Overlay network

An **overlay network** is a logical computer network that is layered on top of a physical network. The concept of overlay networking is distinct from the traditional model of OSI layered networks, and almost always assumes that the underlay network is an IP network of some kind.[1]

Some examples of overlay networking technologies are, VXLAN, BGP VPNs, and IP over IP technologies, such as GRE, IPSEC tunnels, or SD-WAN.

Structure

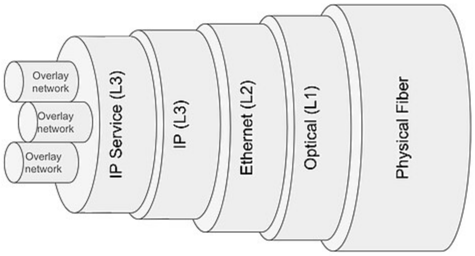

Figure 1: Physical to logical overlay networks

Nodes in an overlay network can be thought of as being connected by logical links, each of which corresponds to a path, perhaps through many physical links, in the underlying network. For example, distributed systems such as peer-to-peer networks are overlay networks because their nodes form networks over existing network connections.[2]

The Internet was originally built as an overlay upon the telephone network, while today (through the advent of VoIP), the telephone network is increasingly turning into an overlay network built on top of the Internet.

Attributes

Overlay networks have a certain set of attributes, including separation of logical addressing, security and quality of service. Other optional attributes include resiliency, encryption and bandwidth control.

Uses

Telcos

Many telcos use overlay networks to provide services over their physical infrastructure. In the networks that connect physically diverse sites (wide area networks, WANs), one common overlay network technology is BGP VPNs. These VPNs are provided in the form of a service to enterprises to connect their own sites and applications. The advantage of these kinds of overlay networks is that the telecom operator does not need to manage addressing or other enterprise-specific network attributes.

Within data centers, it was more common to use VXLAN, however due to its complexity and the need to stitch layer-2 VXLAN-based overlay networks to layer-3 IP/BGP networks, it has become more common to use BGP within data centers to provide layer-2 connectivity between virtual machines or Kubernetes clusters.

Enterprise networks

Enterprise private networks were first overlaid on telecommunication networks such as Frame Relay and Asynchronous Transfer Mode packet switching infrastructures but migration from these (now legacy) infrastructures to IP-based MPLS networks and virtual private networks started (2001~2002) and is now completed, with very few remaining Frame Relay or ATM networks.

From an enterprise point of view, while an overlay VPN service configured by the operator might fulfill their basic connectivity requirements, they lack flexibility. For example, connecting services from competitive operators, or an enterprise service over an internet service and securing that service is impossible with standard VPN technologies, hence the proliferation of SD-WAN overlay networks that allow enterprises to connect sites and users regardless of the network access type they have.

Over the Internet

The Internet is the basis for more overlaid networks that can be constructed in order to permit routing of messages to destinations not specified by an IP address. For example, distributed hash tables can be used to route messages to a node having a specific logical address, whose IP address is not known in advance.

Quality of Service

Guaranteeing bandwidth through marking traffic has multiple solutions, including IntServ and DiffServ. IntServ requires per-flow tracking and consequently causes scaling issues in routing platforms. It has not been widely deployed. DiffServ has been widely deployed in many operators as a method to differentiate traffic types. DiffServ itself provides no guarantee of throughput, it does allow the network operator to decide which traffic is higher priority, and hence will be forwarded first in congestion situations.

Overlay networks implement a much finer granularity of quality of service, allowing enterprise users to decide on an application and user or site basis which traffic should be prioritised.

Ease of Deployment

Overlay networks can be incrementally deployed at end-user sites or on hosts running the overlay protocol software, without cooperation from ISPs. The overlay has no control over how packets are routed in the underlying network between two overlay nodes, but it can control, for example, the sequence of overlay nodes a message traverses before reaching its destination.

Advantages

Resilience

The objective of resilience in telecommunications networks is to enable automated recovery during failure events in order to maintain a wanted service level or availability. As telecommunications networks are built in a layered fashion, resilience can be used in the physical, optical, IP or session/application layers. Each layer relies on the resilience features of the layer below it. Overlay IP networks in the form of SD-WAN services therefore rely on the physical, optical and underlying IP services they are transported over. Application layer overlays depend on the all the layers below them. The advantage of overlays are that they are more flexible/programmable than traditional network infrastructure, which outweighs the disadvantages of additional latency, complexity and bandwidth overheads.

Application Layer Resilience Approaches

Resilient Overlay Networks (RON) are architectures that allow distributed Internet applications to detect and recover from disconnection or interference. Current wide-area routing protocols that take at least several minutes to recover from are improved upon with this application layer overlay. The

RON nodes monitor the Internet paths among themselves and will determine whether or not to reroute packets directly over the Internet or over other RON nodes thus optimizing application-specific metrics.[3]

The Resilient Overlay Network has a relatively simple conceptual design. RON nodes are deployed at various locations on the Internet. These nodes form an application layer overlay that cooperates in routing packets. Each of the RON nodes monitors the quality of the Internet paths between each other and uses this information to accurately and automatically select paths from each packet, thus reducing the amount of time required to recover from poor quality of service.[3]

Multicast

Overlay multicast is also known as *End System* or *Peer-to-Peer Multicast*.[4] High bandwidth multi-source multicast among widely distributed nodes is a critical capability for a wide range of applications, including audio and video conferencing, multi-party games and content distribution. Throughout the last decade, a number of research projects have explored the use of multicast as an efficient and scalable mechanism to support such group communication applications. Multicast decouples the size of the receiver set from the amount of state kept at any single node and potentially avoids redundant communication in the network.

The limited deployment of IP Multicast, a best-effort network layer multicast protocol, has led to considerable interest in alternate approaches that are implemented at the application layer, using only end-systems. In an overlay or end-system multicast approach, participating peers organize themselves into an overlay topology for data delivery. Each edge in this topology corresponds to a unicast path between two end-systems or peers in the underlying internet. All multicast-related functionality is implemented at the peers instead of at routers, and the goal of the multicast protocol is to construct and maintain an efficient overlay for data transmission.

Disadvantages

- No knowledge of the real network topology, subject to the routing inefficiencies of the underlying network, may be routed on sub-optimal paths.
- Possible increased latency compared to non-overlay services.
- Duplicate packets at certain points.
- Additional encapsulation overhead, meaning lower total network capacity due to multiple payload encapsulation.

List of overlay network protocols

Overlay network protocols based on TCP/IP include:

- Distributed hash tables (DHTs) based on the Chord
- JXTA
- XMPP: the routing of messages based on an endpoint Jabber ID (Example: nodeId_or_userId@domainId\resourceId) instead of by an IP Address
- Many peer-to-peer protocols including Gnutella, Gnutella2, Freenet, I2P and Tor.
- PUCC
- Solipsis: a France Télécom system for massively shared virtual world

Overlay network protocols based on UDP/IP include:

- Distributed hash tables (DHTs) based on Kademlia algorithm, such as KAD, etc.
- Real Time Media Flow Protocol – Adobe Flash

See also

- Darknet
- Mesh network
- Computer network
- Peercasting
- Virtual Private Network

References

1. Sasu Tarkoma (2010). *Overlay Networks: Toward Information Networking* (https://archive.org/details/overlaynetworkst00tark_514) . CRC Press. p. 3 (https://archive.org/details/overlaynetworkst00tark_514/page/n16) . ISBN 9781439813737.
2. Peterson, Larry; Davie, Bruce (2012). "Chapter 9: Applications". *Computer Networks: A Systems Approach* (https://book.systemsapproach.org/index.html) . Elsevier. Retrieved 19 December 2022.

3. David Andersen, Hari Balakrishnan, Frans Kaashoek, Robert Morris (December 2001). "Resilient overlay networks" (http://portal.acm.org/citation.cfm?id=502048) . *Proceedings of the eighteenth ACM symposium on Operating systems principles*. Vol. 35. pp. 131–45. doi:10.1145/502034.502048 (https://doi.org/10.1145%2F502034.502048) . ISBN 978-1581133899. S2CID 221317942 (https://api.semanticscholar.org/CorpusID:221317942) .

4. Braun, Torsten; Arya, Vijay; Turletti, Thierry (2006-08-04). "Explicit routing in multicast overlay networks" (https://www.sciencedirect.com/science/article/pii/S0140366406001022) . *Computer Communications*. **29** (12): 2201–2216. doi:10.1016/j.comcom.2006.02.022 (https://doi.org/10.1016%2Fj.comcom.2006.02.022) . ISSN 0140-3664 (https://search.worldcat.org/issn/0140-3664) .

External links

- List of overlay network implementations, July 2003 (http://himalia.it.jyu.fi/ffdoc/storm/pegboard/available_overlays--hemppah/peg.gen.html)
- Resilient Overlay Networks (http://nms.csail.mit.edu/ron/)
- Overcast: reliable multicasting with an overlay network (https://www.cs.brown.edu/~jj/papers/overcast-osdi00.pdf)
- OverQoS: An overlay based architecture for enhancing Internet QoS (http://nms.lcs.mit.edu/papers/overqos-nsdi04.html)
- End System Multicast (https://web.archive.org/web/20050221110350/http://esm.cs.cmu.edu/)