Routing Packets in Provider's Network: A Multi-Service Operator's Perspective

A technical paper prepared for presentation at SCTE TechExpo24

Deependra Malla
Sr. Lead Network Design Engineer
Cox Communication Inc.
deependra.malla@cox.com

Table of Contents

List of Figures

1. Introduction

To accommodate the exponential growth of internet-connected devices and the increasing demand for bandwidth-intensive applications and services, Multi-Service Operators (MSOs) are adapting to evolving technologies, expanding their network infrastructure, and optimizing their operational activities. However, the traditional approach of running a network is not enough to support today's as well as tomorrow's network infrastructure that is becoming more complex and diverse.

In this paper, the author explores contemporary approaches and strategies shaping the network architecture of service providers that are used to route packets inside the provider's network with a focus on MSOs. The emphasis is on optimizing routing protocols, addressing evolving security challenges, and harnessing innovative technologies to meet the demands of modern network environments. Current routing protocols used in provider networks have served the networking industry very well, but they are not safe from the evolving cyber security threats. The importance of Internet can't be underestimated and to make it secure and reliable we must mitigate threats like BGP (Border Gateway Protocol) hijacking through the implementation of Resource Public Key Infrastructure (RPKI) and protect protocol adjacencies with robust authentication mechanisms.

The advancement in network processor chips such as merchant silicon and custom silicon have transformed the network architecture into a service specific architecture which is helping providers to optimize their network deployment. Similarly, the advancement of coherent optics has enabled network operators to move to higher bit rates such as 400G ZR/ZR+, and 800G ZR/ZR+ thereby helping service providers realize economic benefits, maximize fiber usage, and ultimately reducing data transport costs. The new network infrastructure and routing design should adapt to these evolving technologies.

The paper also highlights the role of Multiprotocol Label Switching (MPLS), and Segment Routing (SR) in enhancing scalability, efficiency, flexibility, and network programmability in service providers' networks.

In general, end-to-end provider networks can be visualized using the following diagram. While this diagram is very high-level, it illustrates how modular and hierarchical network design facilitates data communication for customers. This paper discusses the general practices seen in multi service providers network design based on Figure 1. Majority of the discussion provided in the paper is based on author's experiences on designing, implementing, and supporting Cox Communication's metro and backbone networks, but the concepts discussed in this paper is equally applicable to other providers.

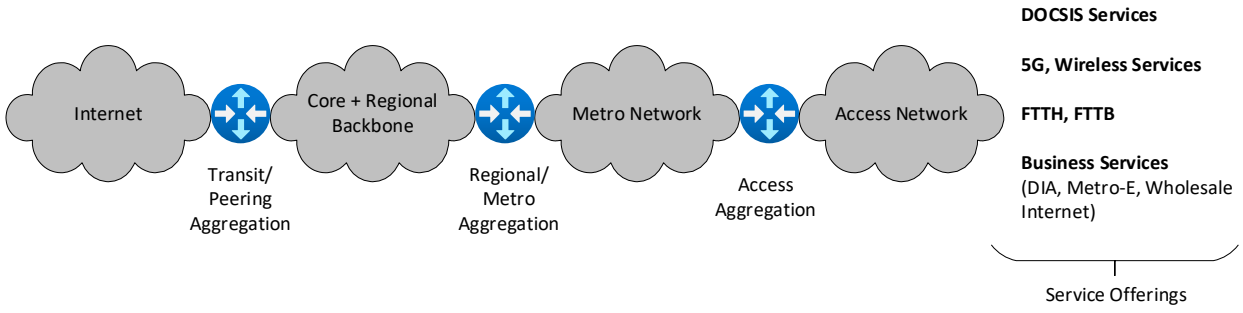

Figure 1 – High level overview of provider's network topology

2. Routing in Access and Metro Networks

2.1. Access Network Evolution

The evolution of access networks in Cable Multi Service Operators (MSO) has always been driven by the need to meet increasing demands for bandwidth, better service quality, and support for emerging applications and technologies. Since its inception in the late 1990s, the combination of analog fibers and the HFC technology with the possibility of two-way communication marked the significant evolution in the cable industry and set the stage for multiple service offerings from the MSOs' perspective.

The DOCSIS® standards that drive cable broadband services have gone through significant evolution to reach today's standard. The evolution of DOCSIS reflects the substantial advancements in cable modem technology to meet the growing demand for high-speed Internet and other data services. Introduced in 1997 as DOCSIS1.0, it enabled Internet access with 38Mbps downstream and 9Mbps upstream. Subsequent versions of DOCSIS such as 1.1, 2.0 and 3.0 introduced Quality of Service (QoS), enhanced upstream capabilities, and channel-bonding respectively, pushing download Internet speed to 1Gbps. In 2013, CableLabs introduced DOCSIS 3.1 specifications. This standard further revolutionized the cable Internet by enabling the use of advanced modulation techniques such as OFDM and increased spectral efficiency that allowed speeds up to 10Gbps downstream and 1-2Gbps upstream. The upcoming DOCSIS 4.0 standard promises to deliver symmetrical multi-gigabit speeds and enhanced network reliability, positioning cable networks to support future high-bandwidth applications and services efficiently.

In the past decade, the industry trend has been to push fiber optics deeper into the network and closer to the customers. This strategy, often referred to as "Fiber Deep," involves reducing the length of coaxial cable runs and increasing the number of fiber-fed nodes. This Fiber Deep strategy led to the innovative access network design called Distributed Access Architecture (DAA) used by MSOs to enhance the performance, scalability, and efficiency of the HFC network. The DAA involves moving certain key components of the cable infrastructure from headend or hubs closer to the end users by leveraging advanced technologies like Remote-PHY and Remote MAC-PHY.

The explosive growth of high-bandwidth applications like streaming, gaming, virtual reality, and smart home devices created an insatiable demand for faster and more reliable internet connections. The evolution of PON to deliver FTTH for Cable Internet Service Providers marks a transformative shift towards high-performance, low latency, and highly reliable future-proof network infrastructure. By adopting FTTH, cable MSOs can meet the growing demands for high-speed internet, stay competitive in the broadband market, and provide their customers with reliable and scalable internet services. This transition, while challenging, positions Cable MSOs to effectively address the technological advancements and bandwidth requirements of the digital age.

Cable MSOs are also increasingly integrating Wi-Fi and mobile services to their existing portfolio to provide seamless connectivity to their customers. This includes deploying public Wi-Fi hotspots and offering mobile virtual network operator (MVNO) services. The integration of 5G technology presents opportunities for cable MSOs to offer enhanced mobile broadband services and low-latency applications, leveraging their extensive fiber infrastructure to support 5G backhaul.

2.2. Access Network Architecture

Most multiple services operators (MSOs) use linear point-to-point optical fiber on their access fiber network between the headend and primary optical node, but some MSOs like Cox Communication use an access fiber network with a diverse ring topology to add a level of protection from fiber cuts, as shown in figure 2. The access fiber path can range in overall distance up to 60 km and meets at the primary optical

node into an optical bypass switch. The optical bypass switch is responsible for selecting the primary or backup path and provides an optical failover associated with loss of light on the primary path during a fiber cut event. A typical primary optical node in Cox legacy HFC network services 500 household passed (HHP).

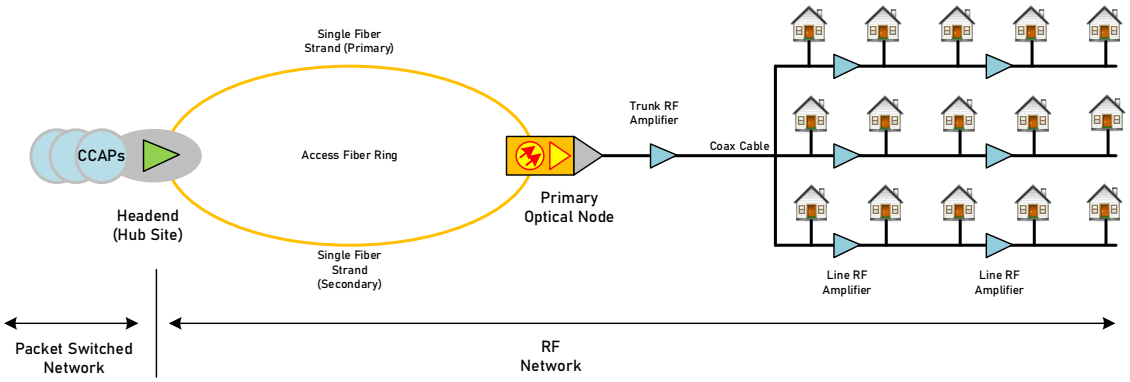

Figure 2 – Cox Communication legacy HFC network architecture

To meet the continuous increase in demand for bandwidth and scalable services, MSOs have started to evolve and transform their analog access network to a modern digital access network by adopting the new Distributed Access Architecture (DAA). DAA is a Fiber Deep technology developed by CableLabs. DAA technology allows cable operators to disaggregate traditional Integrated CCAP (I-CCAP) into several key network components and functions and move them closer to the subscribers. It helps in reducing power and space requirements at headend and improves signal quality from customers to the headend. This digital transformation also enables operators to automate and virtualize various aspects of the new access network infrastructure.

DAA can be broadly classified into two technological variants:

a. **Remote PHY Architecture:** This architecture relocates the PHY component of I-CCAP closer to the subscriber. A Remote PHY Device (RPD) replaces an existing fiber node or a primary optical node in Cox's case. Given the maturity of RPHY specifications from CableLabs and availability of RPHY devices from various vendors, several MSOs including Cox, have chosen RPHY technology as their DAA architecture. RPDs in DAA can be deployed in N+0 as well as N+X models.

b. **Remote MacPHY Architecture:** Another variant of DAA is Remote MAC PHY technology where the PHY as well as MAC domains are relocated close to the subscriber. The new access and aggregation network needs to support a seamless transition from RPD to RMD solutions where the control plane and data plane are truly separated.

Figure 3 shows the high-level architecture of Cox DAA network deployment. As mentioned previously, Cox access fiber network is unique in that it utilizes a diverse ring topology from headend to primary optical node instead of linear point to point fiber. To preserve the ring topology of the access fiber, Cox designed and deployed Optical Communication Module Link (OCML) Extenders as DWDM components to transport multi-wavelength optical signals over the existing ring fiber infrastructure. OCML amplifies and multiplexes unique 10G DWDM wavelengths onto a single fiber. It also demultiplexes all DWDM wavelengths in the reverse direction.

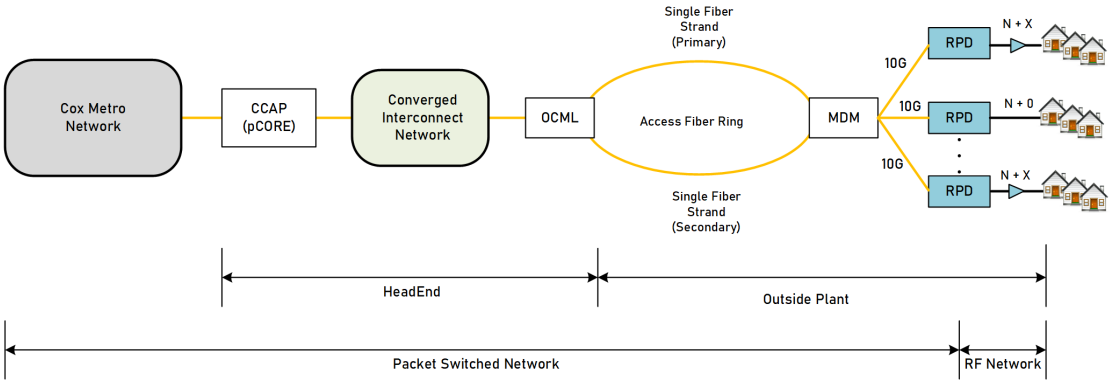

Figure 3 – Cox Communication high level DAA network topology

To enable the deployment of Distributed Access Architecture, MSOs must build a Converged Interconnect Network (CIN). In Cox's case, the OCML interfaces with Cox's packet switch network and provides connectivity between the CIN at headend and RPDs at field.

Converged Interconnect Network (CIN)

CIN provides the connectivity between service cores at headend and nodes at fields for DOCSIS traffic. Although the CIN network primarily connects RPDs with digital CCAP cores, it can support multiple access network terminations such as RMDs, R-OLTs and wireless backhaul and fronthaul. From the topology perspective, CIN is often deployed as spine and leaf architecture with leaf routers aggregating RPDs.

Different MSOs have different deployment architectures for CIN. Figure 4 shows Cox Communication's CIN topology in a typical metro network. The defining characteristics of this architecture are the implementation fully layer 3 solution based on IPv6 addressing only, use of SR-MPLSv6, and any-to-any solution.

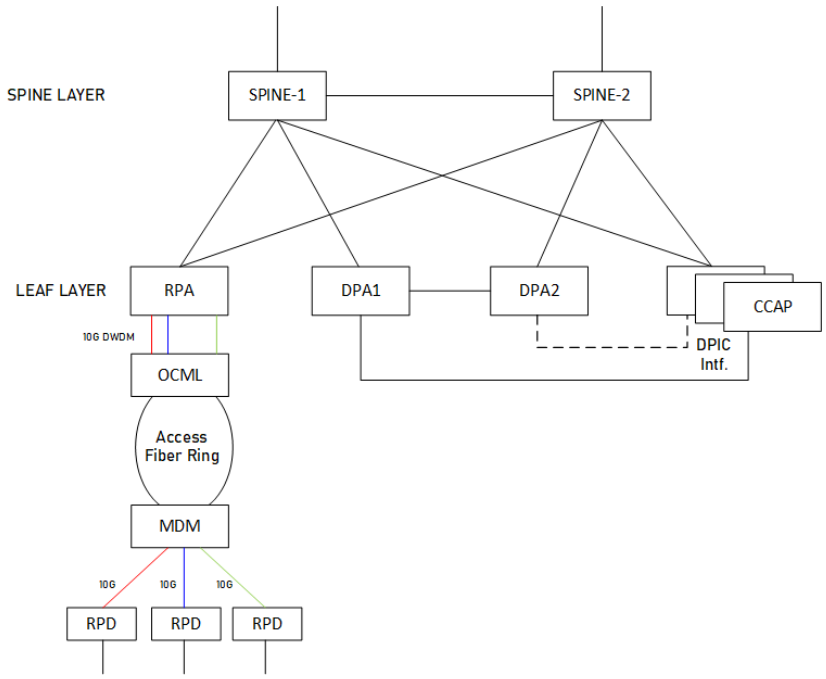

Figure 4 – Cox Communication CIN topology

Extension of packet switching technology using CIN and DAA to the field up to RPDs have reduced the length of RF cables in MSO footprint. This has several implications from the perspective of routing packets in access networks as well as from the customer experience. The extension of ethernet to the field nodes enhances access network's performance by improving signal quality and reducing latency, resulting in a better customer experience. It also increases network capacity and scalability, enabling higher data rates and easier expansion. Additionally, the packet switching technology extension to the field supports future technologies like DOCSIS 4.0, ensuring the network is future-proof and ready for advanced services.

2.3. Metro Network Architecture

Metro network architecture is a crucial segment of an MSO's network infrastructure that connects residential and business customers to larger core or regional core networks, enabling the delivery of various services such as internet access, voice, and video. These networks are designed to provide high-bandwidth connectivity within metropolitan or urban areas and bridge the gap between local access networks and the broader core networks that span a region or a nation.

The physical topology of the metro network varies among service providers, but the design philosophy is usually consistent among them. The primary characteristics of a metro network in a provider's network are as follows:

- High throughput and scalability
- Low latency
- Reliability and redundancy
- Advanced traffic management
- Dense network topology
- Diverse service support
- Interoperability

From the physical topology perspective, a metro network can be full mesh, partial mesh, ring, or hub-and-spoke network. Each of these topologies are used to optimize performance, reliability, scalability, and cost. The choice of topologies depends on the provider's size, scale, and underlying physical infrastructure. Figure 5 shows a high-level overview of a metro and access network. The example architecture shows the current deployment standards in Cox Communication's metro network.

The metro network in Cox is a hub-and-spoke topology with access routers (ARs) as spokes aggregating RPDs, OLTs, FWA, etc. At every headend, Cox has a pair of redundant routers that serves as an aggregation router for all access routers. These headend aggregation routers are further aggregated at regional layers by regional distribution routers. Underlying DWDM transport in each metro is in a ring topology that provides diverse two-degree fibers to each pair of headend aggregation routers.

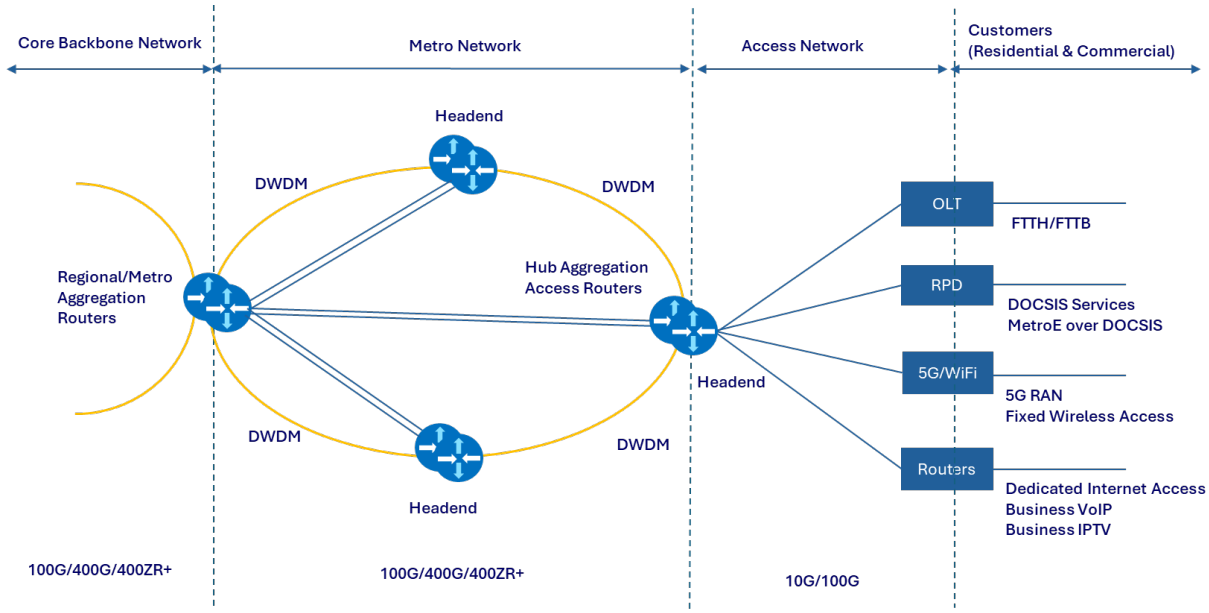

Figure 5 – High level overview of metro and access network

In modern metro networks, MSOs and service providers face challenges of ensuring efficient routing, scalability, and manageability to meet growing customer demands and complex traffic patterns. Although the choice of routing and label switching protocols varies among individual service providers, most service providers typically use Border Gateway Protocol (BGP) and IS-IS or OSPF as their Interior Gateway Protocol (IGP). MSOs deliver linear broadcast video across their metro network as multicast traffic. Most providers use PIM-SSM to deliver multicast traffic. Advanced techniques such as BGP hierarchical route reflection (BGP HRR), MPLS and segment routing, are used as solutions to provide efficient routing at metro networks.

BGP Hierarchical Route Reflection (BGP HRR)

BGP is a de facto protocol to exchange routing prefixes between and within provider networks. Since its introduction, it has evolved tremendously to adapt to the changing network dynamics. BGP route reflection is a method used to reduce the number of BGP sessions in a network and to simplify the management of BGP routing tables. Traditional BGP requires a full mesh of BGP peering sessions between routers within the same autonomous system (AS), which becomes impractical as the network grows. Inline Route reflectors (RRs) are used to eliminate the need for a full mesh by allowing certain

routers to act as intermediaries that reflect routes to other routers. Hierarchical route reflection further extends this concept by organizing route reflectors in a hierarchical manner. This hierarchical approach optimizes the scalability and manageability of large networks. Below are some benefits of BGP HRR:

- Scalability:
  - Compared to the BGP full mesh, hierarchical route reflection significantly reduces the number of BGP sessions required, making it feasible to scale the network to accommodate many routers and routes.
  - It allows for a tiered structure where top-tier route reflectors handle route aggregation and distribution, and lower-tier reflectors manage routes for local regions or segments.
- Improved Convergence:
  - The hierarchical structure helps in faster route convergence, as updates are propagated efficiently through the levels of route reflectors.
  - This results in improved network stability and reduced downtime during routing changes or failures.
- Simplified Management:
  - Hierarchical route reflection simplifies the management of BGP configurations by centralizing route policies and controls at various levels of the hierarchy.
  - This centralized approach reduces the administrative overhead and complexity associated with managing many BGP sessions.

In metro networks, hierarchical route reflection is particularly beneficial due to the high density of routers and the need for efficient routing within metropolitan areas. By implementing a hierarchical structure, service providers can ensure optimal route distribution and scalability, which is essential for maintaining high-performance and reliable services in metro networks.

Limitation of traditional label switching techniques

Traditionally, service providers have been using Label Distribution Protocol (LDP) and Resource Reservation Protocol (RSVP) to label switch their traffic in metro and core backbone networks. However, emerging technologies such as Multi-access Edge Computing (MEC), 5G networks, and the Internet of Things (IoT) are driving latency-sensitive traffic in metro networks, forcing service providers to rethink how to provide uninterrupted services to customers. The existing rigid label switching protocols, such as LDP and RSVP, cannot support the new stringent traffic characteristics and emerging network slicing requirements. To meet these demands, service providers are adopting programmable and software defined networks (SDN)-friendly label switching mechanisms such as segment routing.

LDP and RSVP, while foundational in traditional MPLS networks, have notable limitations. LDP lacks scalability and flexibility with a growing number of routers in the network and lacks dynamic traffic engineering, leading to slower convergence times. RSVP, although capable of reserving resources, is complex to manage and not scalable for large networks, requiring extensive state information to be maintained at each router. Both protocols fall short in supporting modern requirements like low-latency, fine-grained traffic engineering, and network slicing essential for emerging technologies.

Segment Routing (SR)

Segment Routing (SR) is a modern network architecture and forwarding paradigm that simplifies the way packets are routed through networks. It leverages source-routing principles and enables efficient traffic engineering, optimal path selection, and seamless integration with software-defined networking (SDN) principles. SR is particularly suited for Multiprotocol Label Switching (MPLS) and IPv6 networks. There are two types of Segment Routing technologies - SR with MPLS data plane (SR-MPLS) and SR with

IPv6 data plane (SRv6). Although there are two schools of thought on the implementation of segment routing for IPv6 traffic (SRv6 and SR-MPLSv6), the choice between these two technologies depends on the specific needs, existing infrastructure, and strategic direction of the multi service operator. Many service providers today have significant investments in MPLS infrastructure as well as operational expertise and can easily transition their network into an SR-enabled network. Compared to LDP, SR offers the following benefits:

- Ability to introduce traffic engineering and path optimization,
- Simplicity and reduced protocol states in the network,
- Improves scalability,
- Flexibility and programmability,
- Unified control plane,
- Less than 50ms traffic re-routes during link and node failure,
- Easy integration with SDN and automation.

Apart from Internet services, MSOs also provide time sensitive real-time traffic such as voice, video, and streaming services to their customers. These critical services are the driving factors for the enablement of fast reroutes in the metro network. In SR enabled network, Topology Independent Loop-Free Alternate (TI-LFA) provides the desired protection mechanism for such critical traffic. TI-LFA is a fast reroute (FRR) mechanism used in networks to provide protection against link and node failures. It is specifically designed to work in IP networks, including those running Segment Routing (SR), and aims to quickly restore connectivity in case of failures while avoiding the creation of forwarding loops. TI-LFA enhances network resilience and ensures that traffic continues to flow smoothly even during network disruptions.

There are three types of FRR – Classic Loop Free Alternate (cLFA), Remote Loop Free Alternate (rLFA) and Topology Independent Loop Free Alternate (TI-LFA). cLFA and rLFA do not provide 100% coverage and TI-LFA does. At Cox we have deployed TI-LFA with link protection option. TI-LFA provides 100% link and node protection and micro loop avoidance. It always routes protected traffic on the post convergence path. Since Cox metro topology is dual egress hub-and-spoke topology, the primary benefit of TI-LFA implementation is micro-loop avoidance rather than post-convergence optimization.

Since TI-LFA uses Segment Routing for the repair path, SR must be deployed in the network for TI-LFA to work. Following are the benefits of TI-LFA:

- TI-LFA provides less than 50ms link, node and SRLG (Shared Risk Link Group) protection with 100% coverage.
- The repair path is automatically computed by IGP.
- TI-LFA uses a post-convergence path as a backup path.
- TI-LFA can be incrementally deployed; it is locally significant.
- TI-LFA also protects LDP and IP traffic in addition to SR traffic.

As the networking landscape continues to evolve, transitioning from LDP to SR can offer significant advantages to network operators. MSOs like Cox Communications are actively transitioning their metro network to segment routing to replace legacy label switching protocols building foundations for the evolution of modern and programmable networks. So, when packets get routed through a MSO's metro network, they are properly label switched with preprogrammed backup paths to avoid any interruptions in services.

3. Routing in Core Backbone Networks

Serving as the primary infrastructure of a service provider network that interconnects regional and metro networks, today's core backbone networks facilitate the efficient transport of extremely high volumes of traffic across long distances. They ensure seamless connectivity between diverse network segments, data centers, and peering points, supporting critical functions like Internet services, content delivery, cloud services, and real-time applications. The robustness and performance of core backbone networks are extremely important in meeting the growing demands for bandwidth, low latency, and high availability in modern digital communication networks.

Although the physical topology of core or regional backbone networks varies among service providers, most are designed as partial mesh networks to ensure high reliability while spanning regions, countries, or even continents through long-haul connections. Below are some key characteristics of core backbone networks:

- High capacity and scalability
- Highly redundant, reliable, and lossless connectivity
- Low latency
- Interconnectivity
- Operationally efficient
- Simplified architecture

Figure 6 presents a high-level network diagram of a core backbone network. Typically, for larger networks, a hierarchical structure is implemented that consists of a core backbone and multiple regional backbone networks in a layered architecture. Usually, medium to small size service providers have a contiguous single core backbone network connecting metro networks, peers, and transits. The example shown in figure 6 models the high-level backbone network of Cox Communications.

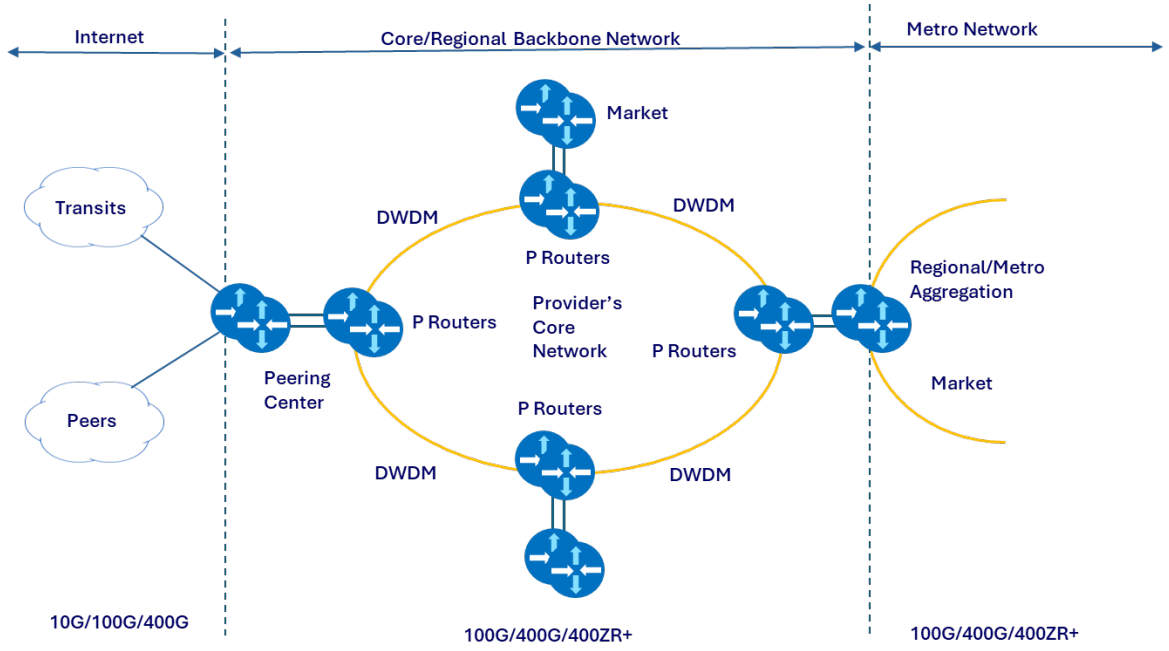

Figure 6 – High level overview of core backbone network

As customer traffic demand, the size of Internet routing tables, and the number of hardware devices in the core backbone network continue to increase, the resulting pressure on both the control plane and the data plane of the core network intensifies significantly. The control plane, responsible for maintaining the network's routing information and making decisions on data packet forwarding, must manage a rapidly growing and increasingly complex set of routes and traffic patterns. Simultaneously, the data plane, which handles the actual forwarding of packets based on the control plane's decisions, must cope with escalating volumes of data traffic, ensuring that packets are transmitted efficiently and reliably.

To manage this traffic effectively, service providers employ proven routing techniques such as BGP, IGP, and label switching protocols. BGP is utilized for inter-domain routing, enabling different networks to exchange routing information. Interior Gateway Protocols (IGPs), such as OSPF (Open Shortest Path First) and IS-IS (Intermediate System to Intermediate System), are used within the provider's own network to ensure efficient and reliable routing whereas label switching protocols such as RSVP, LDP and SR are used to efficiently route packets in provider's core network.

3.1. Routing in the Core Backbone Network

BGP Route Reflection is a critical routing architecture for managing large scale networks in a provider's core network. It enables scalability, reduces complexity, and optimizes resource utilization on core routers while facilitating the exchange of routing information between autonomous systems (AS). In large core networks, the traditional full-mesh Internal BGP (iBGP) peering can become impractical due to the exponential increase in the number of Internet routes along with increasing peers and transits as the network grows. BGP Route Reflection is a scalable solution to this problem. Usually, providers logically group their devices in a region and implement several route reflector servers per region that are responsible for reflecting routes to their respective region's route reflector clients while maintaining iBGP full mesh between regional route reflector servers.

Another important component of any core backbone routing is the interior gateway protocols. While both OSPF and IS-IS are popular choices for IGPs in the core backbone networks of service providers, IS-IS is often favored in very large and high-performance environments due to its protocol efficiency, scalability, and robustness. However, OSPF remains a widely adopted and trusted protocol due to its comprehensive feature set, rapid convergence, and broad vendor support. The choice between OSPF and IS-IS ultimately depends on the specific requirements, design preferences, and operational considerations of the service provider's network.

These IGPs facilitate the routing of packets in the provider's network by providing the appropriate BGP next-hop information to BGP learned prefixes. One of the critical design requirements of a core backbone is to provide low latency to the transit traffic. By default, IGP metric or cost design plays in important role in providing low latency to transit traffic. Cox Communications uses *delay-based cost/metric* to define the IGP cost of the layer 3 links between routers. This ensures that customers traffic always stays on the low latency path in the core network.

Label switching protocols like LDP, RSVP and SR play critical roles in a provider's network. These protocols enable the creation of Label Switched Paths (LSPs) that allow packets to be forwarded based on short, fixed-length labels rather than long network addresses, thus streamlining the routing process and reducing the load on the control plane. These technologies together ensure that even as the network scales and traffic grow, the core backbone can maintain high performance, reliability, and scalability, providing customers with the seamless and efficient service they expect.

The choice of which protocols to use in a core network depends on the provider's size, network architecture, and design requirements. LDP offers simplicity for basic label switching deployment but

lacks stringent traffic engineering capabilities that a provider's core network demands. RSVP and SR enable efficient traffic engineering, quality of service, and rapid failure recovery, ensuring that service providers can meet the ever-growing demand for high-speed, reliable network services.

Cox Communication's core backbone network consists of a collection of provider routers (P) and provider edge routers (PE), utilizing RSVP-TE full mesh between all PE routers. Cox leverages advanced RSVP-TE features such as auto-bandwidth, fast reroute, MPLS TE++, advanced Constrained Shortest Path First (CSPF) tie-breaking, Shared Risk Link Group (SRLG), and Next-Generation Multicast VPN (NG-mVPN) to ensure efficient and lossless traffic switching in the core network. Delay-sensitive traffic, such as voice and video, particularly benefits from these advanced features. Cox's inner core network, which interconnects P routers, operates without BGP, PIM, and IPv6, ensuring a streamlined and efficient core. Linear video traffic is delivered to each market via the core backbone using NG-mVPN, while IPv6 traffic is managed and delivered using IPv6 Provider Edge (6PE).

3.2. Coherent Optical Routing

High bandwidth links such as 400G and 400G ZR+ coherent optics represent a significant advancement in optical networking technology that is designed to enhance the performance, scalability, and efficiency of core and metro network infrastructure in the provider's network. They provide high capacity, extended reach, cost efficiency, and simplified network architecture while meeting the growing demands for exponential increase in bandwidth and the need for an efficient, scalable, and reliable network.

Figure 7 shows the deployment of 400G gray optics with transponders. This deployment is needed when the distance between routers exceeds the deployable range of 400G ZR+ pluggables. Figure 8 shows the deployment of 400G ZR+ coherent optics that don't require transponders thereby saving power, space, and capital expenditure where distance is not a concern.

Cox is redesigning the metro and backbone links to optimize the deployment of 400G gray and 400G ZR+ optics in its metro networks and core backbone networks. Today, Cox uses a mix of express and point-to-point links in the backbone with layer 3 bundles containing up to 30 x 100G (3Tbps) links. By deploying the 400G solution, Cox can reduce the physical number of links by 75%. The 400G ZR+ deployment can cover up to 70% of Cox backbone links.

Figure 7 – 400G links using transponders

Figure 8 – 400G links using coherent optics

400G ZR+ offers significant economic benefits compared to traditional 400G solutions with separate transponders. These benefits include lower capital and operational expenditures, space and power savings, simplified network design, interoperability, and enhanced performance. By adopting 400G ZR+, service providers can achieve cost-effective, scalable, and efficient network upgrades, meeting growing bandwidth demands while optimizing their investment.

4. Security in Provider's Network

As the customer's traffic passes through a service provider's network, it is crucial that a provider maintain the integrity, confidentiality, and availability of data transmitted across their network. Ensuring secure communication involves multi-layered approach of implementing various measures and technologies to protect network infrastructure against threats such as spoofing, hijacking, DDOS, and unauthorized access. Some of the key protocols and methods used to enhance security are discussed below:

- Routing Protocol Authentication

  Routing protocol authentication is crucial for securing the dynamic routing infrastructure of a network. Protocols such as BGP, IS-IS, OSPF, and LDP must use *MD5 authentication* to ensure that the routing information exchanged between routers is authentic and untampered. This is critical for maintaining the integrity, stability, and security of the entire network.

  MD5 (Message Digest Algorithm 5) authentication is a common method used to secure routing protocols. It involves creating a cryptographic hash of the routing message using a shared secret key. The hash is then included in the routing message. The receiving router generates its hash of the message using the same key and compares it to the received hash to verify authenticity.

- Secure network management protocols

  Simple Network Management Protocol version 3 (SNMPv3) is an essential tool for managing and monitoring network devices. It provides significant improvements over earlier versions of SNMP such as SNMPv1, and SNMPv2c, primarily in terms of security and functionality. Although SNMP has been a de facto standard for monitoring networks, the evolving complexity of modern network environments has highlighted its limitations. The traditional SNMP methods are not suitable for providing real-time insights into network performance.
  Streaming telemetry has emerged as a solution to overcome SNMP challenges. Streaming telemetry uses a push-based model to continuously stream data from network devices to a collector in near real-time. This approach offers lower latency, higher frequency updates, and enhanced scalability, making it well-suited for dynamic and large-scale networks.

- Securing BGP

  BGP security is crucial for maintaining the integrity and reliability of the global internet routing system. BGP is inherently vulnerable to attacks like prefix hijacking and route leaks, which can cause significant disruptions. To mitigate these threats, service providers use BGP route origin validation (ROV) through resource public key authentication (RPKI). RPKI is a cryptographic framework that binds IP address blocks to their legitimate owners, enabling network operators to verify the authenticity of BGP route announcements. When RPKI is deployed, a certificate authority issues a Route Origin Authorization (ROA), which specifies which Autonomous Systems (AS) are authorized to originate specific IP prefixes. In addition to RPKI/ROV, other best practices for securing BGP include implementing prefix filtering, AS path filtering, and deploying BGP session authentication using TCP MD5 or TCP-AO.

- Control plane protection

  The control plane of routers is responsible for routing and signaling of routing information in a network, making it a prime target for attacks. To prevent such critical aspects of the network, service providers use several security measures such as access control lists (ACL), control plane policing (CoPP),

5. Conclusion

As the networking landscape continues to evolve, new and efficient technologies are redefining how packets are routed in providers' networks efficiently and securely. The demand for bandwidth and the diversity of traffic with unique characteristics will continue to grow. Emerging technologies such as 400G, 800G, and 1.6T will provide much-needed relief to MSOs in terms of bandwidth capacity. BGP and IGPs like ISIS and OSPF will continue to dominate the routing domain in providers' networks. Efforts are being made to simplify the network to enhance efficiency. Removing LDP and implementing SR offers an opportunity for network simplification by unifying IGP and label switching protocols. Properly securing these protocols is essential for network stability and growth. With emerging services such as IoT and cloud computing, low latency treatment of this traffic has become imperative. Delay-based IGP routing and fast reroute methods will help service providers route traffic with minimal latency and without service disruptions. Since legacy protocols such as LDP and RSVP cannot meet the new traffic characteristics requiring low latency, network slicing, and service continuity, service providers are implementing segment routing (SR) with TI-LFA. The goal of all providers' network designs is to route customers' traffic efficiently and economically by designing solutions that meet today's and tomorrow's demands which would ensure better customer experience.

Abbreviations

AS	Autonomous System
BGP HRR	Border Gateway Protocol Hierarchical Route Reflection
BGP	Border Gateway Protocol
CIN	Converged Interconnect Network
COPP	Control Plane Protection
DAA	Distributed Access Architecture
IGP	Interior Gateway Protocol
IoT	Internet of Things
6PE	IPv6 Provider Edge
IS-IS	Intermediate System to Intermediate System
LDP	Label Distribution Protocols
MD5	Message Digest Algorithm 5
MEC	Multi-access Edge Computing
MPLS	Multiprotocol Label Switching
OSPF	Open Shortest Path First
PIM	Protocol Independence Multicast
QoS	Quality of Service
ROA	Route Origin Authorization
RPKI	Resource Public Key Infrastructure
RSVP	Resource Reservation Protocol
SDN	Software Defined Networking
SNMP	Simple Network Management Protocol
SR	Segment Routing
TI-LFA	Topology Independent Loop Free Alternate
ZTP	Zero Touch Provisioning

Bibliography & References

Segment Routing, Part 1, Clarence Filsfils, Kris Michielsen, Ketan Talaulikar
Segment Routing, RFC 8402, Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir
Segment Routing: A Comprehensive Survey of Research Activities, Standardization Efforts, and Implementation Results, Pier Luigi Ventre et. al., IEEE Communication Surveys & Tutorials, Vol. 23, No.1, 2021
Cox Next Generation 400G IP+OLS Architecture for Maximum Network Optimization and Cost Benefits, Saurabh Patil, Jason Bishop, SCTE Cable-Tech Expo 2023
Deploying Segment Routing for PON aggregation in Cox' Metro Network, Deependra Malla, SCTE Cable-Tech Expo 2023