Application of Network Analysis in Network Operations and Maintenance: Postprint

Authors: Liu Chenguang

Date: 2023-10-08T00:00:00+00:00

Abstract

Network analysis constitutes the comprehensive monitoring and analysis of network data, encompassing the decoding, detection, analysis, and diagnosis of data packets transmitted within the network. It aims to eliminate network failures and issues arising from various network application behaviors, accurately and expeditiously locate network anomalies, mitigate network security risks, enhance network performance, and improve network availability. This paper presents a detailed exposition on the positioning of network analysis, data filtering methodologies, statistical techniques, and analytical approaches, as well as the application of network analysis to performance evaluation, network resource management and decision-making, and the identification of security threats within the network. Furthermore, it elucidates the pivotal role of network analysis in practical applications through illustrative examples.

Full Text

Preamble

Title: Application of Network Analysis in Network Operations and Maintenance

Abstract: Network analysis involves comprehensive monitoring and analysis of network data, including decoding, detecting, analyzing, and diagnosing data packets transmitted across the network to troubleshoot faults and issues caused by various network application behaviors. It enables rapid and accurate localization of network problems, mitigates security risks, enhances network performance, and improves network availability. This paper elaborates on the positioning of network analysis, data filtering techniques, statistical methods, and analytical approaches, and details how network analysis can be used for performance evaluation, network resource management, decision-making, and

identifying security threats, demonstrating its critical role in practice through real-world examples.

Keywords: network analysis; network faults; network security; statistical analysis

Classification: TP311

Document Code: A

Article ID: 1671-0134(2018)10-061-02

DOI: 10.19483/j.cnki.11-4653/n.2018.10.020

Author: Liu Chenguang

3. Network Analysis for Troubleshooting

Networks form the foundation of information infrastructure and serve as the highways for network services; their stability and connectivity directly determine the development of network-based business. As network penetration continues to increase, human activities have become increasingly dependent on network connectivity. With constantly evolving applications, large-scale deployments, and complex architectures, network faults have grown more complicated, and the time available for troubleshooting has become increasingly constrained. Rapid fault localization and network traceability have become essential responsibilities for network operations personnel.

While common connectivity issues can be diagnosed using simple commands such as ping and tracert, complex scenarios—including intermittent network failures, sporadic application connectivity problems, and degraded network performance—require sophisticated network analysis. These issues may stem from various sources, including LAN device malfunctions, WAN link problems, application server or client host issues, or defects in the application software itself. In production networks with numerous deployed devices such as switches, routers, firewalls, VPNs, load balancers, and various terminals and servers, any application fault can significantly impact business operations. Network analysis addresses these challenges through comprehensive monitoring and analysis of network data, decoding, detecting, analyzing, and diagnosing transmitted packets to eliminate faults caused by various network application behaviors, enabling accurate and rapid problem localization, mitigating security risks, enhancing performance, and improving network availability.

The positioning of packet capture points is critical for effective analysis and depends on the network topology, data sources, destination servers, and routing paths. In one case involving slow DNS resolution and partial domain name resolution failures, we adopted a systematic approach. First, capturing packets at the client side confirmed that certain DNS queries received no responses. Next, captures at the DNS server revealed that all received resolution requests were being processed and responded to correctly. Finally, by using port mirroring on

intermediate network devices and comparing packets at a firewall' s internal and external interfaces, we discovered discrepancies in packet counts, indicating that some packets were being dropped by the firewall. Further analysis showed that the firewall was discarding large DNS packets due to its small MTU configuration. The issue was resolved by either minimizing DNS packet sizes or adjusting the firewall' s MTU, demonstrating how strategic placement of multiple monitoring points enables systematic fault isolation based on network topology and abnormal data flow patterns.

Given the massive volume of network traffic, effective data filtering is essential to reduce analysis workload. Filtering can be performed during capture when fault characteristics are well understood. In the DNS packet drop case, for instance, we could filter for packets with specific source and destination addresses using the DNS protocol. Alternatively, post-capture filtering can be applied when using bypass logging or analysis systems. Typical filtering criteria include source and destination addresses, network interfaces, protocols, service ports, and switch ports, enabling analysts to focus on relevant data and expedite the troubleshooting process.

Comparison-based fault localization involves analyzing differences between normal and faulty traffic patterns. When users reported intermittent failures in client-server mode application logins, we captured traffic during both successful and failed authentication attempts. By comparing the packet sizes of successful versus failed login transmissions, we identified an application design flaw as the root cause. This method is particularly effective for identifying subtle changes in application behavior that may not be apparent through other diagnostic techniques.

Flow diagram analysis provides visual insights into network behavior and timing issues. In a case where users in Building A experienced normal speeds while Building B users reported slowness, initial bandwidth tests showed identical network rates between locations. However, by capturing a complete data interaction process at the client side and creating a flow diagram of all exchanges and their timing, we discovered that Building B had a consistent 10-second delay waiting for an Internet domain name request to timeout. Building A terminals, lacking DNS server configuration, proceeded directly to the next step, revealing the cause of the performance discrepancy.

Statistical analysis represents the most complex yet frequently employed method for fault localization. When users across the same network segment reported slow internet access, statistical analysis of the switch' s total and directional traffic revealed bandwidth utilization around 80%, with instantaneous peaks causing significant packet loss and excessive broadcast traffic. This pattern indicated a broadcast or routing loop fault. Statistical analysis can be performed across multiple dimensions: protocol statistics reveal the proportion of each protocol type; conversation statistics analyze traffic between specific endpoints; HTTP traffic statistics assess website access patterns. Advanced network statistical tools provide deeper insights into network behavior and facilitate rapid

identification of anomalies.

Network analysis tools such as Wireshark, Sniffer, NetFlow, Jflow, Sflow, Syslog, xlog, httpwatch, tcpdump, and OmniPeek are all valuable when applied appropriately. The effectiveness of network analysis ultimately depends on the knowledge, experience, and analytical capabilities of network technicians who must interpret captured data and apply appropriate methodologies to resolve complex issues.

[1] (Israel) Yoram Orzach, translated by Gu Hongxia and Sun Yuqiang. Wireshark Network Analysis in Practice [J]. People' s Posts and Telecommunications Press.

[2] (USA) Kevin R. Fall, W. Richard Stevens, translated by Wu Ying, Zhang Yu, and Xu Yuwei. TCP/IP Illustrated, Volume 1: The Protocols [J]. China Machine Press.

[3] Yang Ping, Tian Jianchun. Research on Key Technologies of Wireshark for Network Security Risk Assessment [J]. Network Security Technology and Application, 2015(09).

[4] Yang Rong, Zhang Guoqing, Wei Wei, Li Yangyao. Network Attack Behavior Discovery Based on NetFlow Traffic Analysis [J]. Computer Engineering, 2005, 31(13).

[5] Shuai Liang. HTTP Traffic Characteristic Analysis and Generation [J]. Institute of Computing Technology, Chinese Academy of Sciences, 2009.

[6] Wei Ping. OmniPeek Network Protocol Analysis Based on Port Mirroring [J]. Computer Knowledge and Technology, 2009, 5(04).

4. Network Analysis for Performance Bottlenecks

Application transmission performance is affected by parameters including bandwidth, latency, jitter, and packet loss. Identifying bottleneck factors enables performance optimization. In one international network operations scenario, users reported significant slowdowns when backup lines were activated and requested increased bandwidth. However, network statistical analysis revealed that the backup line' s bandwidth was not saturated and had substantial remaining capacity. By capturing and analyzing TCP protocol interactions at both client and server ends, we found that most delays occurred while the server waited for client ACK acknowledgments, though clients were responding promptly. The root cause was the backup line' s latency, which was approximately double that of the primary line due to its circuitous routing. In such cases, simply increasing bandwidth cannot resolve the issue. However, using concurrent connection applications or modifying the operating system' s TCP window size can significantly improve performance under current link conditions.

5. Resource Statistics, Management, and Decision-making

By capturing raw network traffic data over extended periods and analyzing network behavior patterns and operational trends, organizations can establish a scientific basis for decisions regarding network performance optimization, new service deployment, bandwidth planning, and security policy formulation. This data-driven approach enables proactive network management and capacity planning, ensuring that infrastructure investments align with actual usage patterns and business requirements.

6. Network Security Analysis

Through behavioral analysis of data packets and deep network communication inspection, network analysis can rapidly detect security threats including network attacks, unauthorized external connections, Trojan communications, covert channels, abnormal DNS resolution, and policy violations. Effective identification of malicious traffic attacks requires establishing baseline knowledge of normal network traffic characteristics. Once network administrators thoroughly understand normal traffic patterns for protocols such as ARP, TCP, DNS, and typical IP addresses and port numbers, they can quickly detect anomalous flows. In one incident, widespread user reports of network slowness and lag led to packet capture analysis, which revealed several IP addresses attempting to establish connections with all hosts on the LAN using consistent port numbers at short intervals, consuming significant bandwidth. These packets originated from the same network segment, strongly indicating worm-infected hosts scanning the network. Similar analysis can identify issues such as TCP SYN scanning and DoS attacks through abnormal traffic patterns.

(Author' s Affiliation: Xinhua News Agency Technical Bureau)

Note: Figure translations are in progress. See original paper for figures.