APPOSITE
TECHNOLOGIES

SOLUTION BRIEF

Service Provider and Broadband Testing

INTRODUCTION

Put broadband access networks to the test to deliver the high-speed, high-quality services modern customers demand. Confidently launch new premium streaming, conferencing, managed IT and cybersecurity services tailored to the needs of local businesses and remote workers. And conduct automated, repeatable and affordable lifecycle testing to demonstrate performance to secure and maintain government funded grants.

Apposite's simple-to-use traffic generation and network emulation appliances let you emulate residential and business subscribers and simulate high-speed network conditions — at scale — without investing millions in test labs and specialized skills.

CHALLENGES

Testing device and system performance end-to-end: Service providers must ensure that every component of their network operates effectively. This comprehensive approach involves evaluating not just individual devices, but also the complete network path from the end-user device through the entire network infrastructure.

Maintaining quality and accountability as you scale: As service providers expand their networks and customer base, maintaining quality and accountability becomes increasingly challenging. Performance testing helps ensure that network upgrades and expansions do not compromise service quality.

Avoiding outages and preventing customer issues: Regular testing helps deliver a stable, reliable network and prevents costly downtime. By simulating various network conditions and traffic scenarios, service providers can pinpoint vulnerabilities and performance bottlenecks that could lead to service disruptions before they impact users.

Apposite Test Capabilities

Conduct end-to-end broadband access testing

Simulate Internet servers and 100G links

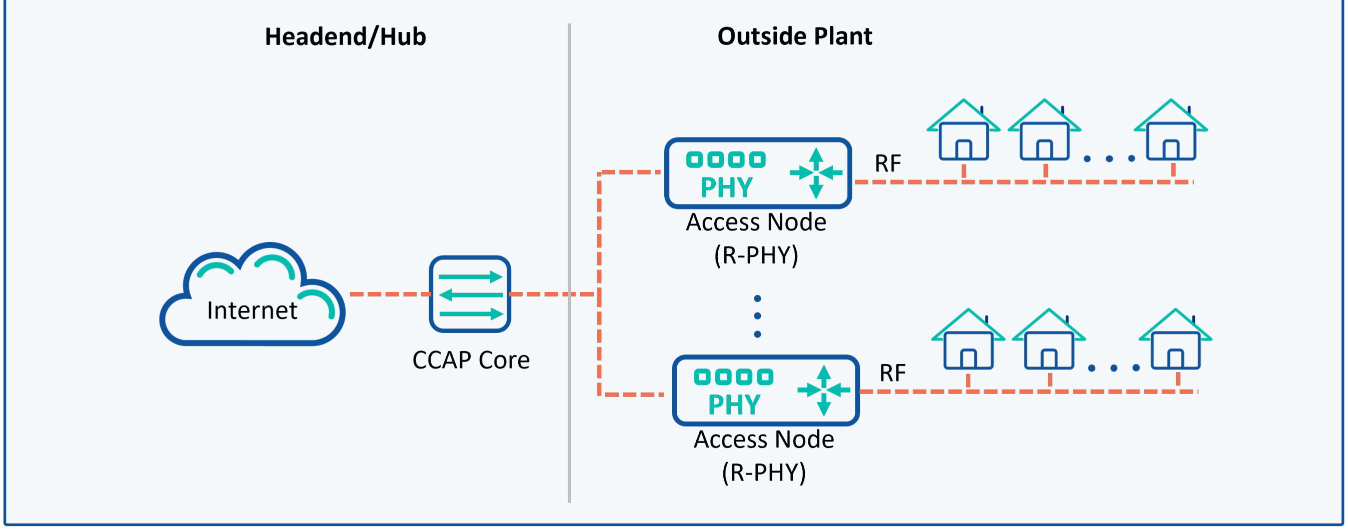
Bulletproof e-commerce, videoconferencing, streaming media and other premium services

Emulate 1G/10G home and business connections at scale

Benchmark and validate network performance, security, and QoS

Demonstrate compliance with federal and state grant funding requirements

TYPICAL CABLE ARCHITECTURE



KEY TESTING AREAS

Evaluating Network and Device Performance

Network and device performance testing is crucial for service providers because it ensures the delivery of high-quality, reliable services. By rigorously testing bandwidth, latency, jitter, throughput, and packet loss, providers can identify and address performance bottlenecks, maintain optimal network operation, and resolve network issues before they affect customers.

This is essential for meeting customer expectations, particularly for applications requiring real-time communication like VoIP and video streaming. Performance testing also supports scalability by ensuring that the network can handle increased load and traffic as the customer base grows.

Ensuring Quality of Service (QoS)

Quality of Service (QoS) involves traffic prioritization, where critical applications are given the necessary bandwidth and low latency to function optimally, ensuring that essential services are not disrupted by less critical traffic. Service providers must also verify compliance with Service Level Agreements (SLAs), which specify performance metrics such as uptime, latency, and packet loss. Meeting these SLAs is vital for maintaining customer satisfaction and trust.

To test QoS it is important to measure performance metrics on the application level, especially when the network becomes over-saturated. This ensures that the correct traffic is prioritized and that critical applications are given priority when network resources become limited.

Testing Network Security

Service providers need to ensure that their networks are reliable, available and secure for customers at all times. Security testing helps protect against attacks such as Distributed Denial of Service (DDoS) attacks, which can overwhelm network resources and cause service outages. Testing security architecture also helps identify and mitigate vulnerabilities that could be exploited to access sensitive customer data, including personal information, financial details, and communication records.

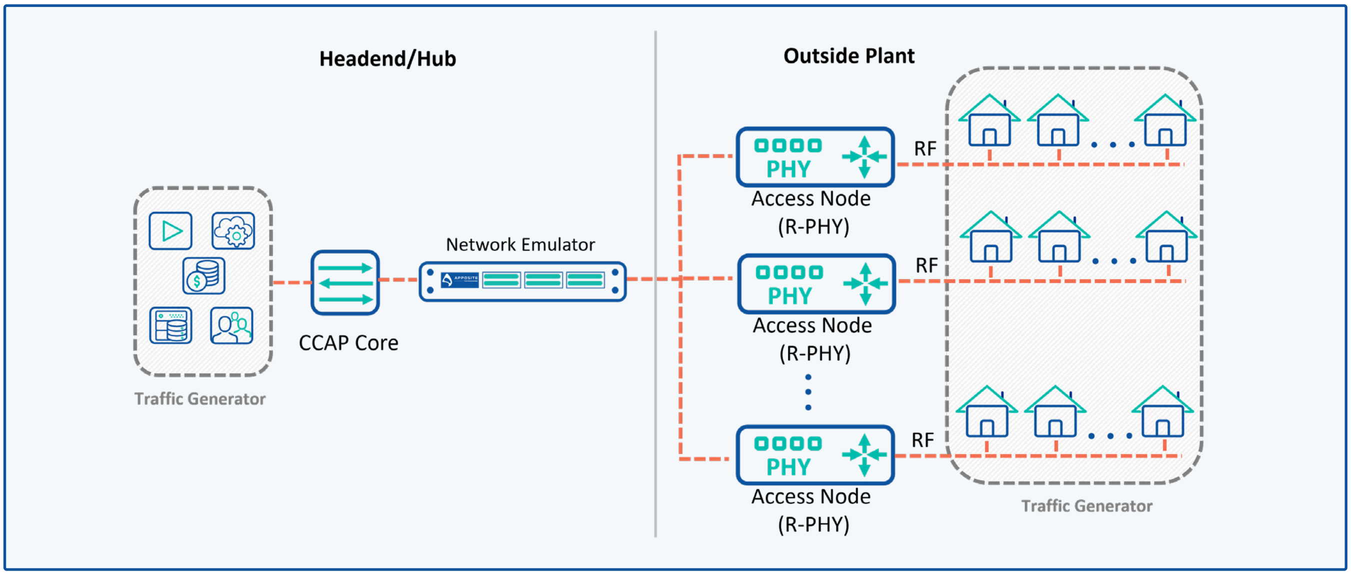
Benchmarking the performance of security devices prior to an attack enables more efficient threat detection. Testing with both malicious and valid application traffic helps validate their effectiveness in identifying and mitigating potential threats.

Compliance Testing

Compliance testing is a critical area for network service providers, ensuring that their networks adhere to industry standards and regulatory requirements. These regulations often cover a wide range of areas, including data privacy, security, and operational standards, and failing to comply can result in significant fines and legal repercussions.

By rigorously testing for compliance, service providers can guarantee that their networks are secure, reliable, and capable of delivering high-quality service to their customers. Furthermore, compliance testing is an essential component of qualifying for and maintaining government funded grants.

TESTING DOCSIS



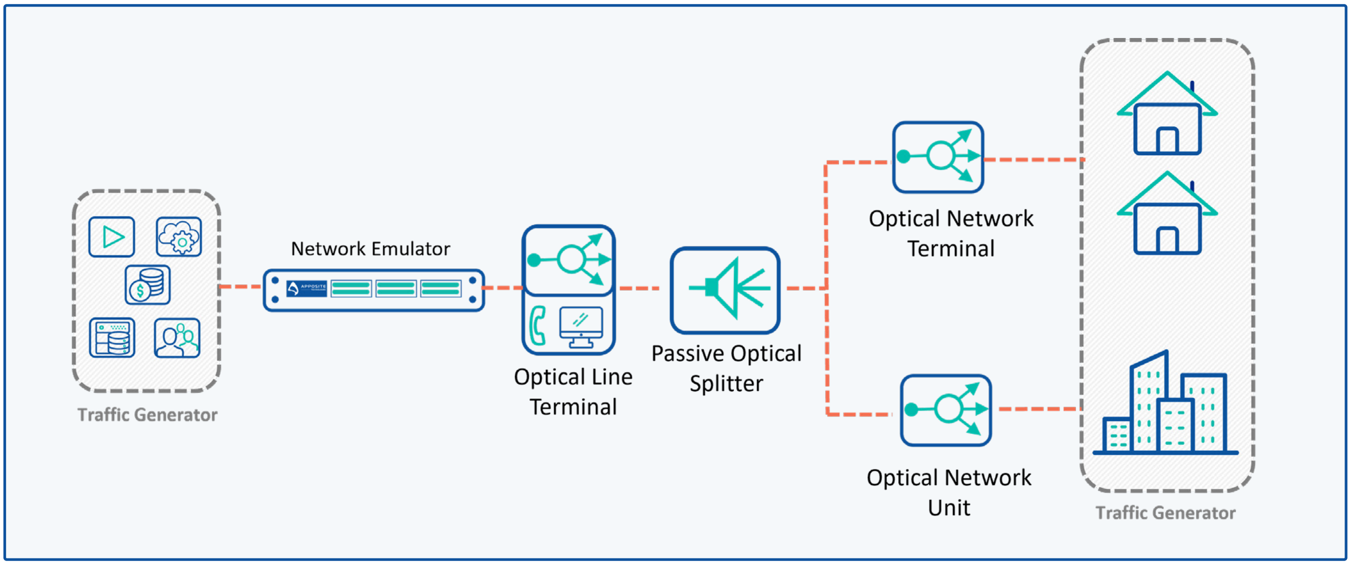
A typical DOCSIS architecture test scenario. Apposite equips engineers and network architects to test the performance of access networks at every juncture from BHRs to RFI access nodes to CCAP (Converged Cable Access Platform) core solutions, edge routers and cable modem termination systems (CMTS) — all without leaving your lab.

As Data Over Cable Service Interface Specification (DOCSIS) technology makes coax networks stronger and faster, cable providers must ensure devices meet the challenge of high-speed video, large file transfers, and remote workers sharing the bandwidth with Netflix and gamers.

Conduct easy, repeatable, scalable testing of broadband home routers (BHRs) and gateways (BHGs), cable modems (CMs), and end-to-end systems to:

- Fine-tune timing and synchronization
- Streamline adoption/migration to DOCSIS 4.0
- Bring multi-gigabit business-class services to market
- Ensure performance with greater distances between CMs and CMTS

TESTING GPON



A typical fiber access test scenario. Apposite lets test engineers define highly specific mixes of application traffic (and attack traffic) to test PON systems and components. Apposite emulates customers on one side of the system under test (SUTs) and severs on the other, simulating a broad mix of traffic profiles and network conditions.

Testing with Apposite also equips providers to maximize the value of fiber-based passive optical networking (PON) and gigabit-capable passive optical network (GPON) infrastructures. Our easy-to-use 'lab in a box' approach delivers a single system to test optical network terminals (ONTs), unpowered optical beam splitters, and optical line terminals (OLTs) — every element of the journey from subscribers' home or business to the Internet or PSTN.

- Fast-track revenue-generating high-speed Ethernet services
- Extend fiber to more business customers – multi-tenant buildings, hospitals, hotels
- Streamline deployment while ensuring compliance with federal and state regulations

SUMMARY

Using network performance test tools like network emulators and traffic generators helps service providers ensure reliability, availability, and security of services. These tools enable providers to benchmark device and system performance to establish a reference for measuring and maintaining consistent service quality over time. By recreating potential issues in a controlled environment, network emulators and traffic generators help avoid outages and proactively prevent customer issues, enhancing network reliability. Additionally, these tools support business growth by accelerating rollouts and ensuring that high-quality service and accountability are maintained as the network scales.

APPOSITE TEST SOLUTION HIGHLIGHTS

- Support for Traffic Generation and Network Emulation
- Easy-to-use, wizard-driven test methodology
- Browser-based GUI that is platform agnostic
- Single platform generates stateless and stateful traffic from layer 2 – 7, including security attacks
- Over 30K app flows included with built-in application library and 10K malicious attacks in the Attack Library
- Interface speeds 1Gbps, 2.5Gbps, 5Gbps, 10Gbps, 25Gbps, 40Gbps & 100Gbps
- Virtual Editions: VMWare, KVM
- Cloud Editions: AWS, Google Cloud, Azure
- Automation through comprehensive RESTful API

SOLUTION OVERVIEW

Netropy Traffic Generators

Benchmark the packet level performance of networks and devices with classic performance measurements like latency, throughput, and loss. Our traffic generators emulate clients and servers and generate a mix of realistic application traffic and malicious attacks at tremendous scale to optimize network performance. Configure up to a million traffic streams or select from our library of pre-defined flows from apps like Zoom, Oracle, Netflix, and SAP to assess access networks from end to end. Validate QoS policies on a per-app and per-stream basis and stress test under the most challenging scenarios.

Netropy Network Emulators

Replicate the dynamic conditions of any broadband or cable network in the test lab. Our network emulators can mimic the exact link characteristics of a network like bandwidth, latency, throughput and packet loss to determine how adverse network conditions could impact customer expeirence. By emulating different types of network conditions, in a controlled environent, service providers can thoroughly evaluate how new devices, applications, and services will perform under a variety of situations. This helps ensure they meet the required performance standards before deployment.

WHY APPOSITE?

Apposite has been in business for over 15 years and has helped customers around the globe from telecoms to system integrators, technology vendors and large enterprises. Our modern, easy-to-use test solutions enable teams to set up performance tests quickly and easily and trust the results.

Apposite Technologies

4223 Glencoe Ave b121, Marina del Rey, CA 90292 USA

www.apposite-tech.com | TEL: 1.310.477.9955 | info@apposite-tech.com