PRODUCT BROCHURE

Keysight Guide To Network Visibility Terms And Acronyms

Introduction

Network visibility is about removing blind spots that are obscuring the ability to readily see or quantify the performance of the network. This includes the applications running over the network as well. This visibility is what enables IT to quickly isolate security threats and resolve performance issues, ultimately ensuring the best possible end user experience. This guide is intended to give you a quick and easy reference to common network visibility and monitoring terms along with their meanings.

Active Monitoring:
Type of network monitoring in which test traffic is injected into a live network to verify network performance.

Application Programming Interface (API):
Set of subroutine definitions, protocols, and tools for building application software. Also used commonly as the documented and open means to access the services and functionality of a piece of software.

Application Performance Monitoring (APM):
Area of information technology (IT) that focuses on making sure software application programs perform as expected to provide end users with a high quality of experience (QoE).

Application and Threat Intelligence (ATI):
Real-time threat intelligence feeds with up-to- the moment content changes for security and application related data.

Automation:
Automation refers to a task or function that is performed without requiring human intervention.

Blind Spots:
Blind spots are areas where there is a lack of network visibility. These areas often contain unforeseen problems or threats.

Bypass Switch:
Specialized network data tap that has fail-over capability integrated within it. Typically used for inline security tools to make them more reliable.

Central Office Re-architected as a Data Center (CORD):
Carriers use SDN and NFV to transform their carrier functions into workloads that are hosted on a common infrastructure. It is an approach of providing infrastructure as a service and networking services as tenant applications for that infrastructure. Major service providers, like AT&T, SK Telecom, Verizon, China Unicom, and NTT Communications already support CORD.

Cisco Application Centric Infrastructure (ACI):
Cisco System's proprietary approach to support Software Defined Networking (SDN).

Command Line Interface (CLI):
Means of interacting with a computer program that uses a text-based interface for creating and issuing computer commands.

Compliance:
Standards and regulations, such as PCI-DSS, SOX and HIPAA, require organizations to take specific action to protect sensitive customer data. This means IT teams must proactively identify processes and solutions to ensure compliance when using public cloud.

Data Masking:
Replaces vulnerable or sensitive data with safe information. When data is masked, it is altered so that the basic format remains the same, but the key values are hidden.

Deep Packet Inspection:
Monitoring that examines the payload or data portion of a packet, as opposed to just the packet headers.

East-West Traffic:
Traffic in a virtual data center that moves from one virtual machine (VM) or application to another but does not pass to the top of the rack.

Element Management System (EMS):
Systems and applications for managing network elements (NE) in the Telecommunications Management Network (TMN) model.

Generic Routing Encapsulation (GRE) Tunnel:
Tunneling protocol that was originally developed by Cisco Systems which could encapsulate a different network layer protocols within virtual point-to-point links using a network based upon IP.

Gigabit Ethernet (GE):
The transmission of Ethernet frames at a rate of a gigabyte per second (e.g. 1,000,000,000 bits per second). This is a standard defined by the Institute of Electrical and Electronics Engineers (IEEE)—802.3-2008.

Graphical User Interface (GUI):
A user computer interface that uses graphical images instead of command lines to interface with the device's central processing unit (CPU). A GUI interface has been proven to be faster and more intuitively obvious than a command line interface (CLI).

GTP Session Controller (GSC):
An Keysight NPB that is focused specifically on correlating long-term evolution (LTE) traffic across multiple physical and logical connections for presentation to mobility analysis tools.

Heartbeat (packets):
Very small network packets transmitted at regularmicrosecond intervals to confirm tools are online and operating.

High Availability (HA):
HA systems are intended to operate continuouslywithout failure for an extended period of time.

This means that a robust design and high-quality parts were used in the design with the intention of preventing a significant number of network failures.

Inline:
Deployment of a device directly in the path of network data to perform some action on the data, such as data inspection, SSL decryption/ reencryption, quarantining of suspicious data, etc

Inline Network Packet Broker:
A network packet broker (which performs, load balancing, aggregation, and regeneration) that is deployed directly in the path of network data to manipulate the data.

Inline Tools:
Network and security monitoring tools that are deployed directly in an active/live network segment

Keysight Fabric Controller (IFC):
Monitoring that examines the payload or data portion of a packet, as opposed to just the packet headers.

East-West Traffic:
Keysight's management tool for software-defined visibility. It is available on Vision NPBs, such as Vision ONE and Vision 7300, to enable centralized management. It allows multiple NPBs to work collectively with resiliency within a single-pane-of- glass management interface and integrates with SDNs including Cisco ACI.

Metadata:
Additional data that is collected and describes other types of data running on the network. The most common form of network data is packet- based data. Metadata (such as the device type used, browser type used, geolocation of data as it crosses the network, border gateway identification, etc.) can be collected about the packet data and sent along with the packet data to monitoring devices to provide more conntext about that packet data

NetFlow:
Aggregated data statistics from the network that can be used to generate meaningful information that a

network administrator can to leverage to troubleshoot a network issue. This includes source and destination of traffic, class of service, and congestion information.

NetStack from Keysight:
A grouping of out-of-band network-oriented dat a monitoring features for the Vision NPBs which include filtering, aggregation, replication, and more.

Network Functions Virtualization (NFV):
NFV decouples the network functions, such as network address translation (NAT), firewalling, intrusion detection, DNS, and caching from proprietary hardware appliances so they can run as software on standard computing hardware to improve the management networking services

Network Packet Broker (NBP):
Device that provides intelligent data distribution of traffic from across the network to a collection of monitoring, security, and analytics tools.

Network Performance Monitoring (NPM):
The routine checking and evaluation of the operation of a network. The goal is to constantly monitor the network to make sure it is in optimum working condition.

North-South Traffic:
Refers to the direction of traffic within a data center. The North-South direction refers to entering or leaving the data center or data center equipment and traveling to other, external devices from that device.

Orchestration:
Orchestration refers to the coordination (or sequencing) of automated tasks and/or functions to accomplish a defined process or workflow. Orchestration is used in larger scale networks for tasks such as provisioning, patching, and resource management that need to be performed at a massive scale

Out-of-Band Tools:
Network and security monitoring tools that receive a copy of network traffic from a SPAN port or a network tap. These tools are not deployed in the direct path of network traffic and do not provide real-time analysis.

PacketStack from Keysight:
A grouping of intelligent packet monitoring features for the Keysight Vision NPBs. These include deduplication, header stripping, packet trimming, timestamping, data masking, Generic Routing Encapsulation (GRE) tunneling, and burst protection.

Passive Monitoring:
Type of network monitoring in which copies of actual traffic, captured from a SPAN port or network tap, are used for analysis.

Quality of Experience (QoE):
This is a measurement of a customer’s experienceswith a particular service (Web browsing, voice calls, videos, call center, etc.).

Quality of Service (QoS):
A description (usually based upon measurement) regarding the performance of a service seen by the users on the network.

Representational State Transfer (REST):
An Internet Engineering Task Force (IETF) protocol that defines an architecture for designing networked applications that relies on a stateless, client-server, cacheable communications protocol.

Resilience:
A characteristic of a network monitoring system, achieved most often through failsafe deployment and redundant components, that allows monitoring to continue in the event of a failure in a system component.

Service Level Agreement (SLA):
A contract between a service provider (which can be either internal or external) and the customer that defines the level of service contracted from the service provider.

Secure Socket Layer/Transport Layer Security (SSL/TLS):
Transport layer protocols that provide session- based encryption and authentication for secure connections between network application clients and servers over an insecure network, such as the Internet.

SecureStack from Keysight:
Security-oriented features for Keysight Vision series network packet brokers (NPBs) that provide optimized handling for secure traffic. Capabilities include secure sockets layer (SSL) decryption.

Service Chain/Service Chaining:
Set of network services that are performed in a specific order and steer the traffic through a chain of connected programs or devices.

Software-Defined Networking (SDN):
A computer networking approach that allows network administrators to programmatically configure and manage network behavior. These functions have been abstracted from the lower- level functionality and hardware through open interfaces.

Software-Defined Visibility (SDV):
Abstraction of visibility management to a software layer. The Keysight Fabric Controller (IFC) can serve as the management tool for SDV since it works much like an SDN controller.

Software-Defined Wide Area Network (SD-WAN):
The application of SDN technology to a wide area network (WAN). This includes connecting enterprises, data centers and branch offices.

Switch Port Analyzer (SPAN):
Port on an Ethernet switch that is dedicated to forwarding replicated traffic from other ports or virtual LANs on the Ethernet switch.

Test Access Port (Tap):
Passive device that creates a copy of traffic in the network.

Top-of-Rack (TOR):
Network architecture in which computing equipment like servers and applies are located within the same or adjacent racks. This equipment is usually connected to a network switch that is located within that rack.

Virtual Local Area Network (VLAN):
A network of computers that are located in different geographical but have the look and feel of one system, one local area network (LAN).

Virtual Network Tap (vTAP):
Software that provides full access (or visibility) to all the traffic moving between virtual machines and virtual network devices in a irtualized environment.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES