Network Optimization

Navigating Network Complexities

Network Critical

The Window to your Network™

Contents

Introduction

As digital transformation continues to accelerate, network optimization has become an increasingly critical aspect of IT infrastructure. With the rise of cloud computing, big data analytics, and the Internet of Things (IoT), networks are being pushed to their limits. As a result, businesses are seeking innovative solutions to optimize networks to stay ahead of the competition.

At Network Critical, we specialize in providing cutting-edge network visibility solutions that help businesses optimize their network performance. Our solutions include a wide range of NPBs, and TAPs that can be customized to meet the unique needs of your organization.

By leveraging our expertise and innovative solutions, you can gain complete visibility into your network traffic, optimize network performance, and reduce the risk of downtime. Our solutions are easy to deploy, scalable, and reliable, ensuring that your critical applications and services remain available and responsive.

In the following pages, we will explore the challenges of network optimization and provide practical strategies for improving network performance. We will discuss the benefits of using NPBs and show how Network Critical's solutions can help you optimize your network and enhance your organization's IT infrastructure.

What is Network Optimization?

Network optimization is the process of improving the performance, efficiency, and reliability of a network by adjusting various network parameters, such as routing algorithms, traffic flow, network topology, and resource allocation. The goal of network optimization is to ensure that the network can meet the requirements of users and applications while minimizing costs and maximizing the use of network resources.

Network optimization involves the use of various techniques, including mathematical optimization, simulation, and modeling, to analyze network behavior and identify areas for improvement. Common optimization techniques include linear programming, integer programming, convex optimization, and stochastic optimization. These techniques can be used to optimize different aspects of the network, such as bandwidth utilization, network latency, throughput, packet loss, and QoS (Quality of Service).

Network optimization is crucial for modern networks, especially for large-scale networks such as the internet, which must handle vast amounts of data traffic and support a diverse range of applications and services. Effective network optimization can improve network performance, reduce downtime, and enhance user satisfaction, leading to significant cost savings and competitive advantages for businesses and organizations.

What to consider when improving network performance?

There are several key metrics that impact network performance and need to be optimized in order to improve the overall network efficiency and reliability. These metrics include:

- **Bandwidth:** The amount of data that can be transmitted over a network in a given period of time. Optimizing bandwidth involves ensuring that network resources are allocated efficiently and that bandwidth is used effectively to support different types of traffic.
- **Latency:** The time it takes for data to travel from one point in the network to another. Optimizing latency involves reducing delays and improving response times to enhance the user experience and support time-sensitive applications.
- **Packet loss:** The percentage of packets that are lost or discarded during transmission. Optimizing packet loss involves minimizing network congestion and ensuring that packets are delivered reliably to their destination.
- **Jitter:** The variation in packet delay, which can cause problems for real-time applications such as voice and video. Optimizing jitter involves minimizing variations in delay and ensuring that packets are delivered in a timely and consistent manner.
- **Throughput:** The rate at which data is transmitted over the network. Optimizing throughput involves maximizing the amount of data that can be transmitted while ensuring that the network remains stable and reliable.

Other important metrics that impact network performance include **QoS (Quality of Service), network availability, network security, and scalability.** By optimizing these metrics, network administrators can ensure that their network is performing at its best and delivering the best possible experience for users and applications.

Improving Network Performance

What is Quality of Service?

Quality of Service (QoS) refers to the ability of a network to provide predictable and reliable service to different types of traffic, such as voice, video, and data. QoS ensures that critical traffic is prioritized over non-critical traffic, and that network resources are allocated efficiently to support the different types of traffic.

Improving QoS can lead to better network performance by ensuring that critical traffic is delivered reliably and with low latency. Here are some ways to improve QoS:

- **Traffic classification:** Different types of traffic should be classified and marked with appropriate QoS tags, such as Differentiated Services Code Point (DSCP) or Class of Service (CoS), to ensure that network devices can identify and prioritize the traffic correctly.
- **Traffic prioritization:** Once traffic has been classified, it can be prioritized based on its importance. For example, voice and video traffic should be prioritized over data traffic to ensure that they are delivered with low latency and high reliability.
- **Traffic shaping:** Traffic shaping can be used to control the flow of traffic and prevent congestion. This involves limiting the rate of traffic on certain network segments to ensure that bandwidth is used efficiently.
- **Resource allocation:** Network resources, such as bandwidth and buffer space, should be allocated based on the QoS requirements of different types of traffic. This ensures that critical traffic receives the necessary resources to ensure reliable delivery.
- **Network monitoring:** Network administrators should monitor network performance and QoS metrics, such as latency, packet loss, and jitter, to identify and resolve issues before they affect network performance.

Network Availability

It refers to the ability of a network to be accessible and functional for users, without any downtime or disruptions. High network availability is essential for ensuring that users can access network resources and services when they need them, and that the network can support critical business operations.

Improving network availability can be a complex task, but here are some general tips to consider:

- **Redundancy:** Having redundant network components, such as multiple routers or switches, can help ensure that network availability is maintained even if one component fails.
- **Monitoring:** Monitoring the network for issues or abnormalities can help identify potential problems before they escalate into serious outages.
- **Load balancing:** Distributing network traffic across multiple network devices can help prevent any one device from becoming overwhelmed and causing a network outage.
- **Regular maintenance:** Performing regular maintenance tasks, such as updating firmware and software, can help prevent issues from arising in the first place.
- **Failover:** Implementing a failover mechanism, where traffic is automatically rerouted to another path or device in the event of a failure, can help ensure that network availability is maintained.
- **Backup power:** Having backup power supplies, such as uninterruptible power supplies (UPS), can help ensure that network devices continue to operate even during power outages.
- **Proper network design:** A well-designed network architecture can help prevent issues such as bottlenecks and congestion that can lead to network downtime.

How Network Security helps improve performance?

Network Security refers to the measures that are put in place to protect a network from unauthorized access, attacks, and data breaches. The goal of network security is to ensure that the network and its data are safe and secure, and that confidential information is not compromised.

Having better network security can help optimize your network in a number of ways:

- **Protection against attacks:** Network security measures such as firewalls, intrusion detection and prevention systems (IDPS), and antivirus software can help protect the network against cyber attacks. This can prevent data loss, damage to the network infrastructure, and downtime, all of which can impact network performance.
- **Improved availability:** Network security measures can also help improve network availability by preventing unauthorized access to the network and its resources. This can prevent denial of service (DoS) attacks and other types of cyber attacks that can cause network downtime and disrupt business operations.
- **Regulatory compliance:** Many organizations are subject to regulatory requirements that mandate the implementation of certain network security measures. By complying with these requirements, organizations can avoid legal penalties and fines, as well as reputational damage that can negatively impact their business.
- **Reduced risks:** Implementing strong network security measures can help reduce the risks associated with cyber attacks and data breaches, which can have significant financial and operational impacts on organizations. This can help optimize the network by minimizing the risks of network-related incidents that can impact performance.

Having better network security can help optimize your network by protecting it from cyber threats, improving availability, ensuring regulatory compliance, and reducing risks. By implementing robust network security measures, organizations can ensure that their network is safe, secure, and performing optimally.

Network Scalability

Network scalability is the ability of a network to accommodate increasing numbers of users, devices, and traffic without experiencing performance issues or downtime. A scalable network is one that can grow and adapt to changing needs, while maintaining its performance, reliability, and security.

Network scalability is an important factor in network optimization, as it can impact the overall performance and efficiency of the network. A network that is not scalable may struggle to accommodate growing demands, leading to slow performance, downtime, and other issues that can negatively impact business operations.

To improve network scalability, network administrators can implement a range of strategies, including:

- **Adding capacity:** Adding more resources to the network infrastructure, such as servers, storage, and bandwidth, can help improve network scalability and accommodate growing demands.
- **Virtualization:** Network virtualization can help improve scalability by allowing multiple virtual networks to share the same physical infrastructure, enabling more efficient use of resources and easier management.
- **Load balancing:** Load balancing can help distribute network traffic evenly across multiple servers, preventing overloading and improving scalability.

Improving network scalability can help optimize the network by ensuring that it can accommodate growing demands and changing business needs, while maintaining its performance, reliability, and security.

What is Network Efficiency?

Network efficiency refers to how effectively a network is able to transfer data between devices while minimizing delays, errors, and other issues. A network that is efficient can transfer data quickly and reliably, with minimal data loss or corruption. Efficient networks are also able to handle increasing amounts of traffic without becoming overwhelmed or causing congestion.

There are many factors that can affect network efficiency, including network topology, hardware and software components, network protocols, and network traffic patterns. To improve network efficiency, it's important to analyze these factors and implement strategies to optimize network performance.

Here are some tips on how to improve network efficiency:

1. **Reduce network congestion:** Network congestion can occur when too much data is trying to travel over the same network infrastructure. To reduce congestion, you can segment your network and distribute traffic across multiple network devices.
2. **Optimize network protocols:** Choosing the right network protocols can help improve network efficiency. For example, the Transmission Control Protocol (TCP) can be optimized to reduce packet loss and improve throughput.
3. **Upgrade network hardware:** Upgrading network hardware such as switches, routers, and wireless access points can help improve network efficiency. Newer hardware can support faster data transfer speeds and more advanced features such as Quality of Service (QoS) and traffic prioritization.
4. **Implement Quality of Service (QoS):** As mentioned before, QoS is a set of technologies that allows you to prioritize certain types of network traffic over others. By prioritizing critical traffic such as voice and video, you can improve network efficiency and ensure that these applications receive the bandwidth they need to function properly.
5. **Monitor network performance:** Regularly monitoring network performance can help identify potential issues and improve network efficiency. Tools such as network analyzers and bandwidth monitors can help you identify bottlenecks, analyze traffic patterns, and troubleshoot network issues.
6. **Use caching and compression:** Caching frequently accessed data and compressing data can help reduce the amount of data that needs to be transferred over the network, which can improve network efficiency.
7. **Optimize network design:** A well-designed network architecture can help improve network efficiency. Proper network design can help minimize bottlenecks, reduce latency, and ensure that network devices are deployed in a way that maximizes their efficiency.

Network Reliability

Network reliability is the ability of a network to consistently and accurately transfer data between devices over a period of time. A reliable network should be available and functioning as expected whenever it is needed, without any unexpected downtime or data loss. In other words, it is the ability of a network to consistently provide a high level of performance without interruptions.

A reliable network is essential for organizations to carry out their day-to-day operations, and it is especially important for mission-critical applications and services that cannot tolerate any downtime. By ensuring that their networks are reliable, organizations can avoid costly disruptions and maintain their competitive edge.

Improving network reliability involves taking steps to ensure that the network consistently functions as expected, without unexpected downtime or data loss.

Here are some strategies to improve network reliability:

1. **Implement redundancy:** Redundancy means having multiple components, such as routers or switches, that can take over if one component fails. This ensures that the network remains available and functional even if one component fails.
2. **Use high-quality network hardware:** Using high-quality network hardware can help ensure that the network is reliable and performs at a high level. Cheap or outdated hardware may not be able to handle the demands of a modern network, leading to performance issues and downtime.
3. **Regularly maintain and update network equipment:** Regularly updating network equipment such as routers, switches, and firewalls with the latest firmware and security patches can help ensure that the network is reliable and secure.
4. **Monitor network performance:** Monitoring network performance can help identify potential issues before they become serious problems. Network monitoring tools can alert IT staff to performance issues and provide data that can be used to optimize the network for better reliability.
5. **Implement a disaster recovery plan:** A disaster recovery plan outlines how an organization will respond in the event of a major network failure or outage. By having a plan in place, organizations can minimize downtime and quickly restore network operations in the event of an emergency.
6. **Train IT staff:** Well-trained IT staff can quickly identify and respond to network issues, minimizing the impact of downtime or other problems.

How We Can Help

Network Critical is a leading provider of network visibility and monitoring solutions for organizations. We offer cutting-edge products and services designed to optimize network performance, improve security, and reduce downtime. Our solutions enable organizations to gain unprecedented visibility into their network traffic and quickly identify potential issues before they impact users. With Network Critical, you can ensure that your network remains secure, reliable, and always available, allowing you to operate at maximum efficiency and productivity. We are committed to providing our clients with innovative and effective solutions that meet their unique needs and help them stay ahead of the competition.

Network Visibility

Network Critical's TAPs provide network visibility, which is essential for optimizing network performance. With real-time insights into network traffic, organizations can quickly identify and address issues, reducing downtime and improving network efficiency.

Network Monitoring

Network Critical's solutions offer comprehensive network monitoring capabilities, including packet capture and analysis, that allow organizations to monitor their network's performance and identify bottlenecks or potential issues.

Network Security

Network Critical's solutions offer advanced security features, such as intrusion detection and prevention, that help organizations protect their networks from potential threats and attacks, ensuring network uptime and availability.

Traffic Management

Network Critical's Packet Brokers can help organizations manage network traffic by directing data flows to the appropriate tools and applications, reducing network congestion and improving overall performance.

Network TAPs

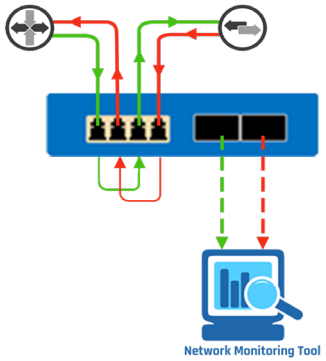
A **network TAP (Test Access Point)** is a hardware device that is used to monitor network traffic. It provides access to the data flowing through a network without interfering with the normal operation of the network.

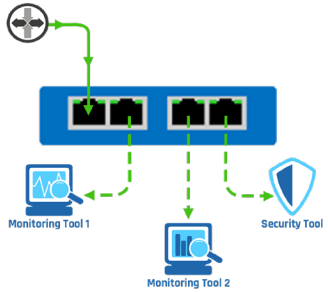
A TAP works by creating a copy of the network traffic passing through a particular link or port. The TAP device then forwards that copy to a monitoring device, such as a network analyzer or intrusion detection system, for analysis.

Network TAPs are commonly used for network monitoring, troubleshooting, and security analysis. They provide a non-intrusive and reliable way to monitor network traffic without affecting network performance or integrity.

TAP Modes

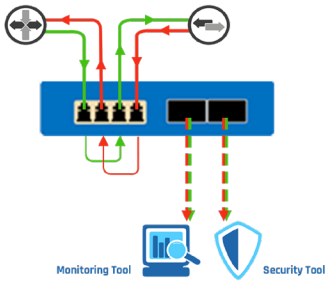
- **Breakout** – A breakout TAP operates like the diagram. The directional traffic is broken out between two output (monitor) ports. This allows each direction of traffic to be sent to a discreet monitor port at full wire speed. For example, if each direction is operating at a full 1Gbps, the total duplex traffic is 2Gbps. So, not to oversubscribe the monitor port, this method uses two 1Gbps output ports to connect to the analysis appliance eliminating any chance of dropped packets.

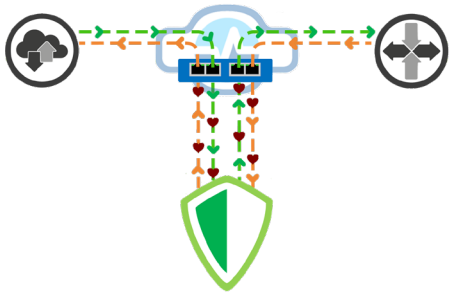




- **Regeneration** – As mentioned above, there are often requirements for specialized analysis using a variety of appliances. Regeneration mode allows the same data stream to be sent to two or more monitor ports.

- **Aggregation** – Providing access for applications with lower throughput, TAPs can aggregate both directions of the traffic and send the frames to a single monitor port. This mode can reduce port costs on probes and other analysis appliances by making efficient utilization of expensive analyzer ports. Aggregation can provide appliance savings, depending on link throughput, up to 8:1. This is accomplished by aggregating multiple 1G ports to a single 10G output. Aggregation can also be used to consolidate traffic from low-utilization 1G ports to an available 1G output port.





- **In-Line or Virtual-In-Line (V-Line)** – This is sometimes called Bypass tapping. In this mode, the live network traffic passes through the analysis device in real-time and then back to the TAP. This is used primarily in security analysis appliances such as IPS and DLP. This allows the appliance to see and act on live data as it passes through the network. In this mode, the TAP continuously monitors the analysis appliance for a heartbeat and bypasses the appliance if the appliance goes down. This Bypass feature allows these in-line appliances to be connected without the risk of taking down the network as a result of a software glitch or power loss to the appliance.

Benefits of using Network TAPs to optimize your network:

1. **Accurate network visibility:** Network TAPs provide an accurate and complete view of network traffic, including packet payloads and protocol details. This visibility allows network administrators to detect and resolve network issues more quickly and accurately than with other monitoring solutions.

2. **Non-intrusive monitoring:** Network TAPs do not affect network performance because they do not introduce any latency or packet loss. This non-intrusive monitoring ensures that network performance remains optimal during monitoring activities.

3. **Real-time monitoring:** Network TAPs provide real-time monitoring capabilities, which enables network administrators to detect and resolve issues as they occur. This proactive approach to monitoring reduces downtime and ensures that network performance remains optimized.

4. **Flexible deployment:** Network TAPs can be deployed at any point in the network, providing visibility into traffic flows between any two points. This flexibility allows network administrators to optimize network performance and detect issues at any location in the network.

5. **Increased network security:** Network TAPs provide complete visibility into network traffic, which enables network administrators to detect and prevent security threats, such as unauthorized access attempts, malware, and viruses. This increased security reduces the risk of data breaches and protects the network from cyber threats.

6. **Improved compliance:** Network TAPs can help organizations meet compliance requirements, such as those specified by HIPAA, PCI DSS, and other regulations. Network TAPs provide the necessary visibility into network traffic to ensure that data is protected and stored securely.

Network TAPs provide a powerful tool for optimizing network performance, improving security, and reducing downtime. With accurate and non-intrusive monitoring capabilities, network administrators can ensure that their networks remain secure, reliable, and efficient.

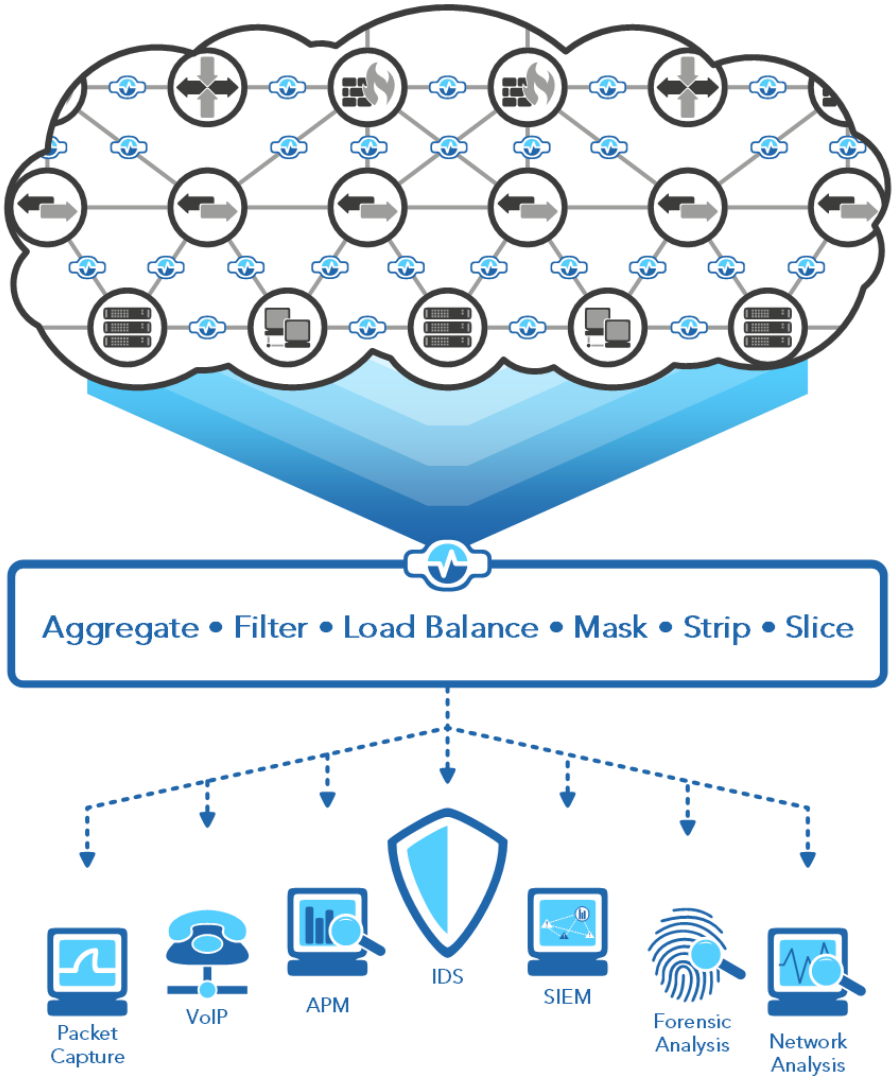
Packet Brokers

A **Network Packet Broker** (NPB) is a network device that is designed to optimize network traffic by aggregating, filtering, and directing data packets to the appropriate destinations. NPBs are used to improve network performance, increase security, and enhance the monitoring and analysis of network traffic.

NPBs are typically deployed in high-speed data center environments where network traffic is extremely high and complex. They allow network administrators to efficiently manage and optimize the flow of data packets across the network, reducing network congestion and improving network performance.

NPBs can perform a variety of key functions, including:

- **Packet aggregation.** NPBs can aggregate packets from multiple network sources and direct them to one or more destinations.
- **Packet filtering.** NPBs can filter packets based on various criteria, such as protocol, source IP address, destination IP address, and port number. This filtering enables network administrators to selectively route traffic to specific destinations or monitoring tools.
- **Load balancing.** NPBs can distribute traffic across multiple network links or devices, such as servers or storage devices. This load balancing improves resource utilization, reduces downtime, and optimizes network performance.
- **Packet Slicing** is when the frame headers are kept, and the payloads dropped. This feature is used to prevent tool overload and reduce bandwidth usage, by removing payloads that are not relevant to the network monitoring and security analysis.
- **Packet Masking** is used to conceal sensitive data in order to comply with data protection and security regulations. Enabling complete visibility into decrypted traffic without the risk of exposing sensitive data.
- **GRE Encapsulation / De-tunneling.** The NPB provides access to traffic encapsulated for a variety of tunneling protocols, such as Encapsulated Remote SPAN (ERSPAN), Generic Routing Encapsulation (GRE), and Virtual Extensible LAN (VXLAN). These cutting-edge de-tunneling features reduce blind spots caused by multiple traffic flow on the network anywhere within the IT infrastructure, whether physically or virtually.



Benefits of using Packet Brokers to optimize your network:

1. **Improved network performance:** NPBs can help optimize network performance by aggregating, filtering, and directing data packets to the appropriate destinations. This improves resource utilization, reduces network congestion, and ensures that critical traffic is prioritized.

2. **Increased network visibility:** NPBs provide a complete view of network traffic, enabling network administrators to detect and resolve issues more quickly and accurately than with other monitoring solutions. This increased visibility also allows network administrators to optimize network configurations to improve performance.

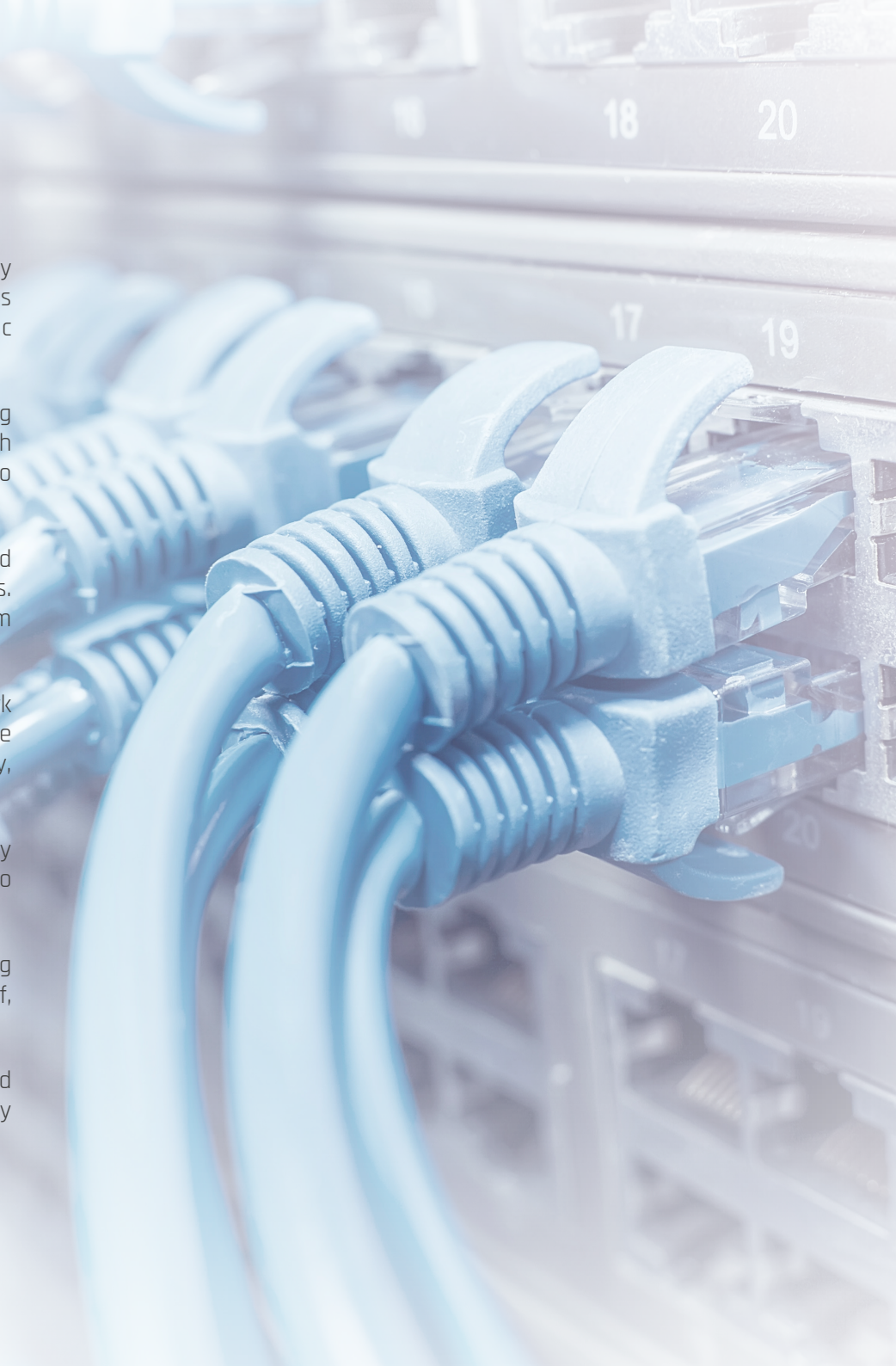
3. **Enhanced network security:** NPBs can be used for security purposes, such as detecting and preventing security threats, including malware, viruses, and unauthorized access attempts. This increased security reduces the risk of data breaches and protects the network from cyber threats.

4. **Reduced network downtime:** NPBs help reduce network downtime by optimizing network performance, improving network visibility, and enhancing network security. This proactive approach to network management ensures that issues are detected and resolved quickly, reducing the risk of downtime.

5. **Flexible deployment:** NPBs can be deployed at any point in the network, providing visibility into traffic flows between any two points. This flexibility allows network administrators to optimize network performance and detect issues at any location in the network.

6. **Cost savings:** NPBs can help reduce costs by improving resource utilization and reducing network downtime. This reduces the need for additional network hardware and IT staff, resulting in cost savings for the organization.

NPBs provide a powerful tool for optimizing network performance, improving security, and reducing downtime. With their ability to manage and direct network traffic efficiently, NPBs play an important role in modern high-speed network environments.



Conclusion

Network optimization is an essential aspect of modern business operations. With the increasing reliance on digital technologies, organizations must ensure that their networks are optimized for efficiency, reliability, and security.

Through this white paper, we have explored the various challenges faced by organizations when it comes to network optimization and the solutions that can help overcome them. We have highlighted the benefits of network optimization and how it can lead to enhanced user experience, improved security, and increased ROI.

At Network Critical, we understand the importance of network optimization and provide solutions that can help organizations achieve their network performance goals. Our range of solutions offers network visibility, monitoring, and security that are essential for optimizing network performance.

With our Network TAPs, Packet Brokers, and Bypass TAPs, we provide organizations with the necessary tools to improve network performance, reduce downtime, and ensure uninterrupted data flow. Our solutions are designed to provide real-time insights into network traffic, allowing organizations to identify and address issues quickly.

We hope that this white paper has provided valuable insights into network optimization and the solutions available to organizations. By choosing Network Critical's solutions, organizations can optimize their networks for efficient, reliable, and secure operations, leading to improved business outcomes.

CONTACT US

Head Office, UK +44 (0) 118 954 3210

US Office, GA +1 (470) 554 7170

or

sales@networkcritical.com