Short Communication

iMedPub Journals
www.imedpub.com

International Journal of Innovative Research in Computer and Communication Engineering

2023
Vol.8 No.1:110

Traffic of Various User Communities Over a Secure Underlying Network

Shinzuke Twang*

Department of Science, Beijing University of Posts and Telecommunications, Beijing, China

***Corresponding author:** Shinzuke Twang, Department of Science, Beijing University of Posts and Telecommunications, Beijing, China; E-mail: twang.shin@gmail.com

Received date: October 28, 2022, Manuscript No. IJIRCCE-22-14837; **Editor assigned date:** October 31, 2022, PreQC No. IJIRCCE-22-14837 (PQ); **Reviewed date:** November 15, 2022, QC No. IJIRCCE-22-14837; **Revised date:** February 06, 2023, Manuscript No. IJIRCCE-22-14837 (R); **Published date:** February 13, 2023, DOI: 10.36648/IJIRCCE.8.1.110

Citation: Twang S (2023) Traffic of Various User Communities Over a Secure Underlying Network. Int J Inn Res Compu Commun Eng Vol:8 No:1

Abstract

An enterprise private network is a network that a single company creates to connect its office locations (such as production sites, head offices, remote offices and shops) in order for them to share computer resources. A Virtual Private Network (VPN) is an overlay network in which some of the connections between nodes are carried by open connections or virtual circuits in a larger network, such as the internet, rather than by actual wires. When this is the case, the virtual network's data link layer protocols are referred to as tunnelling through the larger network. Secure communications over the public Internet is one common use, but a VPN does not necessarily need to have explicit security features like content encryption or authentication. VPNs, for instance, can be used to separate the traffic of various user communities over a secure underlying network.

Keywords: Virtual Private Network (VPN); Service Level Agreement (SLA); Global Area Network (GAN); Technology; World Wide Web (WWW)

Introduction

Administrative control of an extranet

There may be a Service Level Agreement (SLA) between the VPN customer and the VPN service provider or best-effort performance for VPN. Point-to-point networks typically have simpler topologies than VPNs [1]. A Global Area Network (GAN) is a network that supports mobile devices across any number of wireless LANs, satellite coverage areas and other locations. Transferring user communications from one local coverage area to the next presents the most significant challenge in mobile communications. A series of terrestrial wireless LANs are involved in IEEE Project 802 in this regard. Most of the time, the companies that own networks run them intranets and extranets may be used in conjunction in private enterprise networks they might also offer network access to the Internet, which doesn't have a single owner and lets people connect to the rest of the world almost indefinitely [2]. An intranet is a collection of networks that are managed by a single administrative body. The IP protocol and IP-based tools like web browsers and file transfer applications are used in the intranet. The intranet is only accessible to authorized users by the administrative entity.

Description

An organization's internal LAN is typically referred to as an intranet. At least one web server is typically present in a large intranet to provide users with organizational data. On a local area network, anything behind the router is also considered an intranet [3]. Extranet an extranet is a network that supports a limited connection to a specific external network but is also under the administrative control of a single organization. In order to share data with its customers or business partners, an organization might, for instance, grant access to specific parts of its intranet [4]. From a security standpoint, these other entities are not always trusted. WAN technology is frequently, but not always, used to connect a network to an extranet. By layering on top of the various networking software and connecting them together using routers, multiple distinct types of computer networks are connected to form a single computer network in an internetwork. The largest example of internetwork is the Internet. It is a global network of computer networks that connect public, private, academic, corporate, and government institutions. The World Wide Web (WWW), the Internet of Things, video transfer, and a plethora of information services are all made possible by the Internet's optical networking backbone and copper communications.

Average rate of successful data transfer

Several hundred documented and frequently standardized protocols that are compatible with the internet protocol suite, an addressing system (IP addresses) managed by the internet assigned numbers authority and address registries are used by Internet users in a variety of ways [5]. Through the Border Gateway Protocol (BGP), large businesses and service providers exchange information about the reachability of their address spaces, resulting in a redundant global transmission path mesh. A dark net is an overlay network that can only be accessed through specialized software and typically runs on the internet. A dark net is an anonymous network that uses non-standard protocols and ports to connect only trusted peers, also known as Friends (F2F). Dark nets are distinct from other distributed peer-

to-peer networks because users can communicate without fear of government or corporate interference because sharing is anonymous (IP addresses are not shared publicly). Applications that are hosted by servers on a computer network provide members or users of the network with some functionality or aid in the operation of the network itself. Examples of well-known network services include e-mail, network file sharing, the world wide web and printing. Network services like DNS (Domain Name System), which gives IP and MAC addresses names and DHCP, which ensures that network equipment has a valid IP address, are typically based on a service protocol, which specifies the format and order in which messages are sent between the network service's clients and servers. A communication path's average rate of successful data transfer can be referred to as good put or achieved throughput, when measured in bits per second. Technologies like bandwidth shaping, bandwidth management, bandwidth throttling, bandwidth cap and bandwidth allocation (such as the bandwidth allocation protocol and dynamic bandwidth allocation), among others, have an impact on throughput [6]. The average consumed signal bandwidth in hertz, or the spectral bandwidth of the analog signal that represents the bit stream, is proportional to the bandwidth of a bit stream over a given time period. A link or node's quality of service deteriorates when it is subjected to a greater data load than it is rated for, resulting in network congestion. Networks rely on re-transmission because packets must be discarded when networks become congested and queues become overcrowded. Queueing delays, packet loss and the blocking of new connections are all typical outcomes of congestion.

Conclusion

The fact that incremental increases in offered load either result in a modest increase or a decrease in network throughput is a consequence of these last two. Even after the initial load is reduced to a level that would not normally cause network congestion, network protocols that use aggressive retransmissions to compensate for packet loss tend to keep systems in a state of network congestion. As a result, these protocols based networks can exhibit two stablestates at the same load. Congestive collapse is the stable state with low throughput. To avoid congestion collapse (endpoints typically slow down or even stop transmission when the network is congested), modern networks employ congestion control, congestion avoidance, and traffic control techniques. Among these strategies are: Window reduction in TCP, exponential back off in protocols like 802.11's CSMA/CA and the original ethernet and fair queuing in devices like routers. Implementing priority schemes so that some packets are transmitted with higher priority than others is another way to avoid the negative effects of network congestion. Priority schemes can't solve network congestion on their own, but they can help alleviate some services' congestion. 802.1p is one example of this. The explicit allocation of network resources to specific flows is a third strategy for avoiding network congestion. The use of Contention Free Transmission Opportunities (CFTXOPs) in the ITU-T G.hn standard is one illustration of this. These opportunities enable high speed local area networking over existing home wires (such as power lines, phone lines and coaxial cables) at speeds of up to 1 Gbit/s.

References

1. Leiner BM, Cerf VG, Clark DD, Kahn RE, Kleinrock L, et al. (2009) A brief history of the Internet. ACM SIGCOMM Comput Commun Rev 39:22-31
2. Kumar JS, Patel DR (2014) A survey on internet of things: Security and privacy issues. Int J Comput Appl 90:20-26
3. Kumar R, Mukherjee A, Singh VP (2017) Traffic noise mapping of Indian roads through smartphone user community participation. Environ Monit Assess 189:1-4
4. Choi M, Glassman M, Cristol D (2017) What it means to be a citizen in the internet age: Development of a reliable and valid digital citizenship scale. Comput Educ 107:100-112
5. Caviglione L, Davoli F (2008) Traffic volume analysis of a nation-wide eMule community. Comput Comm 31:2485-2495
6. Hienerth C, Lettl C, Keinz P (2014) Synergies among producer firms, lead users and user communities: The case of the LEGO producer–user ecosystem. J Prod Innov Manage 31:848-866