MPLS for mission-critical microwave networks

Building a multi-fault tolerant microwave network

Strategic White Paper

High resiliency and service availability are key design considerations when deploying mission-critical microwave networks. It is imperative that network connectivity can still be provided in the case of a multi-failure scenario. The traditional architecture of ring-and-spoke topology can provide strong protection against failure in the aggregating ring sites but leaves the spokes in access sites vulnerable to upstream failure because there is no path diversity protection. This white paper discusses how deploying a multi-ring topology in backhaul networks can provide the protection required and explains why only Layer 3 microwave technology can be used to leverage the full path diversity to restore connectivity in even a multi-failure scenario.

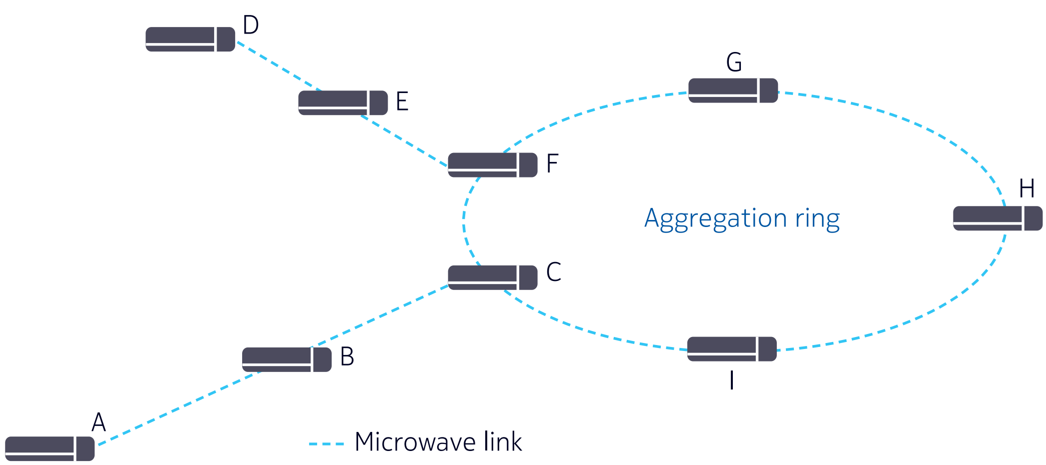
Contents

Introduction
Introduction

Deployment of microwave links in mission-critical networks will continue, particularly in scenarios where wireline alternatives such as fiber link are not feasible or would be too costly to deploy. In some cases, microwave is also an attractive technology to provide a backup path for a fiber link, particularly in the network core.

As shown in Figure 1, a typical microwave network topology is based on an aggregation ring with spokes to the most distant sites.

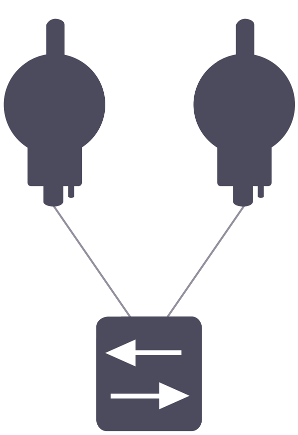
Figure 1. A typical ring-and-spoke microwave topology



As shown in Figure 2, a typical microwave platform typically consists of

- An indoor unit (IDU), which also functions as an Ethernet switch supporting advanced Ethernet features, including ITU-T G.8032[1] Ethernet ring protection switching and different variants of Spanning Tree Protocol (STP)
- One or more microwave radios

Figure 2. A typical Layer 2 microwave platform



1 ITU-T G.8032, Ethernet Ring Protection Switching, February 2012 and Amendment July 2013. http://www.itu.int/rec/T-REC-G.8032/en

Shortcomings of ring-and-spoke topology

In a typical ring-and-spoke architecture, aggregation ring nodes have high resiliency because a SONET/SDH-like ring protection mechanism has been standardized and is available in carrier-grade data communications through Layer 3 IP/MPLS fast reroute (FRR) Label Switched Path (LSP) protection [2] or Layer 2 Ethernet ITU-T G.8032 Ethernet ring protection.

However, the spoke sites in Figure 1 (A, B, D and E) are vulnerable to upstream spoke site failures. For example, service availability at Node A is subject to path access to Node B and Node C. If any failure occurs along Path A-B-C, service at Node A would be down due to lack of path diversity in such a ring-and-spoke topology. The worst case is when Node C fails: service at Node A and Node B also fail.

Similarly, any failure along Path D-E-F results in service at Node D being down. If Node F fails, service at Node D and E also fail.

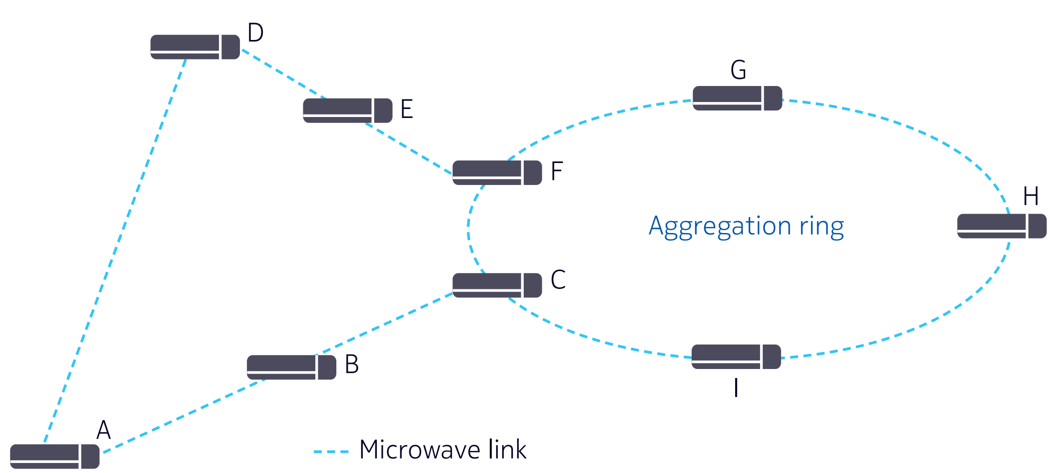
For commercial carriers, non-self-recoverable failures might be acceptable at the remote spoke sites because service impact at far-flung sites might be minimal. However, in mission-critical segments such as public safety or utilities, it is often equally important, and also mandated by government regulations, to extend a similar level of network protection to all spoke sites.

How can service availability be improved for spoke sites?

Migrating from ring-and-spoke to multi-ring topology

Service availability for spoke sites can be improved by using a multi-ring topology, in which subtending spoke end nodes (Node A and Node D in Figure 3) are connected to form an access ring joining with the aggregation ring.

Figure 3. A multi-ring topology



Deploying a multi-ring topology provides multi-path diversity and improves the availability for all spoke sites. For example, Node A and Node B now have alternate paths to the aggregation ring through D-E-F. If Link B-C or Node C fails, Node A and Node B still have a path to reach the aggregation ring through A-D-E-F. This level of protection is vital to ensure that critical operations continue to serve the general public.

Multi-ring deployment with a Layer 2 microwave platform

There are two major Layer 2 options to implement a multi-ring network:

- Spanning Tree Protocol according to IEEE Recommendation 802.ID
- Ethernet Ring Protection Switching (ERPS) according to ITU-T Recommendation G.8032

Option 1: STP

STP was originally standardized in IEEE 802.1D as a loop prevention and network recovery mechanism [1]. Because it was designed mainly for enterprise applications, recovery speed was not optimized and could range from seconds to tens of seconds, depending on network size and topology.

To improve recovery performance, new variants such as Rapid Spanning Tree Protocol (RSTP)[2] were standardized that improve performance to the order of seconds depending on network topology. However, RSTP still falls short of traditional SONET/SDH-based network recovery speed, which is the benchmark for mission-critical network technology considerations and is still network size- and topology-dependent. Furthermore, during the recovery period there is extensive traffic flooding as all nodes in the backup path are learning MAC addresses. Therefore, STP and RSTP are not attractive technical options.

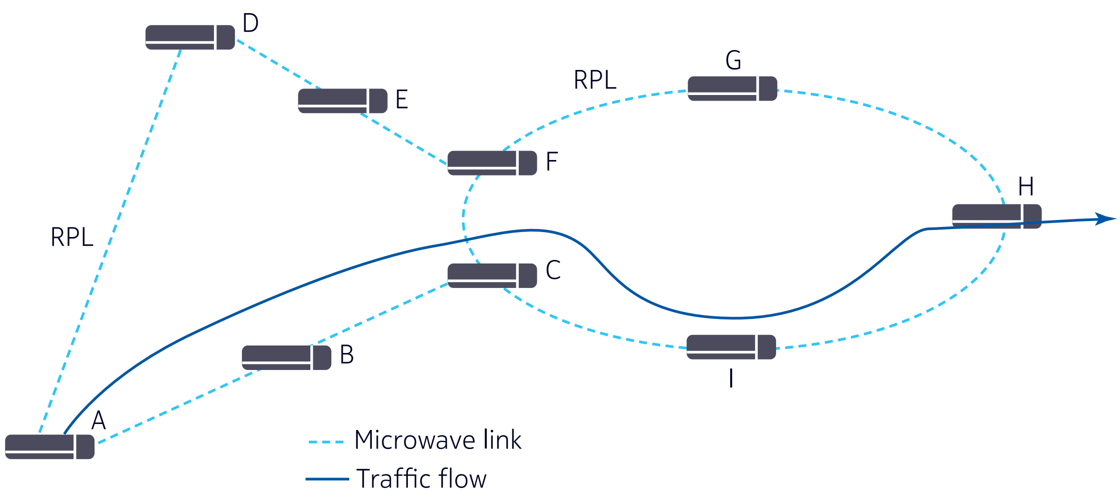
Option 2: ERPS

In an effort to make Ethernet networks as resilient as SONET/SDH-networks, particularly in a ring topology, the ITU-T developed ERPS Recommendation G.8032 to allow an Ethernet ring to recover in 50 ms. ERPS was initially developed for a single ring topology. Later, it was expanded to accommodate multi-ring topology.

In general, ERPS works well at providing protection from a single failure in a ring. To provide ring protection without incurring a loop, ERPS requires operators to designate one link in the ring as a resiliency protection link (RPL) that blocks traffic from looping. As shown in Figure 4, Link A-D and Link F-G are designated as RPLs. Traffic from Node A to Node H will go through Path A-B-C-I-H.

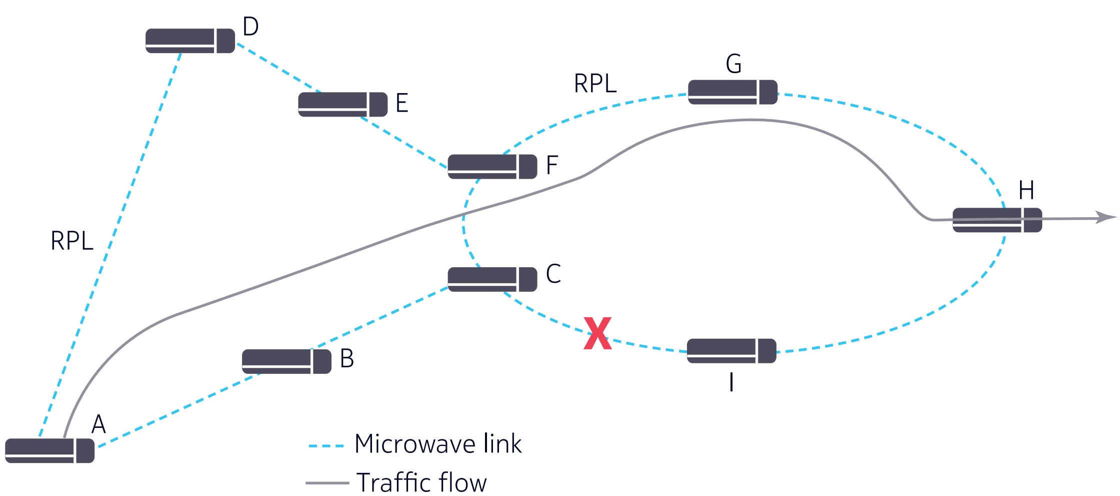
2 RSTP was first standardized in 802.1w and later incorporated into a newer edition of 802.1D. http://www.ieee802.org/1/pages/802.1D-2003.html

Figure 4. Multi-ring deployment with normal traffic flow scenario



If Link C-I fails, the aggregation ring will activate the RPL and the traffic will now follow Path A-B-C-F-G-H (see Figure 5), which becomes the active path.

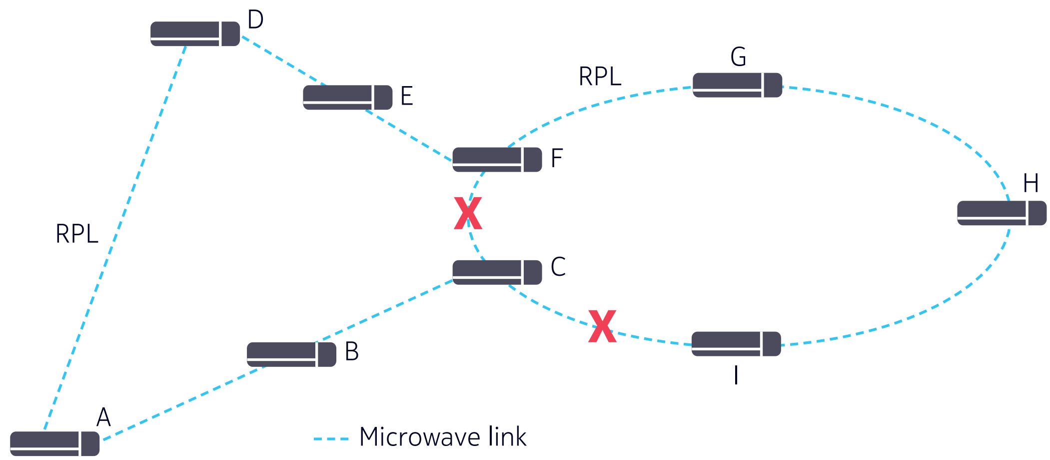
Figure 5. Single-fault scenario: traffic flows restored along the newly active path



However, if another failure occurs, for example, at Link C-F (see Figure 6), the connectivity between Node A and Node H will no longer be able to be restored even though the physical path A-D-E-F-G-H exists. Instead, the network will be segmented: a part of the network (Node A, B and C) is isolated. This phenomenon of segmentation is caused by the lack of a method to propagate the switching trigger in the aggregation ring to the access ring.[3]

3 Please refer to ITU-T G.8032, Ethernet Ring Protection Switching, Appendix X (February 2012) for a fuller discussion of segmentation.

Figure 6. Double faults scenario: no communication despite available communication path



Therefore, when high availability covering a multi-failure scenario is required, a Layer 2 Ethernet-based microwave platform is not a viable solution because it cannot make use of available path diversity to protect traffic in multi-fault scenarios.

Multi-ring deployment with a Layer 3 microwave platform

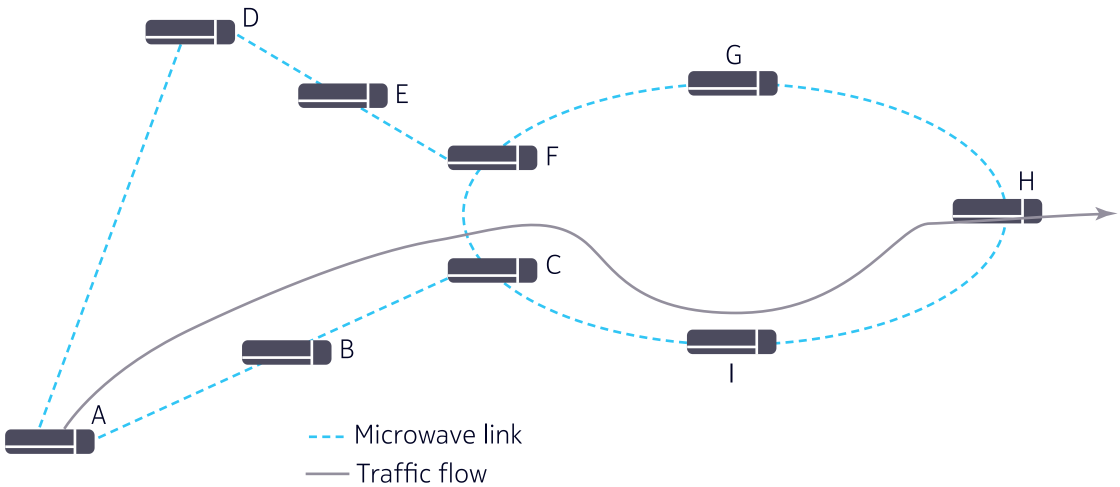
A Layer 3 microwave platform has:

- An IDU that is a full-fledged IP/MPLS router
- One or more microwave radios
- Versatile support of optical fiber interface for Gigabit Ethernet (GE) and 10 GE
- Scalable support of IP VPN, IP multicast and IPv6 services
- Other value-added IP capabilities, including stateful firewall and encryption of IP and MPLS traffic

Layer 3 IP/MPLS protection excels in a wide range of topologies, including single-ring, multi-ring and mesh topologies. Unlike other network technologies, such as G.8032 ERPS, an IP/MPLS network can survive a multi-failure scenario as long as physical path reachability exists. This unmatched capability is due to the inherent MPLS intelligence provided by the full routing information of the network.

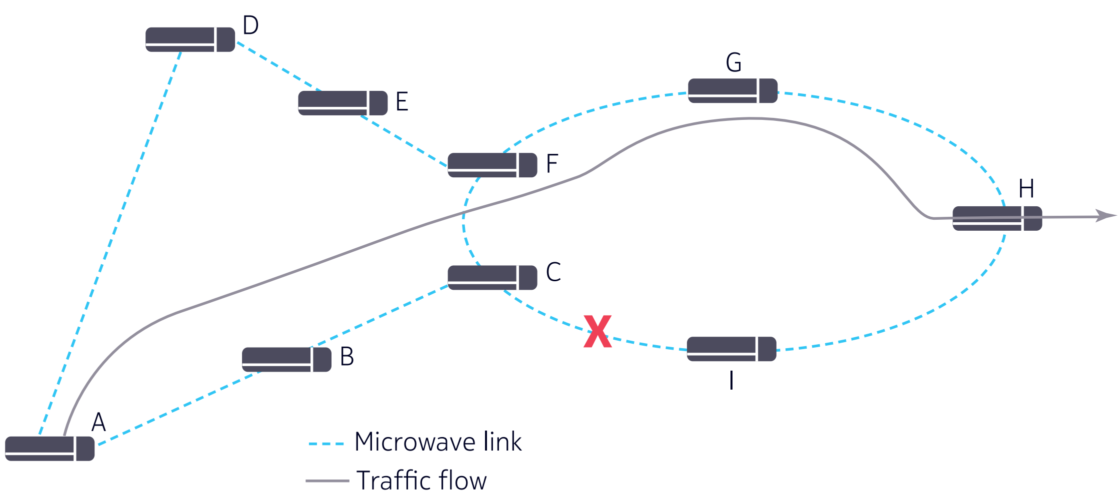
This multi-fault tolerant recovery by IP/MPLS is illustrated by using the same reference network shown in Figure 6. During a normal scenario, the primary LSP follows Path A-B-C-I-H (see Figure 7).

Figure 7. Traffic flows along the primary LSP



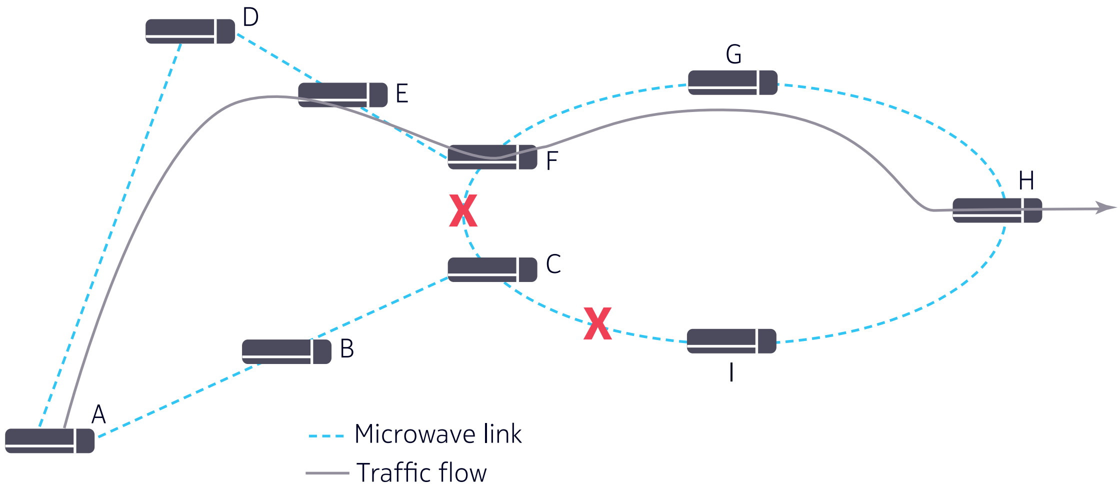
If a fault occurs at Path C-I (see Figure 8), the MPLS router C shunts all traffic to a pre-established FRR tunnel C-F-G-H within 50 ms of detecting the fault to keep user applications from being interrupted. Node A re-establishes the LSP through Path A-B-C-F-G-H.

Figure 8. MPLS recovers by re-establishing the LSP around the single fault



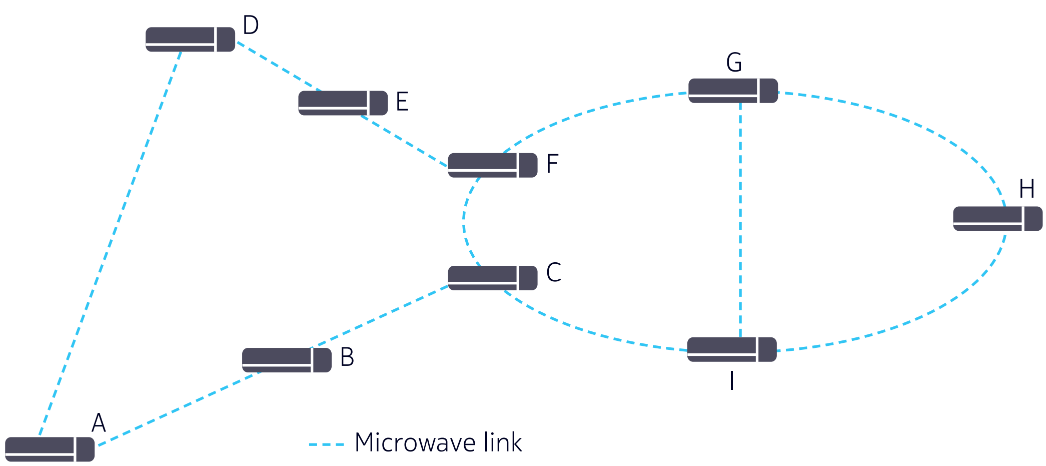
If a second fault occurs along Path C-F (see Figure 9), another secondary path (A-D-E-F-G-H) is still available.

Figure 9. MPLS recovers traffic in a double-fault situation



In the future, if the network operator requires even higher network resiliency, it can add a link between Node G and Node I and expand the aggregation ring to a partial mesh, as shown in Figure 10. Because MPLS path protection depends on routing information, it can leverage this extra connectivity without any operator intervention. For example, if a third failure occurs at Link G-H, the LSP can now take Path A-D-E-F-G-I-H.

Figure 10. Expanding a multi-ring topology to a partially-meshed topology



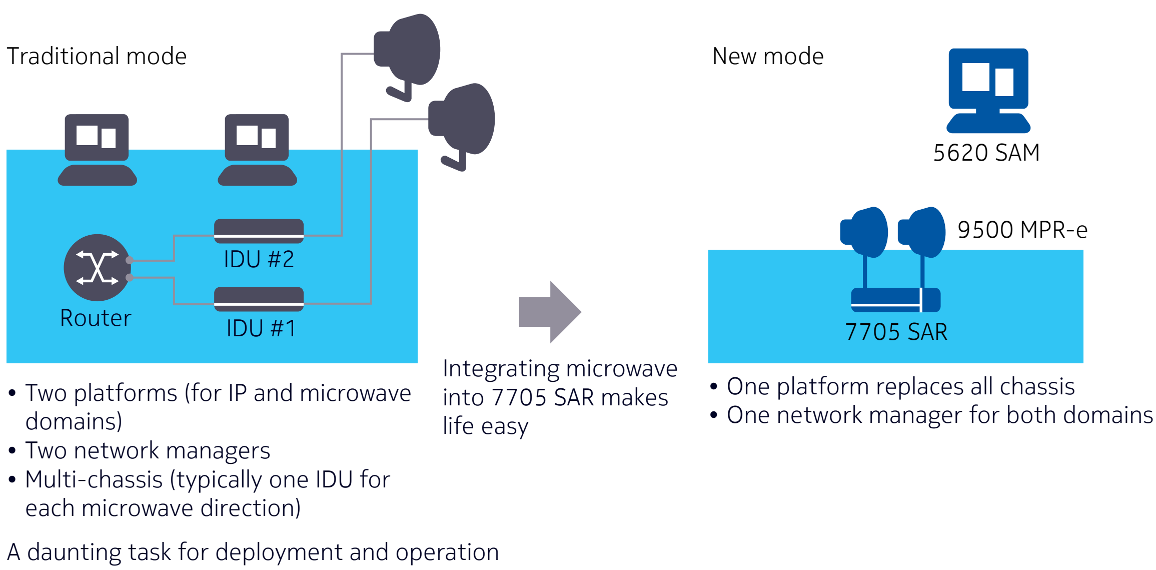
Layer 3 IP/MPLS can take advantage of any path diversity available without any limitations and is also ready to improve network resiliency in any future topology change. These capabilities are the result of the full network topology knowledge possessed by MPLS routers through IP routing.

The Nokia Layer 3 microwave solution

In a traditional architecture, IP/MPLS is overlaid on the microwave transmission as two types of platforms, one for the higher IP/MPLS layer and the other for the microwave transmission layer (see Figure 11). This requires the network to be built on two independent layers and managed by two network management platforms, increasing the complexity for network operators.

The innovative Nokia Layer 3 microwave solution that is also shown in Figure 11 enables seamless deployment of IP/MPLS over microwave networks by integrating the Nokia 7705 Service Aggregation Router (SAR) and the Nokia 9500 Microwave Packet Radio (MPR-e). One 7705 SAR incorporates the functions of the IDU in a traditional architecture. One network management platform, the Nokia 5620 Service Aware Manager (SAM) replaces the two network management platforms in a traditional architecture.

Figure 11. Integrated Nokia Layer 3 microwave transport



The key advantages of the Nokia solution are:

Elimination of dual network managers because the 7705 SAR and 9500 MPR-e are functioning as a single network element managed by one network manager, the 5620 SAM

- Convergence of multiple IDUs and an IP/MPLS router on one platform
- Flexible combination of indoor and outdoor microwave radio
- One management IP address, one network element software image and one maintenance upgrade procedure
- Rapid direct detection of microwave link failures, including high bit error rate
- 1+1 hot standby support with hitless radio protection switching (RPS)
- In-chassis direct power to the 9500 MPR-e
- Less equipment and rack space, easier management, and lower CAPEX and OPEX

Conclusion

Because network outages in mission-critical networks can have immense economic, security and even legal consequences, service availability becomes ever more important. This is particularly true in times of disaster, when multiple simultaneous failures are typical. Therefore, it is vital that the deployed network technology be versatile, resilient and multi-fault tolerant so it can leverage any physical reachability that might remain to restore as much connectivity as possible to the network.

The Nokia Layer 3 microwave solution combines the full-fledged IP/MPLS capabilities of the 7705 SAR with the leading performance of the 9500 MRR-e and the network management capabilities of the 5620 SAM. This solution empowers operators of mission-critical networks with virtually unlimited options in network topology design as networks continue to grow and expand.

For more information about Nokia solutions and products for mission-critical networks. Click here to find out more.

Acronyms

ERPS	Ethernet Ring Protection Switching
IDU	Indoor Unit
FRR	Fast Reroute
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ERPS	Ethernet Ring Protection Switching
IP	Internet Protocol
ITU	International Telecommunication Union
LSP	Label Switched Path
MPR	Microwave Packet Radio
MPLS	Multiprotocol Label Switching
RPL	Resiliency Protection Link
RPS	Radio Protection Switching
RSTP	Rapid Spanning Tree Protocol
SDH	Synchronous Digital Hierarchy
SONET	Synchronous Optical Network
STP	Spanning Tree Protocol
RSTP	Rapid Spanning Tree Protocol

References

1. IEEE. 802.1D-1990 - IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges.
2. IETF. Fast Re-route Extensions to RSVP-TE for LSP Tunnels, May 2005.
3. ITU-T G.8032, Ethernet Ring Protection Switching, February 2012 and Amendment July 2013.

Nokia Oyj
Karaportti 3
FI-02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Product code: PR1502009129EN