situations are avoided, because the system always configures symmetrical paths.

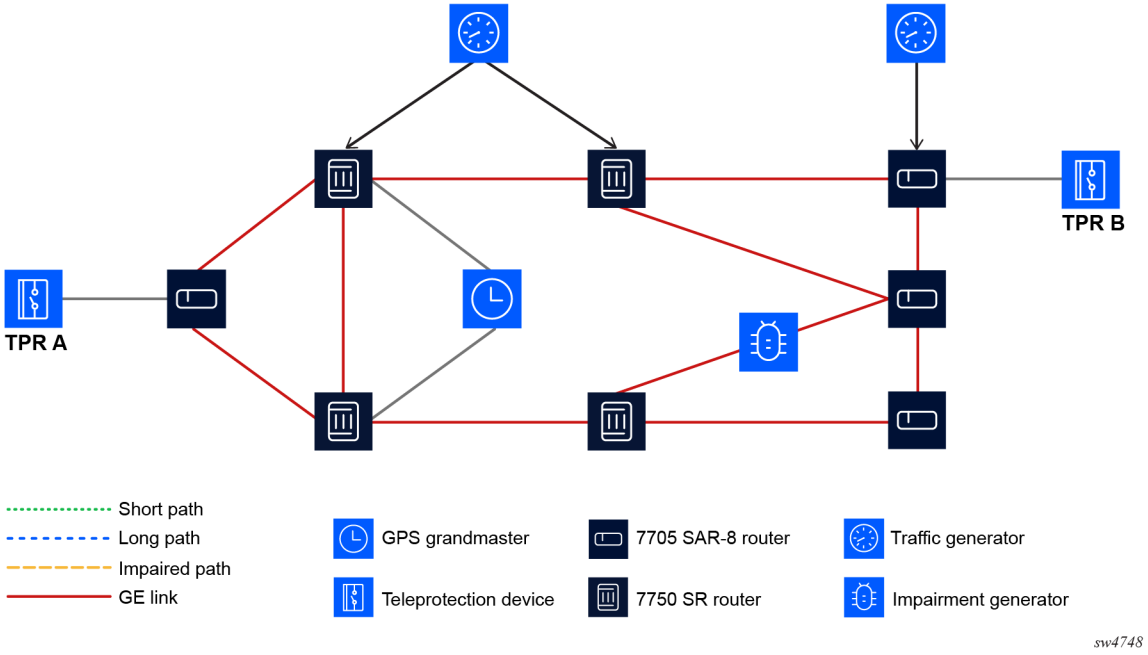
If TDM data is packetized, it is possible that packet delay variation (PDV) in the network has caused jitter buffers to vary in one direction but not in the other. The larger the number of nodes in between two endpoints, the larger the potential PDV becomes. Furthermore, a lack of proper traffic engineering and QoS modeling could adversely impact the latency of the packets carrying teleprotection data if network use is increasing and congestion situations occur.

This problem occurs even sooner when low-speed network links are used, for example E1/T1 circuits, and the mix of traffic consists of highly sensitive but relatively low-speed real-time data and bandwidth-consuming applications such as surveillance video.

Asymmetry can also cause synchronization issues. If the whole telecommunication system is not properly sync-locked to a stable source, a gradual drift may occur in the system clocks, which can accumulate over several network hops until the asymmetry exceeds the tolerance of the protection systems. See Synchronization design for more information.

The following figure shows impairment tolerance testing.

Figure 8 **Impairment tolerance testing**



3.4.8 Asymmetrical delay control

To avoid problems caused by jitter-buffer misalignment, it is important to control the jitter buffer depth of the circuits that carry critical data such as teleprotection. This can be done by monitoring the jitter-buffer depth and setting thresholds.

Whenever a threshold is exceeded, an alarm is raised and the user can decide to restart the CES involved. While this jitter-buffer monitoring method works, it is a reactive approach that puts extra burden on the network-management system.

Nokia recognizes possible issues may occur because of jitter-buffer depth changes caused by different phenomena (discussed in this section), and the challenges this presents to those who manage the network and the critical services. This led to the development of the patented ADC feature, which is designed to keep the jitter buffer within the configured value. This keeps the jitter low, thus avoiding possible false trips of the protection equipment. The ADC feature supports priming of the CEM circuit from the ingress to the egress point with sample data. This supports training the jitter buffer at the egress end to go to the configured value, while taking the actual network load into consideration. This process is initiated at the startup time of the circuit and can be repeated at regular intervals.

The effectiveness of ADC has been demonstrated at Strathclyde University in Glasgow in different scenarios involving congestion, link impairment, and synchronization clock drift. In each of these scenarios, current differential protection systems were used with different settings for current differential tolerance. At the highest sensitivity, the protection relays would trip as soon as a differential delay of 653 microseconds occurred.

3.4.9 High level network design principles for utility networks

This section describes considerations when designing resiliency for teleprotection services.

Grid protection and control (PAC) services are the most critical applications that run on a power utility network. The network must provide maximum availability to the PAC applications by avoiding possible single point-of-failure situations in all parts of the network. This requires implementation of resilience at the following three levels:

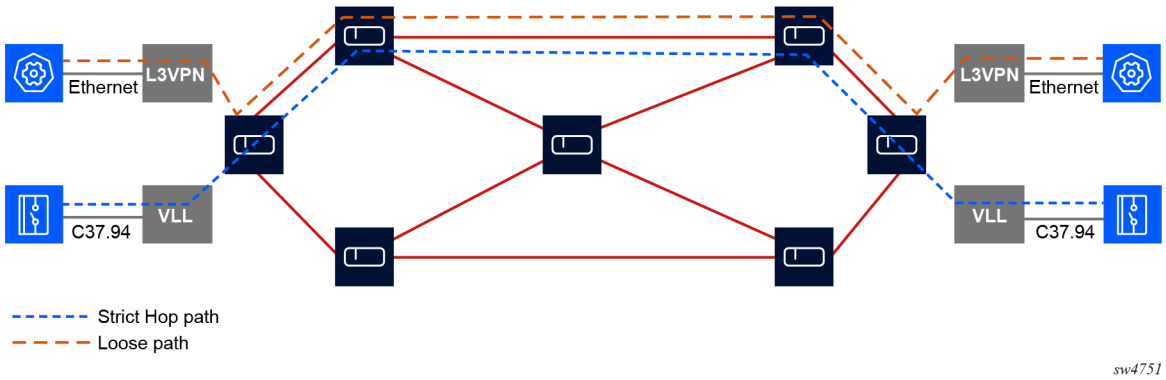
- network
- nodes
- applications

For the network, the best design for PAC resiliency uses dual attached relays. Each relay interface is connected to the IP/MPLS router with two diverse strict paths configured between the relays. Both paths can have different latency characteristics, which the relays handle as two independent connections.

If the relays only have a single attachment, the network must cater to the link redundancy.

The following figure shows differences between strict and loose paths and their failover scenarios.

Figure 9 **Strict and loose paths with failover scenarios**



3.4.9.1 Using active/standby paths

For the failover mechanism, the network administrator can select the active/standby pseudo wire (A/S-PW) mechanism to allow the network to switch to a diverse path in case the primary path has a failure. A/S-PW relies on failure-detection mechanisms, which can take more than 50 ms depending on the type of failure that occurs. For PAC services, this failover time is too long. In addition, if the backup path is significantly longer, the protection relays may consider this to be a fault and consequently open a circuit breaker causing a “false trip”.

To prevent a false trip from happening, Nokia offers the ability to run ADC upon failover. This keeps the interface toward the protection relays down while the ADC process aligns the jitter

buffers in the forward and reverse directions. After this process finishes and there is a symmetrical pseudo wire service running, the interface towards the protection relays is enabled again. This triggers the relays to re-start the process of determining the link latency between them and resume operation.

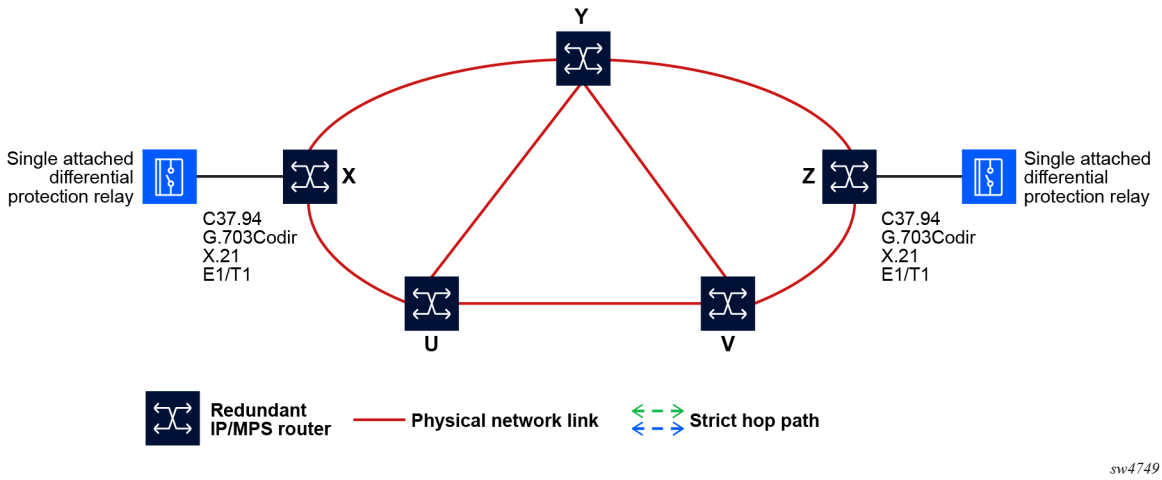
3.4.9.2 Active/active (1+1) resilience

A further evolution of the “graceful failover” with active/standby pseudo wires is the active/active or 1+1 resilience scheme. This resiliency scheme provides two concurrently active and diverse paths between two endpoints in the IP/MPLS network, enabling two protection relays, attached by means of legacy interfaces (C37.94, T1/E1, and so on), to have a fully resilient communication service between them. This feature, also known as active multipath (AMP), is the focus of this document.

The following figure shows active/active resilience operation. The benefits of this solution include:

- higher tolerance for failure scenarios
- protection service not impacted by multiple failures (unlikely) of the links, or nodes between nodes with relays attached

Figure 10 **Active/active (1+1) resilience**



The active/active service uses the packet replication functionality from the IP/MPLS router to take the TDM data stream from the protection relay and send it across the network across the two diverse paths simultaneously. At the egress side of the network, the IP/MPLS node uses a combiner function to eliminate duplicate frames received across the two paths and assures a smooth TDM data-stream playout to the receiving protection relay using the jitter buffer. The benefit of this active/active pseudo-wire solution is the protection relays do not notice if multiple failures happen on a path in the network. If both paths fail, the protection relays see a “comms failure” message, and the protection service is interrupted.

Currently the active/active service is configured to resume when both paths are restored. One of the “downsides” of this solution is the latency is determined by the longest path, and therefore the jitter-buffer configuration on the Cpipe must increase to accommodate for the difference between the fastest path and the slowest path.

To further enhance the active/active capability, Nokia supports using four concurrently active paths between the protection relays, for cases where there are more than two potential transport paths. This avoids separate failures in two paths that affect the protection service. The protection service is still impacted if a major failure occurs, for example, a power or interface failure in either node X or node Z where the relays are attached (see the previous figure).

All these scenarios relate to protection relays that use the legacy TDM interfaces, which still constitute most of the installed base of protection relays. Transport for next-generation protection devices using Ethernet interfaces is not described in this document because the complexities of packetization, synchronization, and jitter handling are largely removed from the network for those types of devices.

4 Network design and implementation

4.1 MPLS design for TPR systems

4.1.1 Strict path LSP relays using standard Cpipe design

The following example shows an MPLS router configuration template that applies to relay circuits that have two types of paths and do not use AMP.

Example: MPLS router configuration for relay circuits with two path types and no AMP

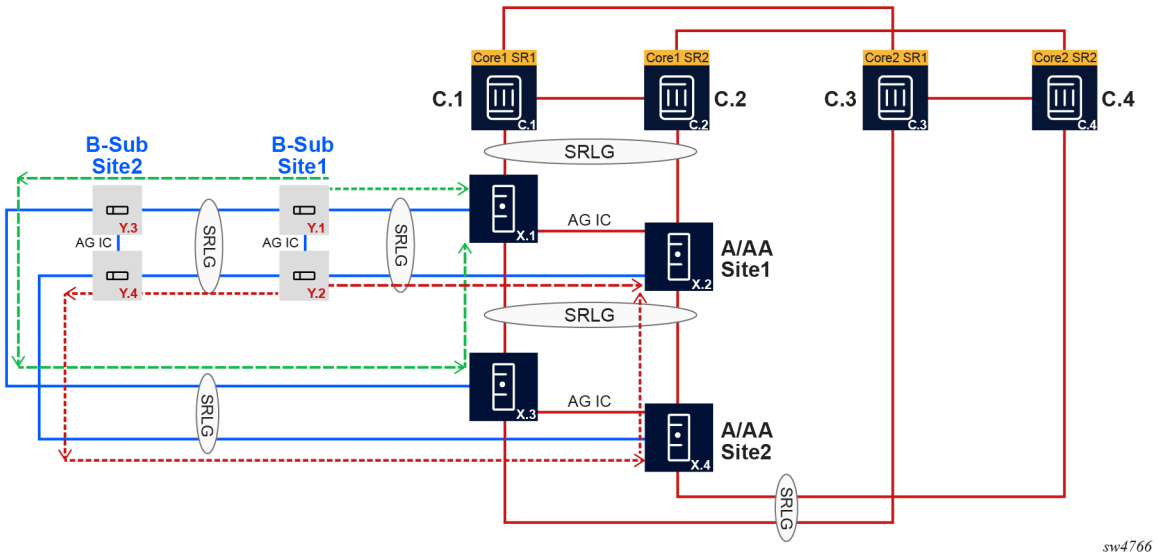
```
/configure router mpls
        path "To-<Dest.Site Name>:Via-<NH site>"
           hop 1 <NH-IP1> strict
           hop N <NH-IPN> strict
           no shutdown
        exit

        path "To-<Dest.Site Name>:Via-<NH site2>"
           hop 1 <NH-link-IP1> strict
           hop N <NH-link-IPN> strict
           no shutdown
        exit
         lsp <see naming section>
                to <far-end System IP>
                cspf #removed for inter-area and see note below
                retry-timer 5
                vprn-auto-bind exclude #Prevents use for corporate/control VPRN
                primary "To-<Dest.Site Name>:Via-<NH site2>"
                exit
                secondary "To-<Dest.Site Name>:Via-<NH site>"  #not used with AMP
                     standby
                     srlg           #design/topology specific for example, for dual-
ring required to keep secondary path disparate.
```

```
                exit
                no shutdown
        exit
```

The following figure provides a reference for the MPLS configuration template. Two substations are shown with dual-relay A and B circuits between them. The primary path for circuit A must be fully diverse (node and link) from the primary path for circuit B. Secondary paths are also used for both LSPs, to keep both the relays up during link and node maintenance along the path.

For cases where AMP is used within the Cpipe, there are two SDPs, each using an LSP with a single strict path.

Figure 11 **MPLS relay circuits with two path types and no AMP**



4.2 Synchronization design

CES transport has strict synchronization requirements in general, and for TPR circuits in particular. This section provides a summary of the synchronization network design considerations and the capabilities of the MPLS devices that are targeted for this application.

4.2.1 7705 SAR sync

The Nokia 7705 SAR product family is designed for legacy networks requiring CES transport of TDM traffic. The following table summarizes the timing capabilities on the 7705 SAR.

Table 2 **7705 SAR timing capabilities**

Node	SSU clock reference sources	Input reference options
7705 SAR	• External via CSM sync port.	• External – 2048, 10MHz

Node	SSU clock reference sources	Input reference options
	• Line-timed via a port's received clock • Sync-E supported • 1588v2 supported • Adaptive using ingress packet stream from TDM VLL **Note**: • 7705 SAR-Hc supports Sync-E and PTP but does not have external clock reference inputs or slots for GNSS. • 7705 SAR-Hm and Hmc do not support Sync-E or PTP because they are VSR based nodes.	• GNSS reference (via GNSS MDA) • Line Timed – Via TDM (T1/DS3/OC3) ports • Line timed via Sync-E • RFC 1588v2 reference

The 7705 SAR CSMv2 provides a 1.0/2.3 coaxial connector for external synchronization input. The CSMv2 supports 2048 (G.703 format) and 10 MHz input signals. With redundant CSMv2s, a Y-cable (Nokia part # 3HE03401AA) can be used to connect to the inputs of both CSMv2s.

Alternatively, each 7705 SAR has two timing references (Ref1 and Ref2). As shown in the preceding table, these references can bind the system clock to the following timing sources:

- line-timing references (either TDM or Sync-E ports)
- GPS via the GNSS MDA
- remote RFC1588v2 clock source (timeTransmitter or boundary)

4.2.2 Sync-E

Without Sync-E, Ethernet ports transmit with an accuracy of +/- 100 PPM. Clock recovery using Sync-E allows IP (MPLS) nodes to transmit Ethernet frames based on the system clock. This in turn allows neighbor nodes to derive clock references from the connected Ethernet ports, similar to how TDM/SONET networks use line-timing on nodes to set their system clocks.

Sync-E (G.8261/8262) is the newest form of Layer 1 synchronization, designed for packet networks with Ethernet interfaces. Sync-E inherits the ease of design and deployment of other Layer 1 sync technologies. In comparison with packet-based clock synchronization protocols (such as 1588v2 PTP), Sync-E offers higher accuracy in frequency synchronization while being immune to the impacts of packet loss, packet delay variations, and network path asymmetry. In addition, the nodes require only frequency sync (not phase sync), making line timing (Sync-E) the primary nodal synchronization method utilized in this design. However, one consideration is that all active Ethernet ports and devices in the synchronization chain (including those used for transport) must support Sync-E.

For transport links that include devices that do not support Sync-E, another method is required to transport the clock to the far-end nodes (assuming there are no GPS/BITs at the remote sites). For those links, RFC-1588v2 (PTP) can be used. This scenario applies to any remote sites that are

connected via leased Ethernet service (E-LAN or E-Line) or any remote sites connected over legacy MW radios that do not support Sync-E or SSM.

For this scenario, the MPLS PE at the remote site (reachable via the leased service or non-Sync-E capable links) is provisioned with a PTP primary reference, configured as a PTP timeReceiver peering with the MPLS PE at the far end of the link that is deriving synchronization from the MPLS network. That remote MPLS PE is then provisioned as the PTP primary (timeTransmitter).

Note: When only frequency sync is required, any Nokia MPLS PE can be the PTP timeTransmitter (no external grandmaster clock (GMC) or GNSS is required). However, if phase/TOD sync is also required, the remote PE must be a standby to a PTP GMC. The 7705 SAR nodes can act as a GMC only if they are equipped with a GNSS receiver MDA.

The G.8263 standard adds support for the Synchronization Status Message (SSM) or Ethernet Synchronization Message Channel (ESMC) signaling information that relays clock quality levels (QL). This helps the network timing architecture adapt to link, node, and device failures.

4.3 PTP

The precision time protocol (PTP) is a timing-over-packet technique defined in IEEE 1588-2008. PTP provides the capability to synchronize the network element to a stratum 1/PRC-traceable source through a network that may or may not be PTP-aware. PTP has the benefit of being able to transport both frequency and phase (time) synchronization. This contrasts with Sync-E, which only provides frequency.

4.3.1 Timing devices

The following are the basic types of PTP devices:

- ordinary clock (timeReceiver or timeTransmitter)
- boundary clock
- end-to-end or peer-peer transparent clock

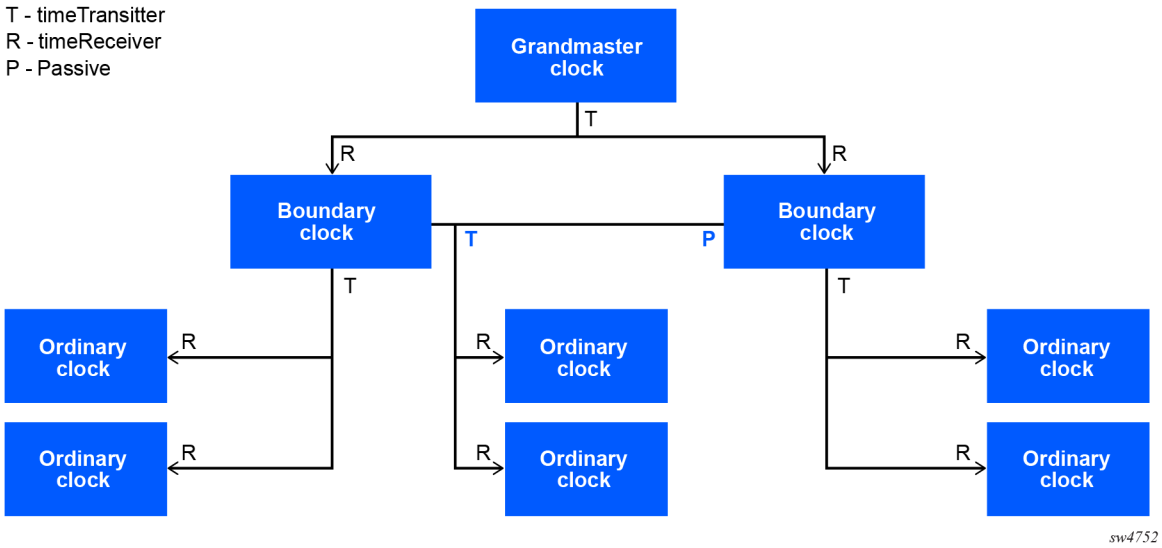
The 7705 SARs and 7750 SRs support the ordinary clock in timeReceiver or timeTransmitter mode or the boundary clock functions.

Note: If time of day (TOD) or phases sync is required, an external GMC is needed or the 7705 SAR that acts as the GMCs must use a GNSS synchronized to a GPS.

The PTP node communicates with peer IEEE 1588v2 clocks. These peers can be ordinary primary clocks, ordinary standby clocks, or boundary clocks. Each peer is identified by the IPv4 address to be used for communications between the two clocks. There are two types of peers: configured and discovered.

The following figure shows a general PTP topology with a GMC timeTransmitter, two boundary clocks, and six ordinary timeReceiver clocks.

Figure 12 **PTP boundary clock topology**



The PTP node operating as an ordinary timeReceiver clock or as a boundary clock should have configured peers for each PTP neighbor clock from which it might accept synchronization information. The ordinary timeReceiver clock initiates unicast sessions with configured peers.

4.3.2 PTP configuration considerations

The PTP protocol accuracy can be impacted by network factors such as packet loss, latency, and jitter. For this reason, boundary clocks are required to limit the number of non-PTP aware IP hops between timeTransmitter and timeReceiver, because each hop adds latency and PDV.

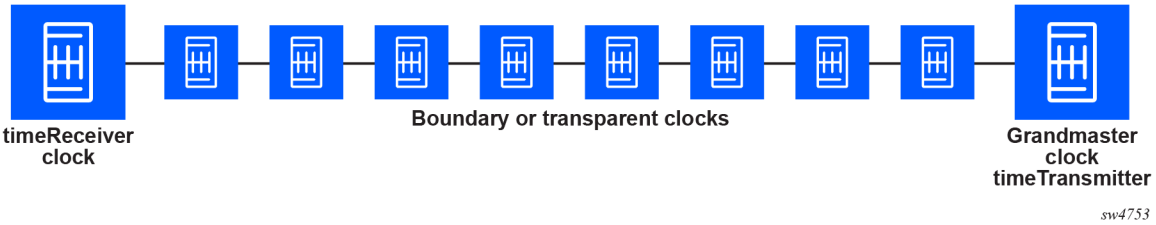
To eliminate issues with PDV, the following configuration must be applied:

- Nokia recommends no more than 20 hops from the clock source in the clock network synchronization design.
- To limit PDV and latency and packet loss during congestion, all PTP packets must be carried in a high-priority QOS FC to limit buffering. The DSCP marking used for PTP is set via the security group tag quality of service (SGT QoS).
- For network group encryption (NGE), any interfaces that are intended to run interface-level NGE (currently only leased-line interfaces), an IP-exception policy must be defined to pass the PTP packets unencrypted.
- Additionally, sites can act as boundary clocks by deriving the clock from their adjacent nodes. In turn, the boundary clocks act as timeTransmitter clocks for their adjacent nodes.

Note: This essentially means every node in the network is configured as a PTP boundary clock.

The following figure shows the configuration of network nodes as boundary and transparent clocks.

Figure 13 **PTP boundary clock**



In addition to the mentioned considerations related to latency, UDP ports 319 and 320 are also required in the CPM filter IP filter to process PTP packets.

4.3.3 PTP profiles

4.3.3.1 7705 SAR profile support overview

The IEEE 1588v2 standard includes the concept of PTP profiles. These profiles are defined by industry groups or standards bodies that define how IEEE 1588v2 is to be used for an application. The 7705 SAR currently supports the following profiles:

- ieee1588v2-2008 – original 7705 SAR default PTPv2 profile that uses IP or Ethernet encapsulation
- itu-telecom-freq G.8265.1 – frequency only using IP encapsulation.
- g8275dot1-2014 – telecom profile for frequency and phase; all nodes must be PTP aware (BC)
- g8275dot2-2016 – For networks with routers without PTP support, this adds transparent clock.
- iec-61850-9-3-2016 and c37dot238-2017 – for NG IP substations; only supports Ethernet encapsulation using multicast

For all profiles supported by the 7705 SAR, the communication between clocks utilizes the unicast communication procedures of the IEEE standard (as opposed to the multicast communications used with G.8275.1). The transport layer for IP encapsulation uses UDP ports 319 and 320.

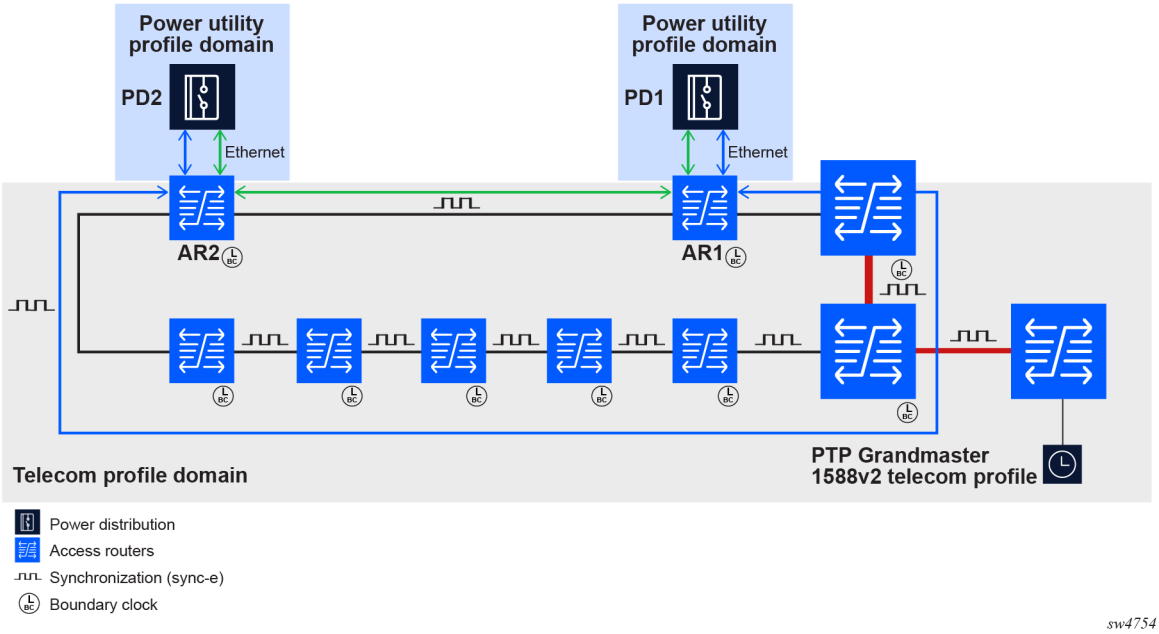
The IEEE 1588v2 standard has evolved over time, and different profiles have been developed, recently adding the power utility profile (IEC/IEEE 61850-9_3, and C37.238-2017) to support specific power utility applications. The PTP profile for power utility automation is based on Layer 2 Ethernet encapsulation and was conceived for station bus and process bus LAN implementations

within a substation. It is therefore not suited for use across a wide-area network, which typically uses the ITU-T G.8275.1 telecom profile for phase/time synchronization, and scales better for large networks using IP encapsulation.

A next-generation substation requires the network to provide frequency and phase syncing. This requires using PTP to substation devices. The MPLS PE must also provide an interworking function between the PTP telecom profile on the IP/MPLS network and the power utility profile (Ethernet encapsulated) on the Ethernet ports of the access routers connected to the protection devices. The following figure shows interworking of the PTP telecom and utility profile (Ethernet encapsulated) on access router ports.

Note: In the following figure, the intermediate MPLS PEs between the end stations and the GMC are provisioned to be boundary clocks, as described in PTP configuration considerations.

Figure 14 **PTP telecom and utility profile interworking**



4.3.3.2 IEC/IEEE 61850-9_3 and C37.238-2017

As described in the previous topic, the IEEE 1588v2 standard has developed different profiles to support specific power utility applications (IEC/IEEE 61850-9_3, and C37.238-2017). The two utility profiles have the following characteristics:

- The utility profiles support only Ethernet encapsulation with multicast addressing and the peer delay mechanism using MAC 01-80-C2-00-00-0E.
- PTP packets must be untagged (VLAN tagged PTP packets are dropped).

- Sync-E can be used for frequency recovery, to optimize performance when used for phase/ToD.
- One-step clock is supported with a default domain ID of 0.
- The C37.238-2017 profile is an extension to IEC61850 that adds the IEEE_C37_238 TLV in Announce messages between the parent and child clocks to report the GMC ID and a time-inaccuracy parameter.

4.3.3.3 7705 profile interworking (IWF)

The 7705 SARs supports both single-clock and multi-clock profile interworking. By default, all ports are associated with the primary (telco) profile. This means to use the alternate profile (toward substation gear) the ports must be explicitly assigned to that profile under the system or PTP clock.

The following requirements apply:

- For single clock interworks between the primary profile (G.8275.1) and the alternate Ethernet encapsulated utility profile (assigned to the clock CSM under the system PTP context), the following apply:
  - Only ports using the primary profile are candidates for the PTP clock source using BTCA.
  - The message rate used for the Announce messages is controlled by the **log-anno-interval** command configured for each profile in use. The Sync and Delay message rates are controlled by the per-port configuration.
- For multi-clock interworks between the G.8275.2 (IP encapsulated) as the primary profile, and the alternate Ethernet encapsulated utility profile, the 7705 SAR-8 and 7705 SAR-18 on 8-port gigabit Ethernet adapter cards and 6-port Ethernet 10 Gb/s adapter cards support multi-clock interworking.

4.4 General service design

4.4.1 SR OS services overview

A service is a logical entity created on a node that defines the service type (VLL, VPLS, VPRN) as well as the logical interconnects or interfaces that are part of the service on the node. Each service is uniquely identified by a service ID and an optional service name within the node.

Note: The service ID must be unique per node. Nokia also recommends using unique service IDs globally (across nodes), although this is not enforced within the CLI. The NFS NFM-P automatically assigns the next available ID not already in use.

The SR OS service model uses logical service entities to define the service and its traffic flow. These logical service entities provide a uniform, service-centric configuration management, and a basic model for service provisioning.

The following logical entities in the service model are used to construct a basic service:

- Customers

  The customer entity includes a logical customer ID with a description field for customer name and contact information. The default customer ID is 1.

- Service access point (SAP)

  Each service type is configured with at least one SAP that identifies the customer interface point for a service. The SAP configuration requires that Ethernet port parameters are configured (as access or hybrid,) prior to adding to a service SAP. The SAP is a local entity that is uniquely identified by the physical Ethernet port, encapsulation type, and encapsulation identifier. Depending on the encapsulation type, a physical Ethernet port can have more than one SAP associated.

- Service distribution point (SDP)

  SDPs have the following two components:

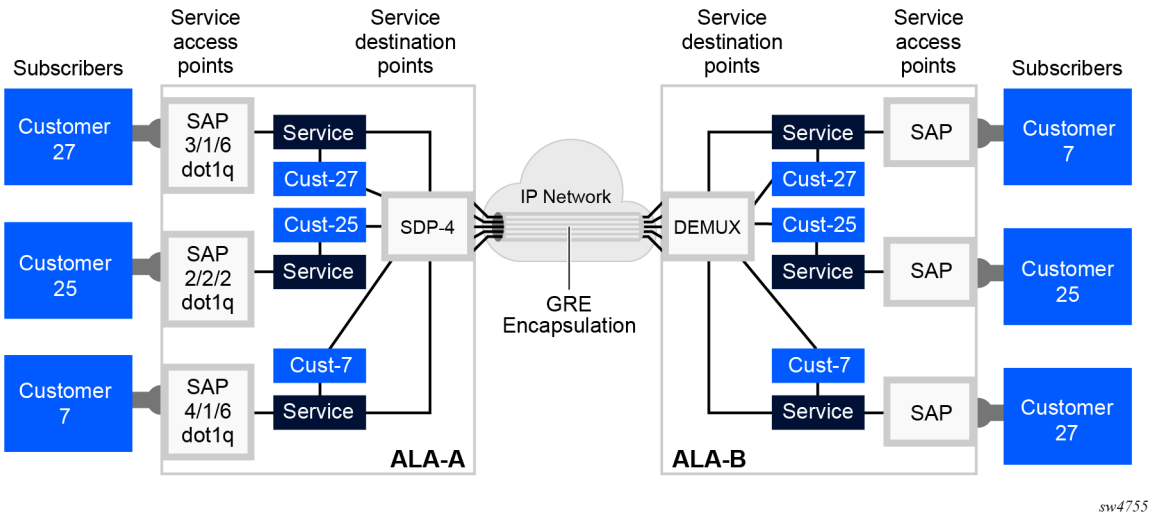
  - Transport tunnels between PEs are configured in the **configure service** context and bound to GRE tunnels, LDP LSPs, RSVP LSPs, or BGP tunnels (RFC-3107).

    Note: For this design the SDPs use RSVP.

  - Service tunnels are spoke SDPs or mesh SDPs provisioned within a given service context (VLL, VPLS). You can bind many services (and service tunnels) destined to a PE to the same transport tunnel (SDP) as shown in the following figure.

The following figure illustrates the relationships between the entities making up the service model.

Figure 15 **SROS service entities**



4.4.1.1 Customer ID

The customer ID is a basic entity that the user must assign when creating the customer account, to uniquely identify the customer. It is used primarily by the network management system to facilitate grouping services together and for troubleshooting when listing services on the network management system (NMS) or via the CLI. The following are some groupings commonly used.

Note: The customer ID is defined when the service is created and to change it the user must delete and recreate the service.

For operational benefits it is generally recommended to use a specific customer ID for internal services built for test purposes (Y.1731, or temp services for link test and turn-up). Additionally, it is useful to have different customer IDs for different categories of traffic, for example, SCADA, TPR/relays, management traffic, and IT/enterprise. This is based on customer preference. For example, some customers may prefer a single ID or one ID for all OT services and another ID for all IT management services. Other larger customers prefer more granular IDs.

4.4.1.2 Service ID

The service ID is broken into ranges representing the type of service being employed. The Service ID is an integer with a value in the range 1 to 2147483647. Nokia recommends that the service ID be unique for all services.

Similar to the customer ID, the service ID is assigned when creating the service, and changing the service ID requires deleting and recreating the service. The specific service ID is based on the customer ID and included in the LLD.

In general, the following methods are recommended to keep service numbering globally unique:

- Use the service portal express or other NMS tool to create new services. In this case, NFM-P NSP assigns unique service IDs. The service name must include information to differentiate the different service types.
- Create rules for assigning service IDs (based on service categories) and manually assigning and tracking the values for individual services. This is common for networks using CLI to provision services. This supports the use of specific service-ID ranges for different service types and subtypes, which helps with troubleshooting and audits.

4.4.1.3 Service ID example

The following service ID example provides a sample numbering convention.

For a service ID: ABBCdddd:

- A – indicates service-type as follows:
  - 1 – VPRN
  - 2 – Cpipe
  - 3 – Epipe
  - 4 – IES
  - 5 – VPLS
- B – constant for different service types (for example, test, SCADA, relay, management, IT)

  Note: This can be set to a different ID per traffic type (as it was in this design).

- C – reserved to increment if needed to differentiate between different service sub-categories, for example:
  - to differentiate between electric versus gas, SCADA or transmission versus distribution, and so on
  - to differentiate different relay types such as LCD, MB, and so on
  - to identify services for partner utilities (with ID per partner), for example: if the customer's own SCADA uses BC=30, and relays use BC=40, the SCADA for partner X is 3X
- dddd – varies per service instance starting at 0001 and incrementing to 9999, using varying assignment rules for different customers based on circuit ID assignment, and so on

4.4.2 Service SAP overview

Each service type is configured with at least one service access point (SAP). A SAP identifies a customer interface point for a service. The SAP configuration itself includes the slot, MDA, and port information.

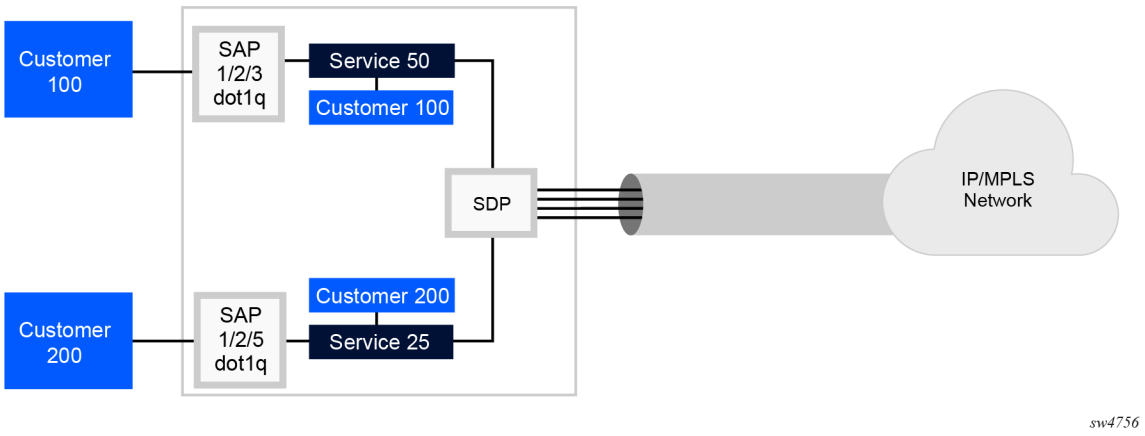
A SAP is a local entity and is uniquely identified by the following configuration aspects:

- physical port (Ethernet port or VLAN) or TDM (E1, E&M, SDI) port or channel
- encapsulation type
- encapsulation identifier (ID)
- depending on the encapsulation, a physical port or channel with one or more SAPs associated

Note: All the 7705 SAR ports are access ports by default (unless the mode is changed explicitly).

The following figure shows configuration of services for customers, including SAP configurations.

Figure 16 **Service configuration using SAPs**



Depending on the encapsulation, a physical port or channel can have more than one SAP associated. SAPs can only be created on ports or channels designated as “access” in the physical port configuration. SAPs cannot be created on ports designated as “network”.

Note: All ports on the 7705 are access ports by default unless a configuration is used to overwrite the default.

A service can be either a local service (it only contains SAPs on the local node), or it can be a distributed service, in which case it must be defined and associated with a SAP or SAPs and an SDP or SDPs.

SAP services include the following configurations:

- Point-to point services (VLLs X-PIPES) only contain two logical entities. A local VLL has two local SAPs, and a distributed VLL has one SAP and one spoke SDP or endpoint.
- VPLS, VPRN, and IES services can contain multiple SAPs on a given service site or node.
- SAPs within VPRN and IES services are provisioned within a Layer 3 interface configuration context.

4.5 CEM SAP configuration options (Cpipe services)

This section provides information about circuit emulation (CEM) SAP configuration options.

For TDM services, encapsulation is defined based on the channel group specified for the TDM port and encapsulation type. Several configuration parameters associated with TDM SAPs on Cpipes impact the delay and jitter seen by the traffic.

The correct values to use are determined by several factors such as latency and jitter tolerance, the packet delay variation (PDV) expected in the network, and the throughput rate of the service (number of timeslots or DS0s bound to the channel). As outlined previously, TPR circuits have very stringent latency and jitter requirements, and the related parameter settings are critical for transporting these circuit types. The following descriptions provide information about functions that are configurable using SAP configuration parameters:

- packet payload size

  This defines the payload size (in bytes) of a TDM pseudowire packet. The payload size directly impacts the packetization delay, however, decreasing the packet-size increases the overhead and total bandwidth used across the network.

  Note: Relay services carried by power utilities, (particularly LCD relays), have extremely strict requirements related to latency. For this reason, the payload size parameter must be set to very small values for these services.

- jitter buffer

  A CES uses a jitter buffer to ensure the circuit is tolerant of PDV introduced by the network. The range of values is from 1 to 250 ms in increments of 1 ms. Playout from this buffer starts when it is 50 percent full. Thus, the steady-state latency introduced is one half the buffer size, divided by the rate. This gives an operational PDV tolerance of one half the jitter-buffer size. The jitter-buffer size must be set to accommodate a minimum of three or more packets, which means the minimum value is related to the payload size.

The following table shows the nominal delay that would be introduced (one way) as a function of the configured payload size, along with the approximate MPLS throughput that is required to carry a

Cpipe service for a relay circuit for different scenarios: This includes Ethernet backhaul with and without NGE, as well as backhaul over PPP (ML-PPP or POS) interfaces.

Table Notes:

Sub-DS0 rate RS-232 ports (9600, 1200) are “pre-padded” to 64 kb/s by the MPLS nodes, and the table applies to relay circuits connected via 4-wire, RS-232, or TPR (single 64 kb/s) ports.

The latency shown does not account for hop-hop network queue delay or variable propagation delay across the transport.

The difference between L1 and L2 Ethernet bandwidth is the L1 line throughput includes 20-bytes of L1 line overhead (inter-frame gap and pre-amble), whereas the L2 excludes this (for the scenario of Ethernet MW which removes it).

Table 3 **Latency value versus payload for low speed (64 kb/s) service**

Payload (bytes)	Packet delay (ms)	jitter-buffer (ms)	Steady-state 1-way delay (ms)	Eth L2 rate (kb/s)	Eth L1 rate (kb/s)	Eth L2 with NGE	Eth L1 with NGE	PPP rate (kb/s)
4	0.5	3	2	1024	1344	2320	2640	352
6	0.75	3	2.25	683	896	1547	1760	256
8	1	4	3	512	672	1160	1320	208
12	1.5	6	4.5	341	448	773	880	160
16	2	8	6	256	336	580	660	136
64	8	24	20	90	110	171	190	82

4.5.1 SDP Tunnels

The SDP acts as a logical way to direct traffic from one PE to another PE through a unidirectional transport tunnel. The SDP terminates at the far-end node, which directs packets to the correct service egress SAPs on that device.

By default, when an SDP is provisioned to the far-end node, the T-LDP protocol is enabled so a T-LDP session is established when two PEs have SDPs. The session is used to advertise service-labels for each L2 service between the PEs.

For VPRN services, no explicit SDP configuration is required. VPRN services instead are provisioned with an "auto-bind" parameter enabled, which automatically binds any VPRN next-hops to an available MPLS LSP. Auto-bind can be set to use LDP, RSVP, or both. By default, all RSVP LSPs are eligible to be used, but this can be disabled on a per-LSP basis.

SDPs are unidirectional which means that for a service between node A and node B, an SDP is needed on both the terminating peer nodes. Each router must have an SDP defined for every remote PE node that is a termination point for L2 services from that node. Before a distributed service can be configured, SDPs must first be explicitly created.

An SDP has the following characteristics:

- The SDP specifies the system IP address of the far-end PE router.
- The SDP is not specific to a particular service or type of service. One or more services can be bound to the SDP after it is created.
- For L2 services to use network group encryption (NGE), requires that NGE be enabled (via NSP) on the SDPs that are used to carry the service.
- All services mapped to an SDP use the same transport encapsulation type defined for the SDP, which can be MPLS or GRE.
- The operational and administrative state of the SDP controls the state of service entities bound to it.

Note: Similar to MPLS or SR LSPs, SDPs are provisioned on an as-needed basis only.

There are four types of SDP tunnels. After creating an MPLS SDP the user can bind it to the following tunnel types through the configuration indicated:

- GRE – default type creates a GRE (non-MPLS IP based tunnel)
- LDP – bound by adding the **ldp** keyword under the SDP configuration
- Segment Routing – via SR-ISIS, SR-OSPF, or SR-TE
- LSP – specified by a preprovisioned RSVP or SR-LSP (by LSP name)
- BGP tunnel – maps to an RFC-3107 BGP tunnel (not planned for this design)

Note: SDPs by default are created in CLI with the GRE tunnel type, that is, they use GRE IP tunnel encapsulation. The MPLS keyword must explicitly be added to create MPLS-based SDPs.

4.6 TPR service design

4.6.1 Asymmetric delay control

Cpipe circuits used to carry TPR traffic have strict requirements for delay symmetry between the two sites. This is particularly true for LCD relays, which can generate alarms with as little as 1 to 4 ms of asymmetry (varies by model). This may occur because asymmetry causes phase errors in

the relay calculations, which could then cause the relay to mistakenly trip the transmission line it is controlling.

As mentioned in the MPLS design for TPR systems and General service design, relay circuits use strict paths to ensure that the two directions are carried over the identical transport paths. Additionally, the QoS design prioritizes relay traffic over all other traffic to ensure minimal queueing latency through the network. However, some packet jitter is expected within an IP/MPLS transport network, and for this reason jitter buffers are required on the circuits as described previously. The ADC feature was explicitly developed for the 7705 SAR family for use with LCD relays, to detect and compensate for asymmetric latency on the Cpipe.

4.6.1.1 Configuration overview

The following examples describe some of the reasons a service could have asymmetrical delay:

- A small amount of traffic discard (1 or 2 packets) occurring in the network or a path reroute event may introduce a positive or negative delay as the depth of the jitter buffer changes.
- Delay asymmetry may be caused by asymmetric packet delay variation in the network (although provisioning in the expedited forwarding class h1 should prevent this).
- If the nodes are not correctly synchronized the play out rates may vary, resulting in differences in the depth of the jitter buffer which then results in asymmetric delay.

A configurable option (**asym-delay-control**) is available for some Cpipes, to minimize the amount of asymmetric delay that may be caused by variations in the fill level of jitter buffers.

Note: This option does NOT compensate for asymmetric difference in external transmission delay.

At system startup or during a restart with the new option enabled, the router samples a configurable number of packets to calculate the average jitter-buffer latency. The idle-payload-fill pattern, or all 1’s (for 8-port TPR MDA), are played out during start-up analysis, and the service is considered down. If any packet loss is detected during analysis, the system restarts the analysis.

Depending on the difference between the average and expected latency of the buffer (based on the configured jitter-buffer size), the network processor either drops several octets or inserts some idle packets. During the periodic-sampling cycle, the service remains in the “up” state.

4.6.1.2 Configuration rules

A configurable analysis can periodically rerun on live traffic and perform adjustments only if the latency exceeds the user-configurable threshold. During the periodic sampling cycle, the service remains in the “up” state and the analysis is done on the live traffic (there is no insertion of idle patterns).

The following configuration rules apply for the Cpipe to become operational. The rules must be applied to ensure the service comes up.

- ADC must be provisioned on both ends of the Cpipes.
- The configuration of the jitter-buffer must match on both ends.
- The MDA and port type on the two SAP endpoints must match.
- ADC is only supported on CESoPSN Cpipes without CAS

The 7705 SAR-8 Shelf V2 and 7705 SAR-18 support ADC for the following MDAs:

- 8-port Voice & Teleprotection card (G.703 (codir) and C37.94 (TPIF) channels)
- 8-port C37.94 Teleprotection card (C37.94 (TPIF) channels)
- 12-port Serial Data Interface cards (RS-232, X.21, and V.35 on all 12-port Serial Data Interface card versions, and RS-530 on a12-SDI-V3 MDA)
- T1/E1 ports on both the 16 and 32 port T1/E1 ASAP Adapter cards
- T1/E1 ports on the 7705 SAR-A, 7705 SAR-M, 7705 SAR-X, and 7705 SAR-H
- 7705 SAR-Hc (RS-232 channels)

Note:

- ADC is not supported on Cpipes on 4-wire/E&M ports, and relays transported using these interfaces cannot use the feature. Tone relay systems generally do not have the same latency requirements as LCD relays.
- This feature was designed and tested with 87L relays, other relay types for example, mirrored bits, tone, and DTT do not require this feature.
- When enabling periodic checks of the latency, both the interval between retest and the number of packets to sample can be provisioned.

4.6.1.3 ADC on redundant paths

The following configuration is enforced when provisioning a Cpipe with ADC using redundant paths. The specific configuration is meant to prevent scenarios where the terminating nodes of the two Cpipes use different paths.

- Two separate SDPs are provisioned between the two PEs.
- Each SDP (on both PEs) is bound to a diverse strict-path RSVP LSP (symmetric on the two PEs).

- One PE controls the SDP selection for both ends, using T-LDP messages to signal which is the primary SDP.

4.6.2 Cpipe latency measurement

The 7705 SAR family includes configurable options for the user to enable the measurement of latency on a given Cpipe, by enabling the **network-latency-measurement** command for the Cpipe. When this is enabled, the 7705 SAR measures the minimum, maximum, and current latency. If AMP is enabled, the end-to-end latency is measured on all configured paths. See AMP for more information.

If network latency measurement is enabled, regular Cpipe packets are enhanced to include a proprietary 8-byte timestamp in every packet that the system sends over the service. These timestamps are based on the internal time clock of the router (PTP or GNSS based). At the far-end router, the Cpipe packets are timestamped on arrival based on the time clock of the router, which is again driven by PTP or GNSS. The end-to-end latency calculation is made by comparing the two timestamps over a window of 1024 packets.

Note: Because the measurements are taken one way, using the internal clocks on the two 7705 SARs to compare the timestamp and obtain accurate measurements, the nodes must all be locked to a PTP GMC.

The user can display the measured latencies for the Cpipe service using the following command.

```
tools dump service id network-latency-measurement
```

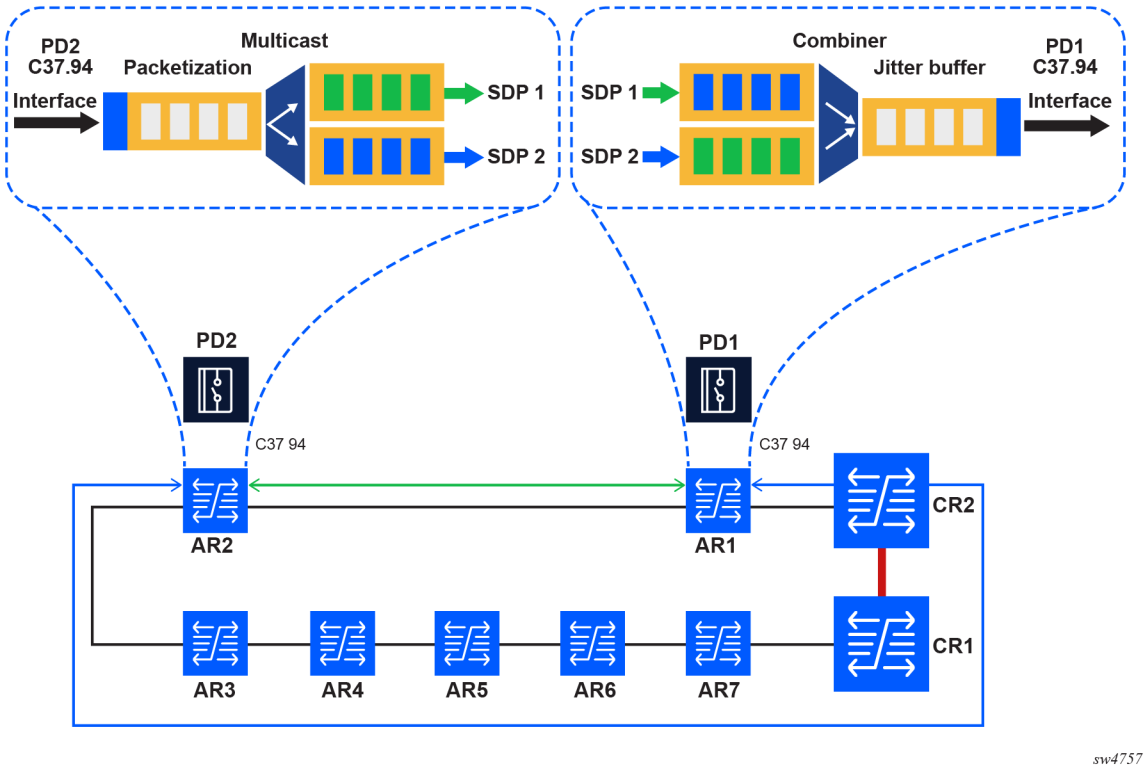
You cannot display the measured latencies using SNMP.

4.6.3 AMP

As described in Strict path LSP relays using standard Cpipe design, a single IP relay has separate A and B paths across the network with packets being sent across both paths. To provide a similar type of transport for single-attached TDM relays, the 7705 SARs supports the AMP service architecture. With this architecture, the network provides two active connections between the protection devices across completely diverse paths.

In the IP-relay case, the relay is dual-attached. The relay sends duplicate packets out both interfaces and is responsible for resequencing packets and dropping duplicate packets. In this case, the relay is single homed to one 7705 SAR node, which duplicates the packets across two paths. The 7705 SAR on the far end resequences the packets and drops duplicate packets, as shown in the following figure. This operation is transparent to the relays.

Figure 17 **AMP circuit diagram with combiner function**



4.6.3.1 AMP configuration overview

The preceding figure shows the following AMP configuration information:

1. The single C37.94 interface is bound to the Cpipe as a SAP with CEM parameters set as described in CEM SAP configuration options (Cpipe services). There are two additional considerations for AMP as follows:
   - Without AMP, the jitter-buffer must be set to only compensate for network jitter. With AMP, the jitter-buffer size must be increased to accommodate the difference in latency between the two network paths. Thus, a measurement or estimate of latency on both paths is required to size the jitter buffer. This can be obtained using the 7705 SARs during turnup, assuming both are locked to a PTP GMC (see Cpipe latency measurement).
   - The active-multipath timeout option controls how long a node waits for additional paths to become available, from the time the first path becomes available. The range is 1 to 60 s, with a default of 10 s.
2. The two paths are bound to the Cpipe by provisioning an endpoint within the Cpipe that is provisioned with the active-multipath parameter.

3. Within the Cpipe, two spoke-SDPs are bound to the provisioned AMP endpoint (step 2). These use two different SDPs to the same destination 7705 SAR bound to different strict-path LSPs.

4.6.3.2 AMP with ADC

AMP and ADC can be provisioned independently from each other. For example, an ADC-enabled Cpipe can be used with or without AMP and vice-versa.

If ADC is enabled for the Cpipe service, only one common path is selected for ADC analysis and jitter-buffer adjustment. If more than one common path is available, the path with the lowest virtual circuit identifier (VCI) is selected for initial ADC analysis and jitter buffer adjustment.

ADC analysis and adjustment are based on the traffic egressing the combiner. After the ADC process is completed, there may be a shift in the jitter-buffer fill level corresponding to the other available paths with different latencies.

4.6.4 Relay Cpipe overview

Relay circuits provide critical monitoring services between adjacent sites on transmission lines. Government regulations are in place requiring full redundancy and path diversity for any relays for transmission lines greater than 250 kV.

Cpipe services transport services for different types of relays (for example, mirrored bits, LCD, DTT, or POTT) carried over different types of ports (for example, C37.94, RS-232, 4-wire). These relays have different requirements related to latency, however for consistency they are all provisioned using the same service template (if feasible).

4.6.5 Service specifications

The following service specifications are used for the TPR service design:

- The jitter buffer (3 ms) and payload size (6 bytes) are off set on all relay Cpipes to meet the strictest latency requirements provided (from SEL recommendations).
- A common SAP-ingress policy is provisioned with default forwarding class (FC=h1), and no SAP-egress policy is used.
- Strict path LSPs are utilized with no FRR enabled.
- ADC is enabled on the LCD Cpipes using RS-232 or C37.94 ports.

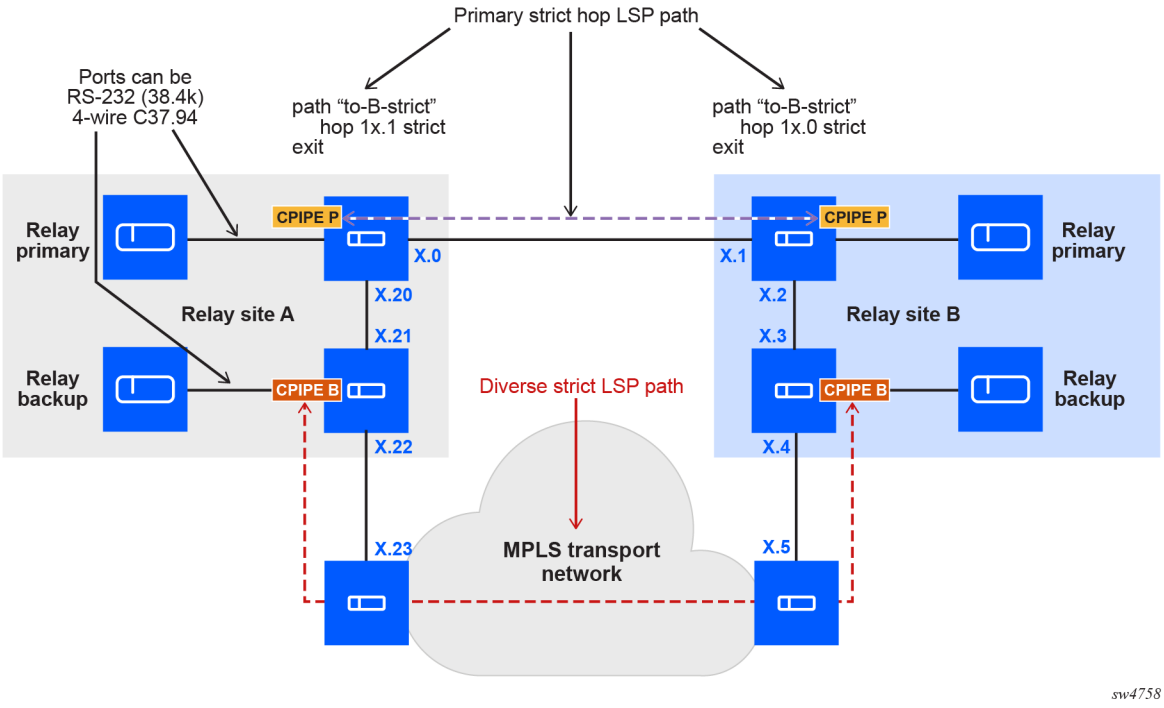
  Note: 4-wire relays on E& M do NOT support ADC. The feature was designed and tested specifically for LCD relays, not mirrored bits or tone relays.

- All C37.94 interfaces are single 64 kb/s timeslot.

- To meet the redundancy requirements for A and B relay pairs, Cpipes are provisioned on different 7705 SARs, and the primary strict-hop path on the two LSPs must be on diverse paths.

The following figure shows the Cpipe layout for dual A and B relays.

Figure 18 **Diverse primary or backup Cpipes for high-V sites with A/B relays**



4.6.5.1 Standard relay Cpipe template

This section provides an outline for the configuration under the **/configure service** context used for relay circuits not being transported with AMP. See MPLS design for TPR systems for more information about the MPLS LSP configuration related to the following configuration templates.

Example: Relay circuit without AMP configuration

```
/configure service
     customer 4 create
       description "CPIPE Services For Relay/Teleprotection Circuits"
     exit
     sdp <ID> mpls create
            description "to-<farend Node>:Relay Via <path 1st Hop Node>"
            far-end <Farend SYS-IP>
            lsp < LSP naming>
            no shutdown
     exit
     cpipe <SVC-ID > customer 4 vc-type cesopsn create
         service-name "Relay-<type>:<site codes>:<Dest-Site>-<CID>-<primary|Backup>"
```

```
          network-latency-measurement
         sap <port-ID>.1 create
              cem
                 packet jitter-buffer 3 payload-size 6
                 asym-delay-control samples 16 min-repeat 720 threshold-repeat 1000
#LCD Relays ONLY
              exit
              ingress
                   qos <ID>
              exit
          exit
          spoke-sdp <SDP-ID>:<SVC-ID> create
                no shutdown
          exit
          no shutdown
    exit
```

4.6.6 Using Cpipe services with AMP

The AMP feature can be used to provide two active circuit paths within a given Cpipe, with packets duplicated over both paths. This means that a link or node failure over one path does not cause packet loss on the circuit.

One potential benefit of this is for relay circuits, where a relay with a single interface can be transported over a single Cpipe using AMP. Utilities can use this option instead of having the protection team add a second relay interface, which requires an additional port and circuit on the transport network.

Using AMP has the following considerations. Beyond these, the same CEM payload size and QoS policy are used.

- Jitter buffer

  With AMP, the jitter-buffer size must be increased to accommodate the latency difference between the two paths.

  Note: Increasing the jitter-buffer size also increases the steady-state latency by one half the jitter-buffer size and the potential peak latency by the jitter-buffer size. Because relays have strict requirements for latency and jitter the implications related to AMP use with relays are described in the following points.

- End-end latency

  Given a goal of one-way delay maximum of 10 ms with the assumption of 3 ms allocated for transmission and transport and packetization, this leaves a 7 ms margin. Therefore, setting the jitter-buffer size to 7ms can exceed the 1-way delay requirements for some relay types.

- Asymmetry

  With increases in jitter-buffer size there can potentially be increases in asymmetry, introduced by network events that lead to shifts in the jitter-buffer levels on one node.

  Note: Nokia does not recommend using any circuits where the latency delta between the two paths exceeds 4 ms. This would lead to a total jitter buffer of 7ms, using the base jitter-buffer size 3ms.

  When AMP is used with circuits with delta latency greater than 2ms, Nokia recommends ADC is enabled to allow for auto-adjustment of the jitter-buffer size.

- LSP configuration

  The Cpipe still has two strict RSVP paths provisioned, but instead of using a secondary path on a single LSP, there are two LSPs each with a primary path and no FRR.

- ADC

  ADC is enabled on all AMP relay circuits where supported (see the following note). But with AMP the repeat interval must be set to 0 (only runs on startup).

  ADC is enabled on the LCD Cpipes using RS-232 or C37.94 ports.

  Note: 4-wire relays on E&M do not support ADC and the feature was designed and tested specifically for LCD relays not mirrored bits or tone relays.

4.6.7 Path and LSP templates for AMP

This section provides MPLS LSP configuration templates for the router and service configuration.

4.6.7.1 MPLS LSP template

The following example provides an MPLS LSP template configuration. See earlier topics of this document for configuration templates related to port and MPLS LSP configuration.

Example: MPLS LSP template

```
/configure router mpls
        path "To-<Dest.Site Name>:Via-<NH site>"  #example: "To-Grimes:Via-direct"
           hop 1 <NH-IP1> strict
           hop N <NH-IPN> strict
           no shutdown
        exit
        path "To-<Dest.Site Name>:Via-<NH site2>"    #example: "To-Grimes:Via-Norwalk"
           hop 1 <NH-link-IP1> strict
           hop N <NH-link-IPN> strict
           no shutdown
```

```
        exit
         lsp <see 10.11.5.4>  #Example: lsp RAU-To-ACE-SAR8-1/S-1
                to <far-end System IP>
                cspf #removed for inter-area
                retry-timer 5
                vprn-auto-bind exclude #Prevents use for corporate/control VPRN
                primary "To-<Dest.Site Name>:Via-<NH site>"
                exit
                no shutdown
         exit

         lsp <lsp>  #Example: lsp "RAU-To-ACE-SAR8-1/S-2
                to <far-end System IP>
                cspf #removed for inter-area
                retry-timer 5
                vprn-auto-bind exclude #Prevents use for corporate/control VPRN
                primary "To-<Dest.Site Name>:Via-<NH site2>"
                exit
                no shutdown
         exit
```

4.6.7.2 SDP and service templates for AMP

The following template provides a framework for SDP and services configuration for AMP.

Example: SDP and services template for AMP

```
/configure service
     customer 4 create
       description "CPIPE Services For Relay/Teleprotection Circuits"
     exit
     sdp <SDP-ID> mpls create
            description "to-<farend Node>:Relay Via <path 1st Hop Node>"
            far-end <Farend SYS-IP>
            lsp  RAU-To-ACE-SAR8-1/S-1
            no shutdown
     exit
     sdp <SDP-ID2> mpls create
            description "to-<farend Node>:Relay Via <path 1st Hop Node>"
            far-end <Farend SYS-IP>
            lsp  RAU-To-ACE-SAR8-1/S-2
            no shutdown
     exit
     cpipe <SVC-ID> customer 4 vc-type cesopsn create
         service-name "Relay-AMP:<site codes>:<Dest-Site>-<CID>-<primary|Backup>"

          network-latency-measurement
          endpoint "AMP" create
                active/multipath
          exit
          sap <port-ID>.1 create                        #example: sap 1/3/1.1 create
              cem
                 packet jitter-buffer 6 payload-size 6
                 asym-delay-control min-repeat 0
              exit
              ingress
                   qos <ID>
              exit
          exit
          spoke-sdp <SDP-ID>:<SVC-ID> endpoint "AMP" create
                no shutdown
```

```
        exit
        spoke-sdp <SDP-ID2>:<SVC-ID+1> endpoint "AMP" create
              no shutdown
        exit
        no shutdown
exit
```

4.6.8 Using NSP to deploy AMP TPR services

This section describes the requirements and procedures for using the Nokia Network Services Platform (NSP) to create AMP TPR services using Cpipes. NSP can be used to automate all facets of the network management, including deployment and configuration, security, fault handling, statistics collection, backup, and so on.

Note: This NVD has been tested with NSP Release 24.11.

4.6.8.1 C-Line service requirements

A C-Line service connects two Nokia SR OS SAPs for the AMP TPR service using Cpipes.

The following components are required when using a C-Line service:

- standard Nokia SR OS C-Line service fulfillment (SF) adaptor
- custom service templates, workflows, and intents

The following notes apply to VLAN tagging:

- asterix (*) QinQ

  If the ports are configured for QinQ, the inner tag is an asterix (*), which means that any VLAN tag is accepted. To achieve this in SF, the inner tag must be set to “4095”. This is because the SF has no concept of an asterix (*).

- VLAN TAG (-1) dot1q

  If the network consists of dot1q ports only, the inner VLAN TAG must be set to -1.

  This may become repetitive, so it is possible to modify the intent such that -1 is a default, read-only option.

4.6.8.2 Prerequisites for creating the Cpipe

The following table describes the checks to do prior to creating the Cpipe.

Table 4 **Cpipe relay test cases prior to creating the Cpipe**

Configuration element	Description
Cpipe relay	Verify the Cpipe template can be setup with relay-specific hard-coded SAP CEM parameters (CEM payload set to 6 bytes, and jitter buffer set to 3 ms).
Cpipe relay	Verify the SDPs with NGE described in the previous Cpipe verification can be associated with the specified Cpipe.
Cpipe relay	Verify that ADC can be added to existing P2P Cpipes or templates and applied to nodes.
Cpipe voice specification	Verify if there is a method to provision a Cpipe with Circuit Emulation Services over Packet Switched Network with Channel Associated Signaling (CESoPSN-CAS) between T1 DS0s on the two SAR routers (node-node).
Cpipe voice specification	Verify if there is a method to provision a Cpipe with CESoPSN-CAS between E1 DS0s on the two SAR routers (node-node).
VPRN NGE	Verify if there is a method to associate the NGE with an intent-based service fulfilment (IBSF) created VPRN.

4.6.8.3 Configure and deploy the Cpipe TPR with AMP

Use the following steps to configure and deploy a Cpipe TPR with AMP using NSP:

1. In the **Service Management** menu, click **Create Active Active/Multipath**.
2. Enter the service parameters shown in the following table.
3. When complete, click **Save** and then **Deploy** to send the configuration to the NEs.

Table Notes

- The * indicates mandatory.
- The values shown in the table are samples only. Replace these with values appropriate to your scenario.
- Set the default AMP timeout value under CEM in ICM SAP to 100 although the valid range is 1-60, default 10.

  Entering a valid value (for example, 20) causes the Cpipe configuration to fail.

  The following example shows the related CLI configuration. The parameter "*range 1-60, default 10*" in the NSP GUI is set to 100.

```
/configure service cpipe <svc-id>
    sap x/x/x.1 cem
        active-multipath-timeout <range 1-60, default 10>
```

Table 5 **Cpipe TPR with AMP parameters**

Parameter		Value	Description
Template name		Redundant Cpipe	
Service name *		C37942_AMP	Provide service name
NE service ID *		37942	Provide NE service ID
Customer ID *		1	Select from the list of customer ID
VC type *		CESoPSN	Select from the list VC-type
Admin state		unlocked	
Site details			
Site 1			
Device ID *		10.10.8.145	Select from the list of NE
Site name			Not mandatory
Description			
Mtu			Leave default
Service endpoint details	Endpoint *	C37492_SAR145	Provide endpoint
	Active multipath	☑	Check to enable AMP
SAP details			
Port ID		Channel 1/5/5.tpif-1	Select from the list of port IDs
Time slots *		1	Provide timeslot from 1 to 32
Admin state		unlocked	
Description			
CEM	Payload size	6	Provide the payload size
	Jitter buffer	4	Define the jitter buffer
	Active multipath timeout	100 (see table notes)	Provide the AMP timeout
Asymmetric delay control (ADC)			
Enable		☑	Check to enable ADC
	Sample	Thirty-two	Provide sample value

Parameter		Value	Description
	Repeat period	0	Provide repeat period value
	Threshold-repeat	0	Provide threshold repeat value
Enable QoS		☑	Check to enable QOS parameter settings
QOS parameters			
Ingress			
SAP ingress	Policy name	Relay	Provide policy name
SDP details			
Spoke SDP			
SDP1			
Equipment details	Destination device ID	10.10.8.143	Select from the list of device IDs
	Steering		
	Spoke SDP ID *	5123	Select from the list of SDP IDs
	VC ID *	379422	Select from the list of VC IDs
	Admin state	unlocked	
Endpoint details	Endpoint	C37492_SAR145	Select from the list of endpoints
SDP2			
Equipment details	Destination device ID	10.10.8.143	Select from the list of device IDs
	Steering		
	Spoke SDP ID *	523	Select from the list of SDP IDs
	VC ID *	379421	Select from the list of VC IDs
	Admin state	unlocked	
Endpoint details	Endpoint	C37492_SAR145	Select from the list of endpoints

Parameter		Value	Description
Site 2			
Device ID *		10.10.8.143	Select from the list of NEs
Site name			Not mandatory
Description			
Mtu			Leave default
Service endpoint details	Endpoint *	C37492_SAR143	Provide endpoint
	Active multipath	☑	Check to enable AMP
SAP details			
Port ID		Channel 1/5/5.tpif-1	Select from the list of port IDs
Time slots *		1	Select the timeslot from 1 to 32
Admin state		unlocked	
Description			
CEM	Payload size	6	Provide payload size
	Jitter buffer	4	Provide jitter buffer
	Active multipath timeout	100 (see table notes)	Provide AMP timeout value
Asymmetric delay control (ADC)			
Enable		☑	Check to Enable ADC
	Sample	Thirty-two	Provide sample value
	Repeat period	0	Provide repeat period value
	Threshold-repeat	0	Provide threshold-repeat value
Enable QoS		☑	Check to enable QOS settings
QOS parameters			
Ingress			
SAP ingress	Queuing type	Shared	Set queuing type
	Policy name	Relay	Provide the policy name
SDP details			

Parameter		Value	Description
Spoke SDP			
SDP1			
Equipment details	Destination device ID *	10.10.8.145	Select from the list of device IDs
	Steering		
	Spoke SDP ID *	3125	Select from the list of SDP IDs
	VC ID *	379422	Select from the list of VC IDs
	Admin state	unlocked	
Endpoint details	Endpoint	C37492_SAR143	Select from the list of endpoints
SDP2			
Equipment details	Destination device ID	10.10.8.145	Select from the list of Device IDs
	Steering		
	Spoke SDP ID *	325	Select from the list of SDP IDs
	VC ID *	3794221	Select from the list of VC IDs
	Admin state	unlocked	
Endpoint details	Endpoint	C37492_SAR143	Select from the list of endpoints

5 Test cases summary active/active multipath

5.1 Synopsis

The 7705 SAR family added a new feature for the transport of relay circuits that enables the 7705 SAR to transport TDM packets across two separate network paths. The 7705 SAR on the far-end resequences the packets and drops duplicate packets. This operation is transparent to the relays, however it requires that the 7705 SAR jitter-buffer size be increased to account for the delta latency on the two paths.

5.2 Test case objective

The AMP feature has been used in lab tests and field trials but has not been widely deployed. As noted, the difference in latency between the active paths can impact the Cpipe configuration (jitter-buffer size) and operation.

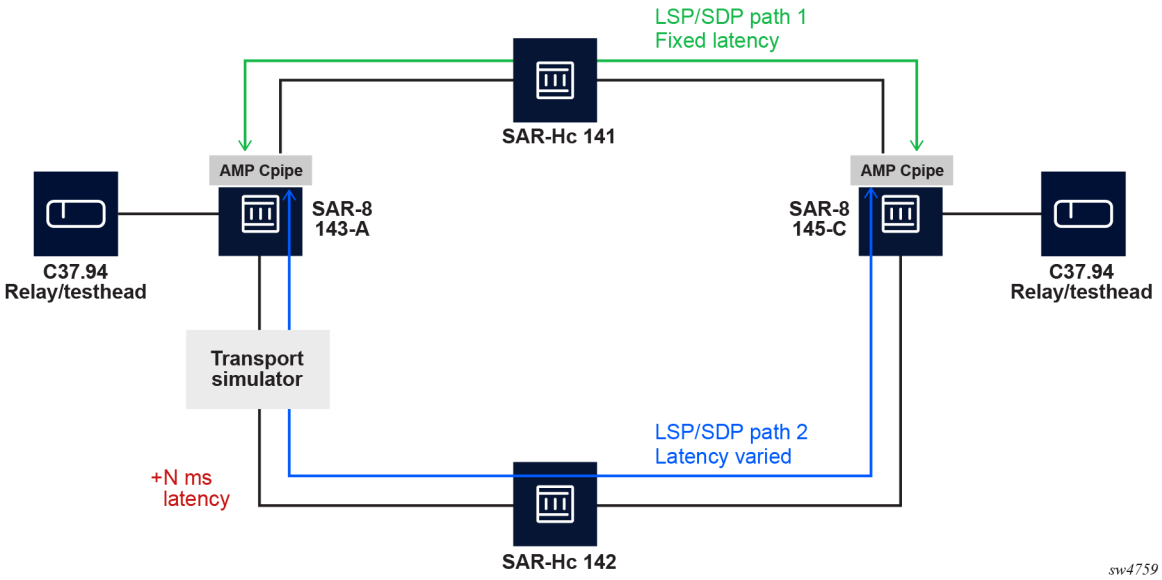
The following test steps quantify the impact:

1. Verify the impact on circuit performance for cases where the jitter-buffer size does not account for the delta latency (jitter buffer =3 ms with delta latency of 5 ms), for both steady-state and rainy day (failover) scenarios.
2. Verify the impact on latency when the jitter-buffer size is increased to accommodate the 5 ms delta.
3. Record the impact on the relay circuits for link and node failover scenarios on the two paths with the 5 ms latency delta.
4. Verify the steady-state, long-term stability of the relay circuits with the described parameters.

5.2.1 Test procedure

The following figure shows the layout of the test AMP Cpipe. For this test case, LCD relays or a test device with C37.94 ports are connected, and the statistics from the devices are monitored throughout the execution of the test cases.

Figure 19 **AMP circuit layout**



5.2.1.1 Baseline circuit-stability and failover stress test

For this test, the AMP circuit for the Cpipe is provisioned with the standard recommended values (6 byte payload and 3 ms jitter buffer).

The following steps are required for the test:

1. View the statistics on the relay or the C37.94 test head, and take a baseline measurement of latency asymmetry and stability to verify there are no packet losses, errors, and so on.

   Note: Given the simple lab architecture, it is expected that the latency on both paths is equal and symmetric in both directions.

2. Record the latency displayed by the 7705 SAR-8 nodes using the following command and check **trap log-99** on both 7705 SAR-8s to verify the Cpipe stability.

   ```
   /tools dump service <id> network-latency-measurement
   ```

3. Perform the stress test and failover impact to verify the circuit stability and impact of network events on the external relay circuits with symmetric latency:

   a. Interrupt the traffic flow on path 1 by shutting down and restoring the link between the 7705 SAR-8s and 7705 SAR-Hc-141, then repeat steps 1 and 2 to verify impact and circuit stability.

   b. Interrupt the traffic flow on the primary path by rebooting the 7705 SAR-Hc-141, and then repeat steps 1 and 2 to verify the impact and circuit stability.

   c. Interrupt the traffic flow on path 2 by shutting down and restoring the link between the 7705 SAR-8s and 7705 SAR-Hc-142, then repeat steps 1 and 2 to verify the impact and circuit stability.

5.2.1.2 Impact of delta latency on Cpipe relay

The following steps test the impact of the delta latency on the Cpipe relay:

1. Provision the transport simulator to insert 5 ms of fixed latency onto the second active path (in both directions).

2. Repeat steps 1 and 2 in the previous test, Baseline circuit-stability and failover stress test, and compare results to the baseline results.

   Note: It is expected that the increased latency is reflected in the measurements.

   If the relay or test head and Cpipe are not stable, stop the test and debug the relay and test head.

3. Perform stress testing by repeating the substeps of step 3 in the previous test, Baseline circuit-stability and failover stress test, to verify the circuit stability during failovers when operating on two paths with a difference in delay on the paths.

4. Increase the injected latency from 5 ms to 10 ms, and repeat steps 2 and 3 in the previous test, Baseline circuit-stability and failover stress test.
5. Reprovision the Cpipe SAP CEM parameters to increase the jitter-buffer size to 8 ms (to account for the 5 ms of delta latency and repeat steps 2 and 3 in the previous test, Baseline circuit-stability and failover stress test.

5.2.1.3 Stability monitoring

The following steps test stability monitoring:

1. Reset SAP and service counters on the Cpipe and counters on the relay or test head, and leave the circuit operational overnight.
2. Record the SAP statistics and relay or test-head statistics to determine if there was any instability.

Customer Document and Product Support

Customer Documentation

Customer Documentation Welcome Page

Technical Support

Product Support Portal

Documentation Feedback

Customer Documentation Feedback