ISP networks - Differences and Challenges

Johannes Rief, Florian Wiedner*
*Chair of Network Architectures and Services
School of Computation, Information and Technology, Technical University of Munich, Germany
Email: johannes.rief@tum.de, wiedner@net.in.tum.de

***Abstract*—This paper presents information about Internet Service Provider (ISP) Networks and their challenges. It takes a closer look at the network structure and covers routing technology such as Internet Protocol Addresses and Multiprotocol Label Switching. Furthermore the paper presents Content Delivery Networks and Data Center Networks and how they work together with ISP networks to offer services over the internet to users. Finally we will present general difficulties that can occur when operating an ISP Network and general attributes of the Networks that are worth optimising. These include network security and internet connection in rural areas.**

***Index Terms*—ISP: Internet Service Provider; IP: Internet Protocol; MPLS: Multiprotocol Label Switching; CDN: Content Delivery Network; DCN: Data Center Network**

1. Introduction

Internet Service Providers (ISP) are essential for todays structure of the Internet because they provide households as well as companies an access to communication via the Internet. Without them, the Internet as we know it today would not exist. They are normally supervised by companies like Telekom and Telefonica in Germany or AT&T and Comcast in the United States and form the "Internet Backbone", a large scale network connecting most parts of the world [1]. Because of the importance of consistent communication especially in the business sector, ISPs have to ensure stability in their network and provide high speed connections. In this paper we will first try to give a structural overview of ISP networks and routing technology like Multiprotocol Label Switching (MPLS) and Internet Protocol (IP) Addresses. Additionally we will look at Content Deliver Networks and Data Center Networks and how they work together with ISP networks. In Section 4 we address the main challenges of ISP networks like network failure and challenges in network security. We conclude with providing solutions to these challenges.

2. Related work

One important reference of this paper is chapter 2 of Rober D. Doverspikes et. al. book about ISP networks [2]. This chapter goes more in depth about the structure of ISP networks and its different network layers. It also addresses network failures and possible fixes that can be applied. Furthermore the MPLS is explained in his work, which is also mentioned in this work. While Doverspikes book about ISP networks describes the networks architecture and network protocols in great detail, this paper tries to give a very broad overview of all aspects of ISP networks. Our focus lies more on different challenges of ISP networks and possible solutions to them.

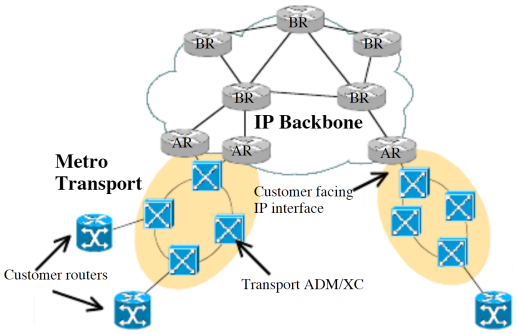

Figure 1: ISP network structure [3]

3. Background

In this part of the paper we will introduce ISPs and how they can be categorized into different tiers. This is followed by an overview of the structure of ISP networks. Additionally, we will look at IP Addresses and MPLS and how they help to perform efficient routing in ISP networks. Finally we present different networks like Data Center Networks and how they work together with ISP networks to offer services to customers over the Internet.

3.1. ISPs

ISPs are companies that provide routing infrastructure to transport data over the Internet. Additionally, they provide services like email hosting and virtual private networks. ISPs can be roughly categorized into three different tiers depending on their provided services and size. Tier 1 ISPs are the largest and maintain wide ranging networks and are connected to other Tier 1 ISP to transport Data over far distances. Well known examples are ISPs like Deutsche Telekom or AT&T [4]. While Tier 2 ISPs still operate their own national networks, they rely on Tier 1 ISPs for wide Internet access. Tier 3 ISPs offer Internet in regional areas and depend on Tier 1 and 2 networks for Internet access [5].

Also the models of different ISPs can vary. A Wholesale ISP offers services to different ISPs as well as

 doi: 10.2313/NET-2024-09-1_04

businesses, rather than end-users like private households. Customers of these ISP present a middle man who sells these services to their own customers. The most commonly known ISPs are Retail ISPs. They provide Internet access to end-users and typically package it into bundles. These include a certain tier of network speed and different services depending on the amount the customers are willing to pay [5]. The Managed Service Providers model includes selling broad IT services to companies like network infrastructure management and network security. There are even more types of models for ISP networks [5].

3.2. Structure of ISP networks

ISP networks are a main part of todays Internet and have the task to enable Internet communication for households and businesses. An ISP network consists of many routers located in different areas that control network traffic and route packets to their correct destinations. As seen in figure 1 customers are connected to an ISP network through their own router which is normally provided by the ISP itself. This router is indirectly connected to an access router (AR) of the ISP network which is part of the the IP-Backbone. The IP Backbone is a network of Backbone routers (BR) that are connected with each other over long distances. This makes communication all over the world possible. Access routers are the entry point for data from customers into the wide ISP network [2].

In between the customer and access router the packets are transported via metropolitan transport networks [3]. The metropolitan network, also called access network, is more local compared to the wide spanning Backbone network. It connects multiple households and businesses to the access routers of the an ISP network. There are multiple technolgies used in metro networks to transport data. A typical contender is Digital Subscrible Line (DSL) which makes use of telephone lines and is quite limited in terms of speed and bandwidth of the Internet access. Fiber-Optic cables are the much superior alternative compared to DSL if they are available in the area. Also very commonly used is a wireless connection between the end-user and an ISP. This includes mobile connection like 5G which is transmitted over radio waves to a mobile device. Another possibility is satellites which can cover huge areas but lack bandwidth and speed [5].

Network layers play a significant role in ISP networks as they organise network hardware into different layers, depending on the functionality. Each layer of ISP networks consits of nodes and links. These together can form connections for packets to travel through. The different network layers are affected by each other. For example each connection in a higher level network layer is represented by one or multiple connections in the lower layer. Therefore if network failures in lower layers occur this directly affects connections in higher layers of the network. A single connection failure in a lower network layer can disrupt multiple connections in a higher layers which makes the lower level network design very important [2].

One of the layers in ISP networks is the network Layer which is also represented in Figure 1 as the IP Backbone. In that layer, nodes are represented as routers that have the task to route packets, sent out by customers, through the network and finally to their correct destination. Transportation itself is performed over lower layers of the network that interact with the network layer inorder to fulfill their task of transportation [2].

The layer at the bottom of the network architecture is the Physical layer. This layer represents the physical optical fiber cables layed mostly underground around the world. They connect all the central offices of the ISP network, which are central Hubs connecting multiple households in one area to a singular network node [2].

At the very top of these layers ISP networks can also offer services like VPN to connect multiple local networks or Voice over IP. Voice over IP is a service to transmit phone calls not via the traditional way but rather as data packets that are routed over the IP layer of the ISP network [6].

3.3. OSI model

Not only the architecture of ISP networks can be structured into different layers. Also important is the protocol layering of Internet communication over ISP networks. Each message that is sent over the Internet is modified by many protocols that turn the message into packets which are fit to be transported over the network. A standardization of this protocol layer modell for package transport via Internet and therefore using ISP networks is the OSI modell defined by ISO, an Organisation for Standardisation. It defines seven different layers that all execute a specific part of the task to make Internet communication possible [7]. An important protocol layer of the OSI model in ISP networks is third layer called network layer. This layers job is to ensure that the data packets send by one source arrive at their correct destination in the network. It includes routing protocols as well as logical addressing of packets [8].

3.4. IP Addresses

As discussed in section 3.3 about the OSI model, the network layer has to correctly address the source and destination of data packets. In most computer networks including ISP networks this is accomplished with IP addresses. Each IP address uniquely identifies every device in the network and there are two different types of IP addresses. IPv4 is the older IP address version and ist represented by a 32-bit Integer while the newer version IPv6 is 128 bits long. To ensure the correct delivery of data packets, the packets receive a source and destination IP Address header in the network layer. This allows routers in the network to correctly pass on the packets [8]. As IPv4 only allows 4.3 billion different addresses, it is by far not enough to address every device of the Internet. Thats why IPv6 usage is increasing in ISP network architecture [5]. Network Address Translation (NAT) is a method which maps a public IP address to multiple private ones and therefore can increase the IPv4 addressing possibilities. This however isn't sufficient in all cases as it can't be applied to applications that use end to end communication [9]. In the case of IPv6 addressing NAT isn't necessary as the amount of addresses cover more than is necessary in the forseeable future. That's why transitioning from IPv4 to IPv6 is important. However the transition is costly,

especially in developing countries, as they are missing the financial opportunities and correct training [9].

3.5. MPLS

Routing data packets is the main purpose of ISP networks. Therefore the routing has to be especially efficient. Two main goals of routing are to determine the shortest path between two endpoints and balancing the load of different connections [10]. Multiprotocol Layer Switching (MPLS) is a technology, used in ISP networks to efficiently route packets through the network. When MPLS is used as the routing protocol in the network, edge routers of the network attach certain labels to incoming packets. After inner routers receive packets with a label, they only have to examine the label to determine its next destination. When forwarding the packet, the router also swaps out the label of the packets for a new one for the next router to examine. The paths that are enforced by the labels are determined by a separate protocol [10]. Using MPLS in an ISP network helps reduce the network latency and keep up with expected quality standards. Therefore it is beneficial to the network [11].

3.6. CDNs

A way to significantly improve latency and performance of services offered over the Internet is through Content Delivery Networks (CDN). They have become especially useful due to rising demand of video on demand or huge download sizes [12]. CDNs are networks of servers that cache data that is frequently used by users. This improves the connection speed because the servers with the cached data are optimally located closer to the user than the actual Data Centers of the content provider. CDNs can be operated by ISPs themselves or seperate companies and in this case have to work together to optimise network speeds [12]. In general CDNs are benefitial to ISPs as they reduce traffic in their network and also improve user experience [5].

3.7. Data Center Networks

One of the Internets main benefits is the variety of services it offers. The services include email, web search and online games. These services would not be possible without Data Centers, that have the task to store and process Data that is relevant for the respective service. Data Centers include computing resources and storage resources which are interconnected with and intra Data Center Network [13].

A possible design for intra Data Center Networks is the cluster network design. In this design a cluster is a basic part of the network. A cluster connects multiple server racks through cluster switches. Devices inside a Server Rack are connected via a Top-of-rack switch. The cluster switch aggregators connect multiple cluster switches and makes communication between cluster in the network possible. A data center also includes core network devices which are the access point for data transport between different data centers and the internet [13].

Data Center providers like Facebook, Google or Amazon typically operate multiple Data Centers. These also have to be connected via an inter Data Center Network to efficiently exchange Data. Not only do providers use their infrastructure for their own services but they also sell it for other companies to offer their own services. Compared to ISP networks Data Center Networks (DCN) do not transport Information between third parties over their network but rather exchange Data between their own Services that are running in Data Centers of their network. Inter DCNs consist of edge nodes that rout traffic in the backbone network. This is very similar to Backbone routers in ISP networks. If users want to use a service provided by the DCN they connect to one of the edge routers over an ISP network. To connect to the correct DCN users use the Domain Name System which can be offered by the users ISP which links Internet Domains to Server locations [13].

3.8. Peering and Transit

As discussed earlier Tier 1 ISP networks can span over huge distances, also connecting multiple countries. On their own however they can only transmit communication between members of their network, which would exclude households or businesses connected to a different ISP. Therefore all ISPs have to agree on contracts with other ISPs to make data transit between their networks possible and provide their customers access to the entire internet. There are two main types of agreements that ISPs can engage in which are Peering and Transit Agreements. A Peering Agreement defines a contract between two ISPs for network traffic between their networks without financial compensation. This is a viable option if both ISPs are similar in size, have similar amounts of customers and around the same amount of network capacity. Peering relationships are not transitive, which means that if the second ISP has another peering relationship to a different ISP, traffic from the first ISP to the additional ISP would not be transported over the second one. In case of a Transit Agreement one ISP has to pay the other for network access depending on the amount of network traffic between them. In this case the agreement is transitive and would allow traffic over the second ISP to another network [14]. This type of agreement is typically used between ISPs of different tiers where lower tier ISPs have to pay higher tier ISPs for their broader access [15].

4. Challenges of ISP networks

In this section of the paper we will address some challenges that occur when operating large ISP networks. For each challenge possible solutions are mentioned that can be applied by ISPs. We will also include some research about making ISP networks more efficient and therefore reducing their substantial contribution to carbon emissions.

4.1. Network Restoration

A main challenge ISP networks have to overcome are network disruptions and outages. This can be caused by the failure of devices which are part of the network or due to maintenance work and can occur in different layers

of the network. In the situation of a network disruption, availability of the Internet can be heavily affected. This is why ISPs have to ensure to always to provide a certain standard of quality, which is defined in the Service Level Agreements (SLA). SLAs are guarantees to the customers which define metrics like latency and packet loss [2].

When it comes to network restoration there are different procedures to apply, depending on the network layer the disruption happens in. For example if a cable in the fiber layer is damaged between two network nodes, the connection has to be manually reestablished over different cables and can take hours [2].

In case of IP layer failures, ISP networks can use the MPLS Fast Reroute to overcome the issue. This method makes use of backup paths for links between network nodes. These alternative paths can reroute incoming packets over functioning connections in case of a failure. It is also quite performant. In case of a connection failure between two network nodes, Fast Rerout is applied in less than 100 ms [2].

4.2. Network Security

Another main challenge ISPs are facing is cyber security in their networks. Their task is to protect customer data as well as protecting network infrastructure. Possible attacks that ISP networks have to defend against include infilitration of malware or Distributed Denial of Serivce (DDoS) attacks. DDoS attacks make use of botnets that overwhelm services, that are part of the Internet, with requests. This hinders users from accessing the service as the servers are overloaded [16]. There are ways for the ISP networks as well as connected servers to protect themselves. Methods include packet filtering to drop packets with suspicious header information. An additional method is load balancing where the ISP temporarily grants the attacked service a higher bandwith to keep the service alive during the attack [17].

4.3. Internet connection in rural areas

In 2019 around 86% of the population used mobile connection to the Internet [18]. The ISPs goals include covering all parts of the world with proper access to the Internet. This is still not the case as many rural areas struggle with a bad quality wireless connection or no connection at all. It stems from the fact that ISPs face geographical challenges when deploying wired or wireless connection in rural areas. Futhermore it is in many cases not worth it to deploy any access in rural areas at all. Compared to cities, rural areas have a much lower population density which means less customers for a similar expense. Eventhough many Internet infrastructure projects are financially supported by the government, the issues still remain [18]. One possible solution to this problem is Satellite connection as Sattelites are not affected by geographical challenges of the area. End-users can directly connect to a Satellite with an Antenna to access the Internet. Satellite deployment still comes with significant costs for the ISP but is a valid option for covering Internet connection of remote areas [18].

4.4. Reducing carbon emissions of ISP networks

The Internet is a a huge carbon emitter. According to Statista, if the Internet itself was a country it would take up the sixth spot on the carbon emission leaderboard [19]. Obviously ISP networks are only a part of the Internet but they do contribute to that number with network routing and operating data centers. A possible solution to that problem is to minimize the amount of active routing devices in the network that are necessary to keep up with the current demand. This is done while still keeping up with certain quality standards for network communications [20]. An approach like this is especially useful, because the normal network design mostly focuses on handling the most amount of traffic during peak-hours. Therefore the energy efficiency falls short when choosing such a design [20]. The theory and approach of this type of network design is explained more in detail in [20].

5. Conclusion and future work

As the paper has shown ISP networks are a very broad topic. Research areas include network architecture, network protocols, network security and many more. Thats why it can be difficult to describe all aspects of ISP networks in just one paper. This paper tried to cover the most important aspects of ISP networks like architecture and routing technologies like IP Addresses and MPLS. We also compared Data Center Networks to ISP networks and how they work together to offer services to customers over the internet. A main aspect of the paper were the challenges that ISP networks are facing. We covered challenges like network security which included DDoS attacks and how to prevent them. The still existing problem of rural internet connection and how satellite internet might be a solution was also addressed. As carbon emission still presents a problem we also mentioned how ISP networks can be optimized to reduce their emissions.

This paper presented more of a broad overview of ISP network challenges. A possible future work could tackle a concrete challenge and go more in depth on the solution to it. The paper could offer a concrete solution to a problem and describe it in detail which was not possible in this paper. Another important topic to present in a future work is user privacy and how ISPs might violate them. As ISPs have huge control over network flow and can easily aggregate data about user behavior, user privacy can easily be violated, and private data misused. A paper could analyze, how ISPs treat their sensitive user data and if any obvious privacy violations exist.

References

[1] A. M. T. Mitchell L. Moss, "The internet backbone and the american metropolis," *The Information Society*, vol. 16, no. 1, pp. 35–47, 2000. [Online]. Available: https://doi.org/10.1080/019722400128310

[2] R. D. Doverspike, K. K. Ramakrishnan, and C. Chase, *Structural Overview of ISP Networks*. London: Springer London, 2010, pp. 19–93. [Online]. Available: https://doi.org/10.1007/978-1-84882-828-5_2

[3] P. Sebos, J. Yates, G. Li, D. Rubenstein, and M. Lazer, "An integrated ip/optical approach for efficient access router failure recovery," 03 2004.

[4] GTT Editorial Team, " Global Tier 1 IP Networks: Everything You Need To Know," 2023, available online at https://www.gtt.net/de-de/resources/blog/global-tier-1-ip-networks-everything-you-need-to-know/; last accessed on 2024/03/18.

[5] PShaun Allen, " ISP Networks: Understanding the Fundamentals," 2023, available online at https://www.shaunallen.co.uk/blog/isp-networks/; last accessed on 2024/03/18.

[6] U. Varshney, A. Snow, M. McGivern, and C. Howard, "Voice over ip," *Communications of the ACM*, vol. 45, no. 1, pp. 89–96, 2002.

[7] F. Becher and J. Steitz, "Iso/osi-referenzmodell."

[8] P. Jasud, "The osi model: Overview on the seven layers of computer networks," *International Journal for Innovative Research in Science & Technology*, vol. 4, no. 3, pp. 116–124, 2017.

[9] B. R. Dawadi, S. R. Joshi, and A. R. Khanal, "Service provider ipv4 to ipv6 network migration strategies," *Journal of Emerging Trends in Computing and Information Sciences*, vol. 6, no. 10, 2015.

[10] X. Xiao, A. Hannan, B. Bailey, and L. M. Ni, "Traffic engineering with mpls in the internet," *IEEE network*, vol. 14, no. 2, pp. 28–33, 2000.

[11] M. A. Ridwan, N. A. M. Radzi, W. S. H. M. Wan Ahmad, F. Abdullah, M. Z. Jamaludin, and M. N. Zakaria, "Recent trends in mpls networks: technologies, applications and challenges," *IET Communications*, vol. 14, no. 2, pp. 177–185, 2020.

[12] N. Kamiyama, T. Mori, R. Kawahara, and H. Hasegawa, "Optimally designing isp-operated cdn," *IEICE transactions on communications*, vol. 96, no. 3, pp. 790–801, 2013.

[13] J. Meza, T. Xu, K. Veeraraghavan, and O. Mutlu, "A large scale study of data center network reliability," in *Proceedings of the Internet Measurement Conference 2018*, 2018, pp. 393–407.

[14] R. Kariyawasam, "Telecoms regulation: Peering and transit over tcp/ip networks," *Computer Law & Security Review*, vol. 17, no. 1, pp. 36–40, 2001.

[15] W. B. Norton, "Internet service providers and peering," in *Proceedings of NANOG*, vol. 19, 2001, pp. 1–17.

[16] N. N. Tuan, P. H. Hung, N. D. Nghia, N. V. Tho, T. V. Phan, and N. H. Thanh, "A ddos attack mitigation scheme in isp networks using machine learning based on sdn," *Electronics*, vol. 9, no. 3, p. 413, 2020.

[17] D. Mahajan and M. Sachdeva, "Ddos attack prevention and mitigation techniques-a review," *International Journal of Computer Applications*, vol. 67, no. 19, 2013.

[18] M. Bhuiyan, "Solutions for wireless internet connectivity in remote and rural areas," Master's thesis, M. Bhuiyan, 2020.

[19] Peter Schmidt-Feneberg, " Infografik: So viel Energie verbraucht das Internet," 2023, available online at https://de.statista.com/infografik/26873/co2-vergleich-dsl-und-glasfasernetz/; last accessed on 2024/03/16.

[20] L. Chiaraviglio, M. Mellia, and F. Neri, "Minimizing isp network energy cost: Formulation and solutions," *IEEE/ACM Transactions on Networking*, vol. 20, no. 2, pp. 463–476, 2012.