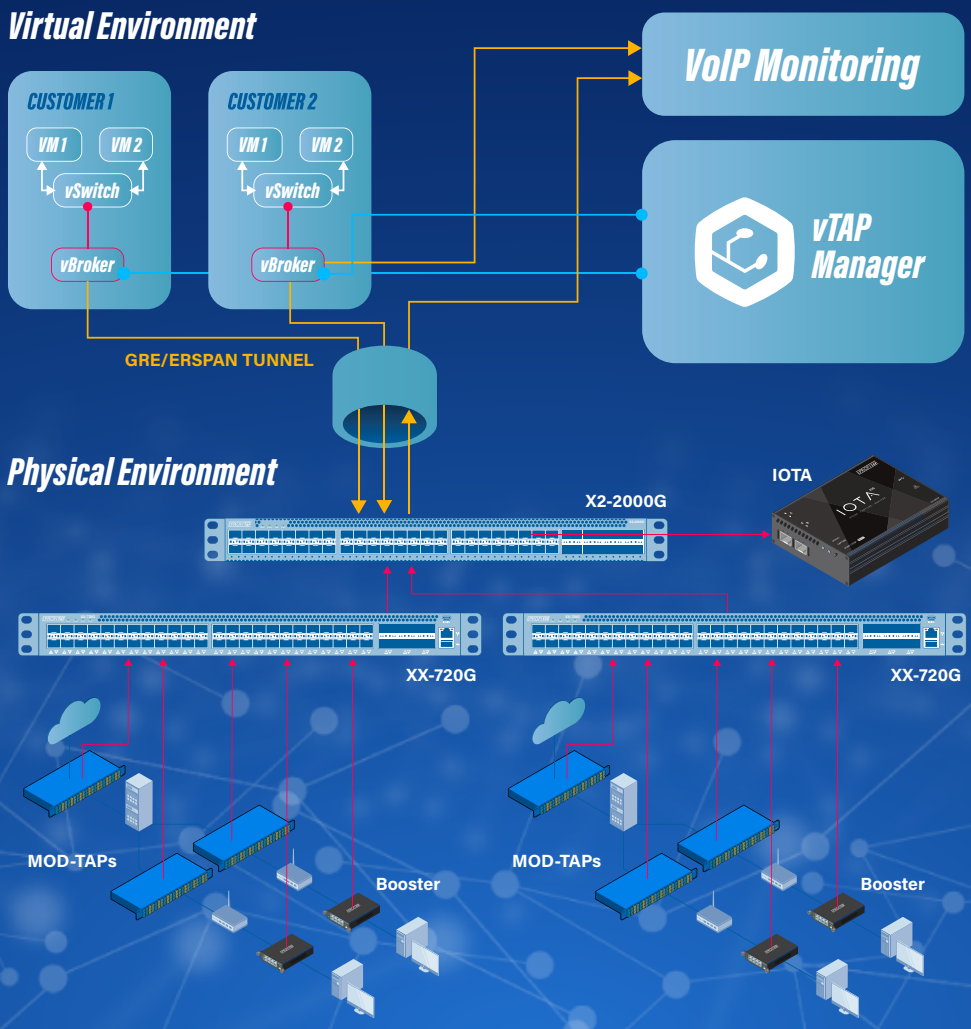
PROFITAP

Use Case

NETWORK MONITORING IN VIRTUAL AND PHYSICAL MULTI-TENANT NETWORKS

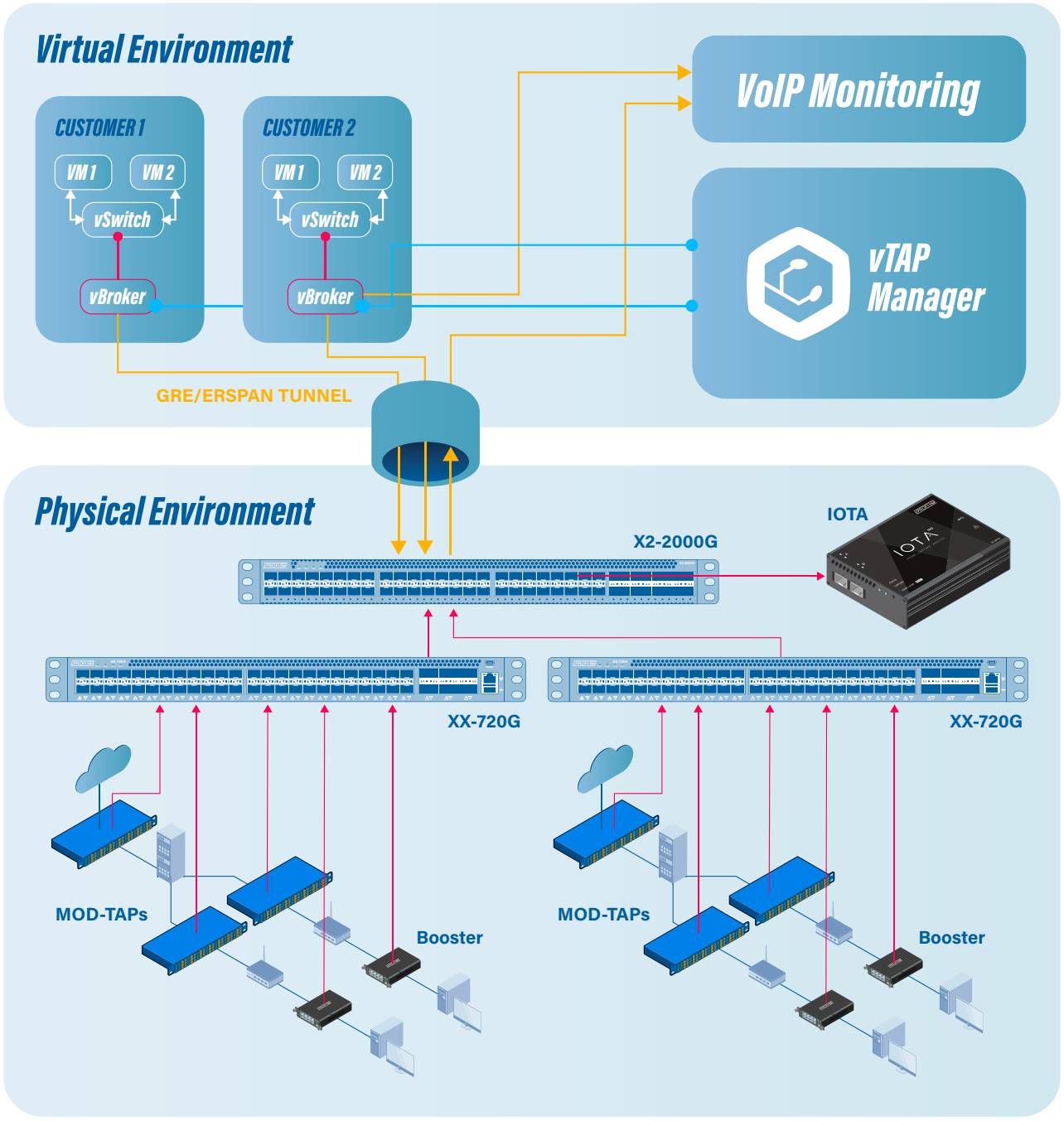


Overview

The Challenge

A multinational technology company specialized in cloud communications and workstream collaboration solutions with multiple global sites tasked Profitap to design a constant and permanently running network infrastructure solution for VoIP monitoring and general performance analysis.

With networks spread over physical and virtual environments and remote sites, finding the root cause of network issues quickly and reliably is challenging. Profitap designed an ad hoc network architecture solution capable of constantly monitoring and troubleshooting network issues the moment they arise. The ultimate goal was to empower the customer with quick and reliable access to packet data in physical and virtual networks.



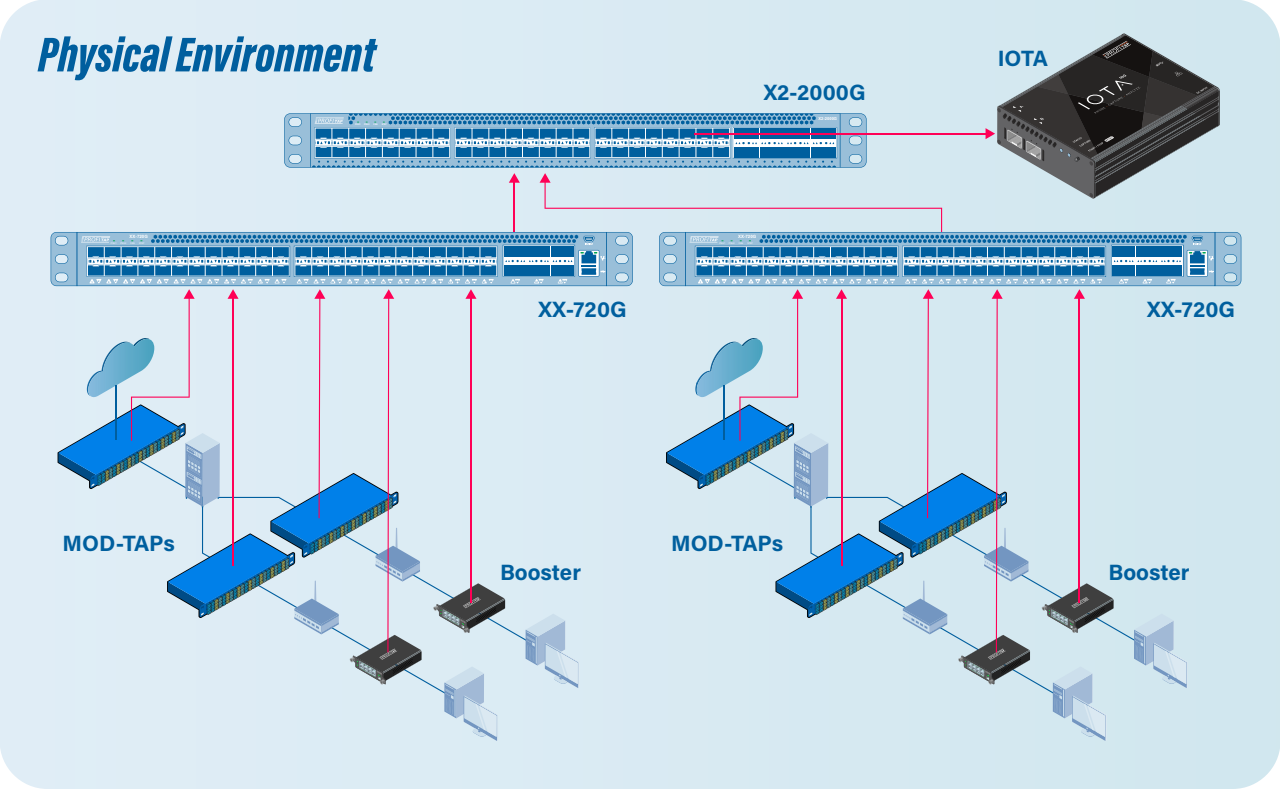
Network Architecture Overview

The company's network architecture contains a virtual environment with separated multi-customer spaces used for VoIP traffic. For each customer, there are virtual machines (VM) dedicated for VoIP traffic. VoIP traffic is also coming from internal sources like physical links and outside sources like the Internet.

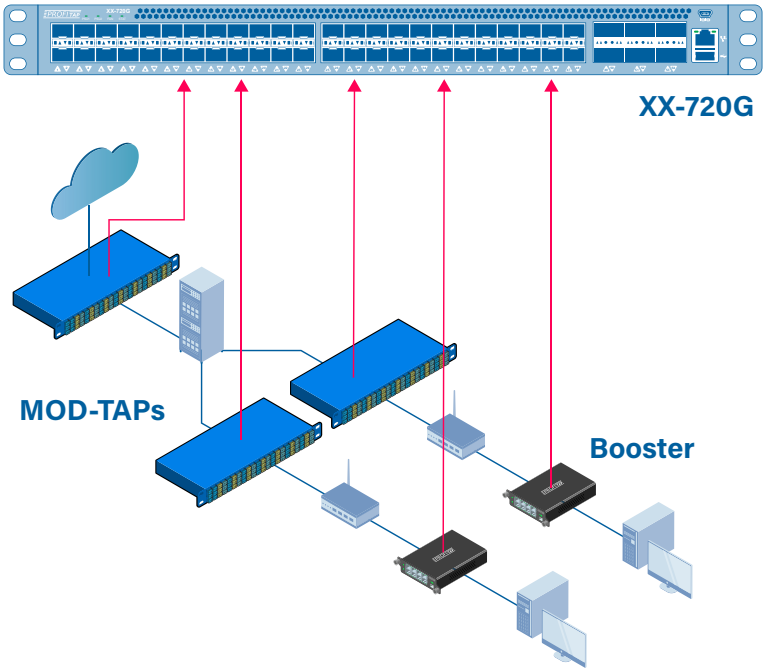
VoIP analysis is needed to continuously monitor VoIP traffic performance inside the virtual network, while the performance analysis capabilities of the solution are used either on-demand or as analysis of historical data captured over time.

Profitap's network monitoring solution is divided into two parts: physical and virtual architecture. This paper will zoom in on each of the architecture's components.

Part 1: Physical Architecture



Accessing the Network Traffic: Fiber TAPs



To access traffic reliably and with high performance, fiber TAPs were used as the first bricks of the network architecture infrastructure.

Profitap fiber TAPs provide secure passive in-line network access for the monitoring of 1–400 Gbps fiber networks. By splitting the light flowing on the network link, fiber TAPs deliver an exact copy of the data for real-time monitoring and analysis without disrupting the network. Passive fiber optic TAPs require no power and therefore introduce no point of failure when deployed in a network.

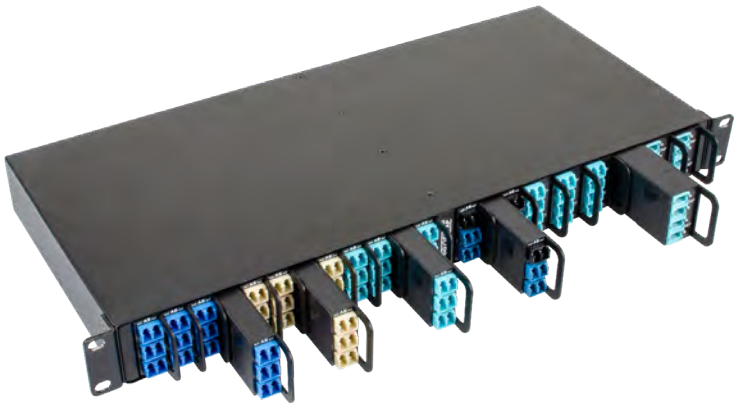
In particular, Profitap MOD-TAP was selected as a flexible and scalable fiber optic TAP solution. The MOD-TAP provides access to network traffic for a wide variety of fiber types and standards.

With a modular design and a wide range of fully passive TAP modules available, the MOD-TAP brings a high density of tapping points to the monitoring system, with up to 24 TAP modules per chassis.

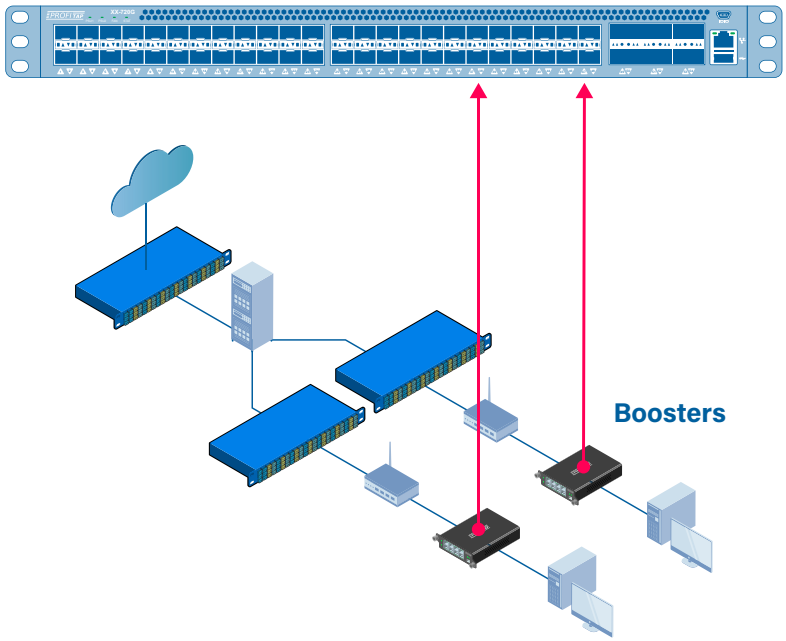
The MOD-TAP forwards traffic to the XX-720G Network Packet Broker.

MOD-TAP Overview:

- Non-intrusive in-line network access
- Permanent network link guaranteed
- Monitoring of all OSI layers
- Passive, unpowered
- LC, MTP, 40/100G BiDi, and DiodeTAP modules available
- DiodeTAP module's diode function protects the network against light insertion from TAP ports (>35 dB insertion loss on TAP port input blocks all signals)



Accessing and Aggregating (Copper) Network Traffic: Profitap Booster



In order to access copper network links of up to 1 Gbps, the Profitap Booster has been placed at key points.

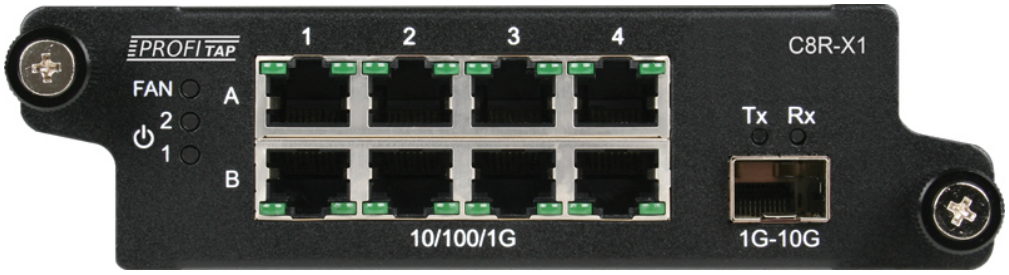
Booster Aggregation TAPs are designed for lossless traffic aggregation from multiple in-line links or out-of-band connections into a single output, optimizing port usage on monitoring tools.

The Booster In-Line Aggregation TAP was selected as it connects 4 x 10/100/1G in-line links to one 1/10G output port, providing fail-safe traffic aggregation and speed conversion in one device.

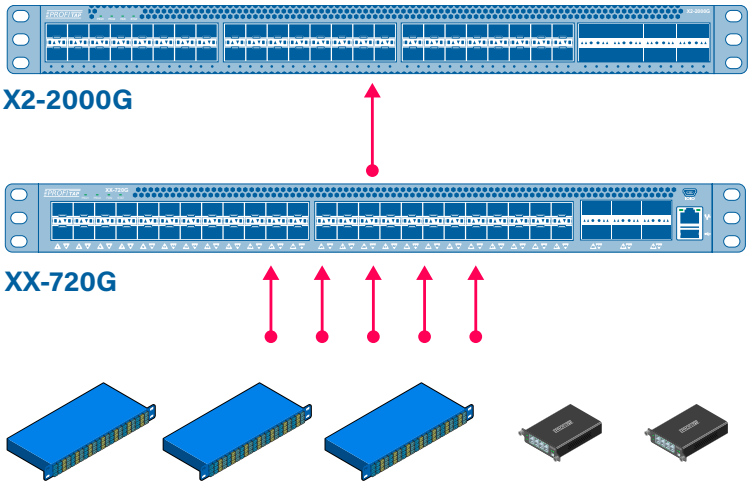
Booster Overview:

- **Lossless Aggregation:** Conventional Aggregation TAP solutions often feature output ports with the same speed as the network links. This causes oversubscription on the output port of the TAP, causing valuable packets to be lost. By aggregating network traffic to a 1/10 Gbps output, no packet loss occurs.

- **Speed Conversion:** Many high throughput devices like network packet brokers feature ports designed for 10/40/100 Gbps operation. This means that lower-speed links, such as 10M/100M/1G, cannot be forwarded directly to such Network Packet Brokers. The Profitap Booster overcomes this challenge by converting these links into a single 1/10 Gbps output.

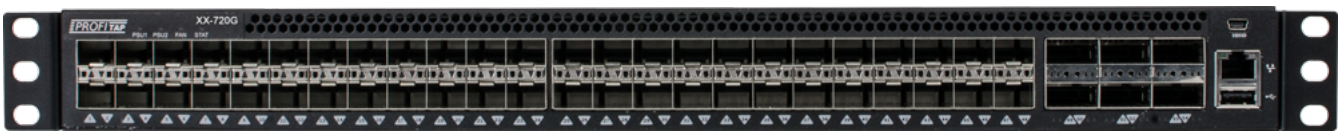


Traffic Aggregation: XX-720G Network Packet Broker



After accessing the network traffic with Fiber and Aggregation TAPs, the traffic needed to be monitored and optimized. In order to aggregate and distribute the right traffic between the TAPs and X2-2000G in a cost-effective way, multiple XX-720G high-density Network Packet Brokers were selected as the first layer of aggregation.

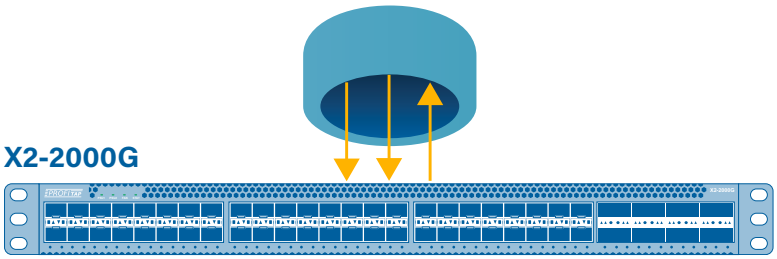
Network Packet Brokers orchestrate the traffic coming from multiple network links and perform advanced, intelligent traffic management to ensure that monitoring tools receive the appropriate packet data. By deploying Network Packet Brokers, a layer of intelligence was added to optimize the monitoring architecture and increase the network performance.



XX-720G Overview:

- Aggregation, replication, filtering, load balancing (any-to-any, any-to-many, many-to-many)
- Local and remote management (CLI, GUI, SNMP, Syslog)
- TACACS+ authentication
- Redundant, hot-swappable PSUs and fan modules available in AC or DC version
- Powerful filtering (layer 2–4, overlapping)
- Flexible role-based access
- High-density, 720 Gbps throughput in a 1U footprint
- 1G, 10G and 40G traffic monitoring (4 x 10G fan-out possible on 40G ports)
- Remote management software

Traffic Filtering and Tunneling: X2-2000G Next-Gen Packet Broker



All the traffic coming out from the Profitap XX-720G Network Packet Brokers is fed into the Profitap X2-2000G: a Next-Generation Network Packet Broker (NGNPB) with a total throughput of 2 Tbps. The Profitap X2-2000G provides aggregation, replication, powerful filtering, and load balancing in very high bandwidth port monitoring and analysis scenarios.

The customer selected the Profitap X2-2000G for mainly three reasons:

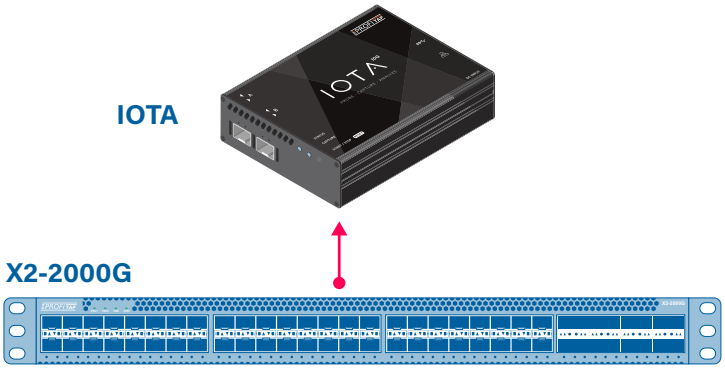
- In-line processing of all features at wirespeed: instead of forwarding the data through a co-processor, there is no other limitation than the device processing capability.
- Non-conflicting rules creation: all rules are active in parallel with each other. This makes sure no conflict between new and existing rules can happen and saves time setting up new rules.
- Tunnel termination and creation were important for the customer to get the right traffic to the VoIP analysis software.

For this use case, X2-2000G redirects traffic to the IOTA analysis monitoring solution, and also creates a tunnel out to the VoIP monitoring system.

X2-2000G Overview:

- Aggregation, replication, filtering, VLAN tagging and stripping, MPLS stripping, and load balancing (any-to-any, any-to-many, many-to-many)
- Packet slicing, timestamping, GRE de-tunneling, VXLAN de-tunneling, and ERSPAN tunneling and de-tunneling
- Local and remote management (CLI, GUI, SNMP, Syslog, Ansible)
- Layer 2–4 filtering
- RESTful API support
- Flexible role-based management access
- In-line mode and in-line tool sharing
- TACACS+/RADIUS authentication
- Redundant, hot-swappable PSUs and fan modules
- Supports 1GbE, 10GbE, 25GbE, 40GbE, 100GbE

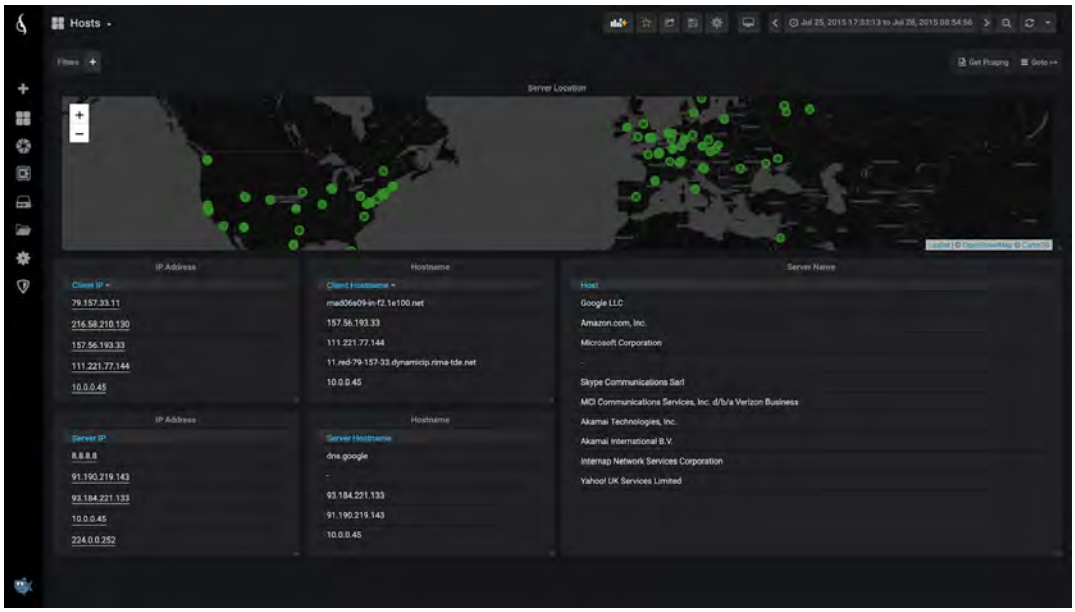
Real-Time and Historical Network Analysis: IOTA



To analyze specific parts of the network data, the company's engineers forward traffic to the Profitap IOTA from a port on the X2-2000G and use it for long-term real-time analysis. IOTA is an All-In-One Network Analysis Solution that combines capture, storage, and analysis capabilities in a single device.

IOTA provided the customer a quick and accurate overview of the network traffic without the need for on-site technical staff, making it easy to quickly identify and resolve network application issues.

Different models are available: the customer selected the IOTA 10G+ model, fitted with GPS and PPS ports to provide advanced timestamping synchronization features, and 2TB storage option.



IOTA Overview:

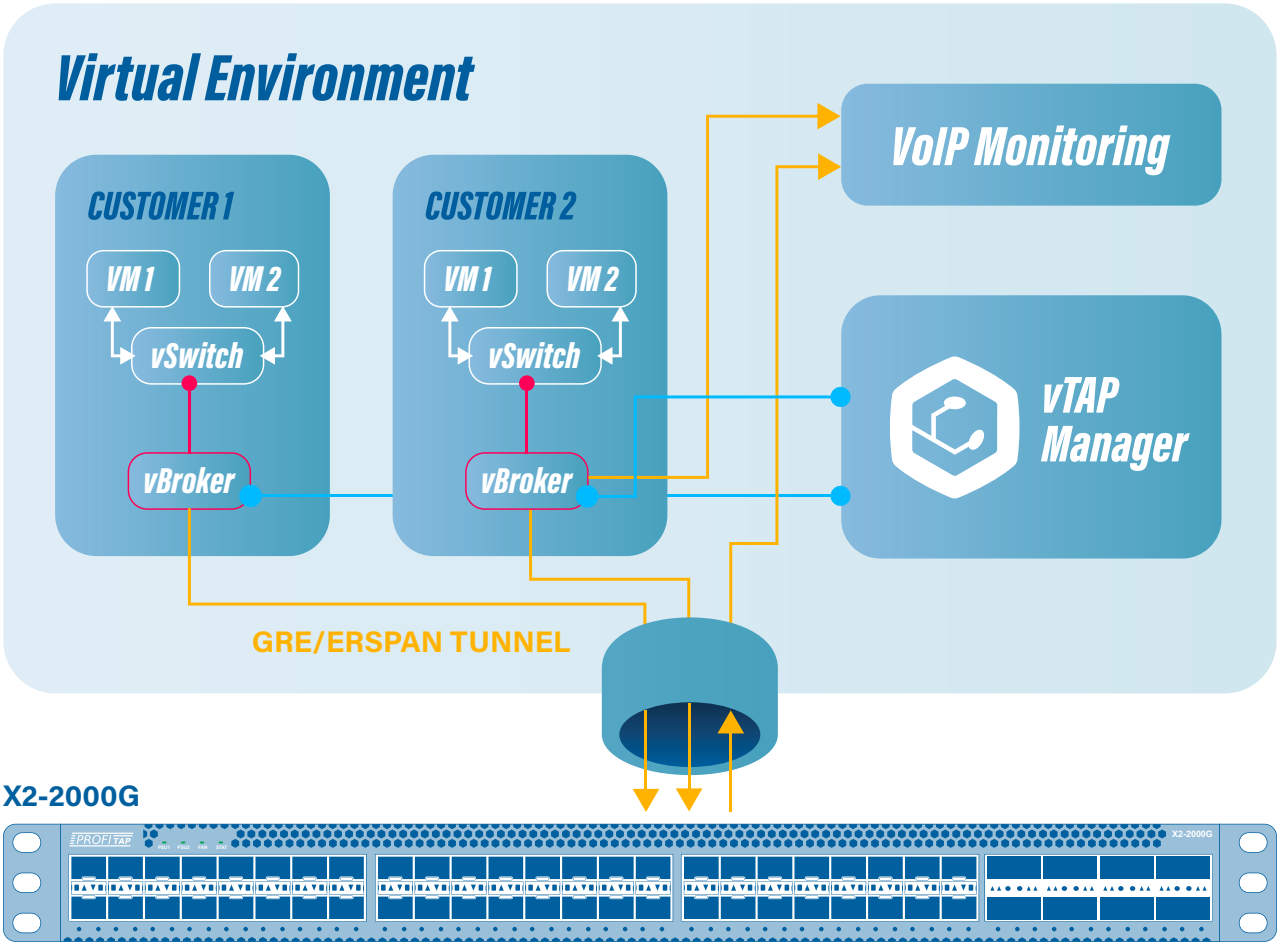
- **2 TB ENCRYPTED REMOVABLE STORAGE:** PCAP collection, metadata database and system are stored on a removable encrypted SSD (AES 256-bit).
- **GPS/PPS TIMING PORTS:** GPS/PPS input for advanced timestamping and accurate latency measurement.
- **CUSTOMIZABLE DASHBOARDS:** Dashboards can be created, modified, and shared across multi-users in a web-based environment.

Part 2: Virtual Architecture

The company's virtual network environment architecture presents separated multi-customer spaces used for VoIP traffic. For each customer, there are virtual machines (VM) dedicated for VoIP traffic. VoIP traffic is also coming from internal sources like physical links and outside sources like the Internet.

All of these VMs are connected to the Profitap X2-2000G Network Packet Broker.

The end-goal is to get full traffic visibility for each VM environment and send traffic of interest to a VoIP monitoring tool and IOTA for analysis.



Accessing and Aggregating the Virtual Traffic

The virtual network environment contains different layers, all equipped with an instance of the Profitap Virtual TAP (vTAP), which provides complete visibility of VM traffic (including inter-VM) for security, availability, and performance monitoring. This gives the customer the means to easily access traffic in a complex virtual network architecture.

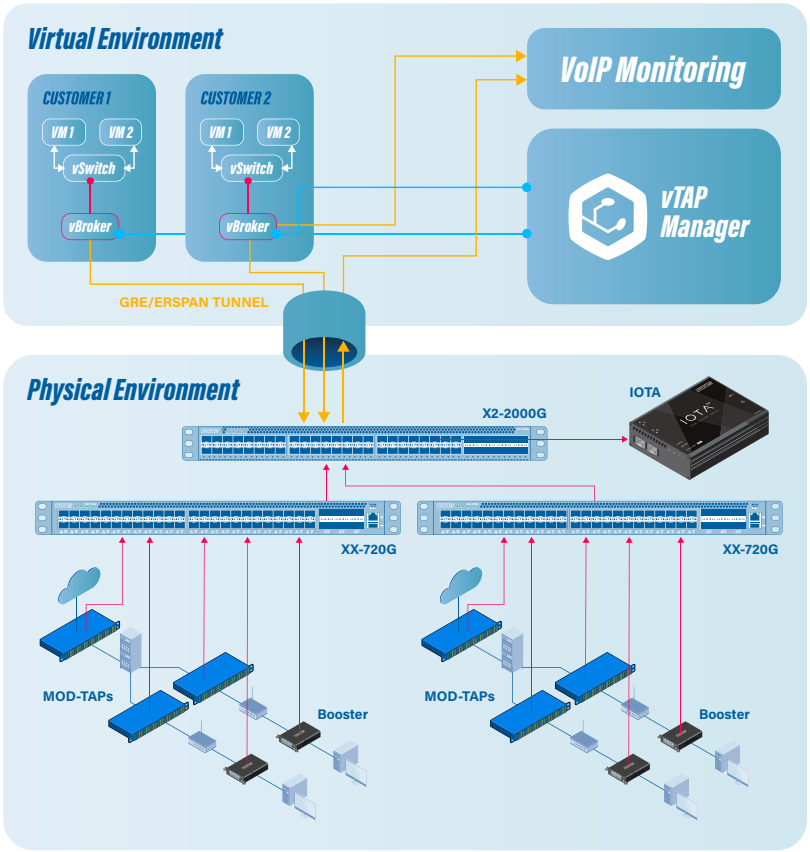
The tapped virtual traffic is aggregated by the Virtual Network Packet Broker (vBroker) — embedded in the vTAP solution. The main role of the vBroker is to perform operations like filtering and creation of data tunnels towards the Profitap X2-2000G.

As soon as the vBroker receives data, such as a VoIP stream, it creates a tunnel, which incorporates the streams inside. The tunnel termination feature of the X2-2000G will remove the stream and allow forwarding data to the IOTA.

Within the X2-2000G, the tunnel is terminated and created in order to forward the replicated traffic back to the VoIP monitoring solution. In a nutshell: when the traffic goes into the X2-2000G, it is decapsulated, optimized (replication and filtering), and then the result is proceeded either to a tunnel creation or to a physical appliance (in this case, Profitap IOTA). Filtering on the vBroker or the NPB is an either-or option for the customer, depending on the configuration chosen between physical or virtual and the traffic source.

vTAP Overview:

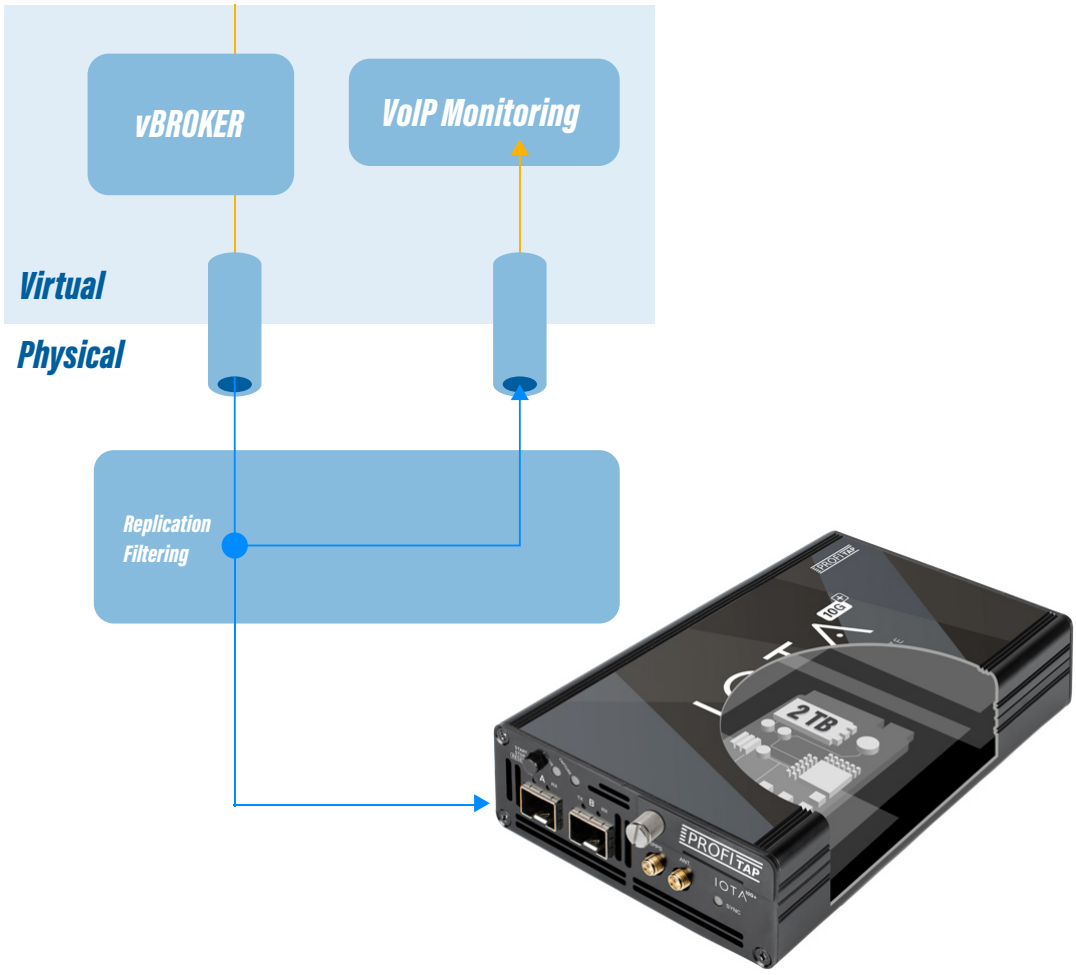
- Enables security, availability, and performance through proactive monitoring of virtual data centers
- Complete visibility of traffic in virtual environments, eliminating blind spots
- Central management interface for a single overview of the entire virtual visibility system
- Filtering helps bring down the virtual traffic to actionable data and prevent network congestion
- Easily scalable



Tunneling, tunnel termination, tunnel stripping

Tunneling, Tunnel Stripping, and Tunnel Termination* are features that can be applied to X2-2000G NGNPB ports allowing them to be used as tunnel sources or destinations. Tunneling protocols are communications protocols that allow data packets from one network to another. A tunnel is often a mechanism used to ship a foreign protocol across a network that normally would not support it. Tunneling works by encapsulating packets: wrapping packets inside of other packets.

Profitap X2-2000G provides access to encapsulated traffic for a variety of tunneling protocols, such as Encapsulated Remote SPAN (ERSPAN), Generic Routing Encapsulation (GRE), and Virtual Extensible LAN (VXLAN). These advanced de-tunneling features helped the customer enhance the network visibility capabilities, allowing the integration of multiple solutions to collect and forward tapped traffic.



---

*Definitions:

- Tunnel Termination: decapsulates incoming tunneled (ERSPAN, GRE, VXLAN) traffic pre-filtering.
- Tunnel Stripping: strips the specified encapsulation (ERSPAN, GRE, VXLAN, IP over IP, Teredo) by removing the tunnel headers from the targeted/filtered packets (post-filtering).
- ERSPAN Tunneling: encapsulates the targeted/filtered packets with the specified ERSPAN tunnel properties (source MAC, source IPv4, destination MAC, destination IPv4, ERSPAN session ID).

Conclusions

The physical and virtual architecture described here is the result of a solution proved in the field to be reliable, enabling the customer to track and monitor the performance of heterogeneous networks.

With one solution, it is possible to analyze remotely any type of network traffic, whether it is coming from a virtual or physical network environment, thanks to the flexibility of the IOTA features, in particular:

- Quickly pin-point network problems, statistics, and troubleshooting
- Diagnose remote problems without on-site assistance
- Secure: physical separation from the network

With the Profitap X2-2000G Network Packet Broker, it is possible to manage and optimize physical and virtual data flow and maintain network flexibility by:

- Delivering filtered traffic of interest
- In-line processing of all features at wirespeed
- All rules handled at the same time, no accidental conflicts
- Easy to use GUI for easy overview of device status and ports and rules setup

With the complete solution in place, the customer is now able to securely and reliably access network traffic throughout the entire network and easily manage and optimize it for analysis purposes.

Profitap develops and manufactures network monitoring solutions that drive network visibility and analytics on all traffic across physical and virtual infrastructures. All these solutions are designed with the security, forensics, deep packet capture, and network & application performance monitoring sectors in mind. Profitap's network visibility solutions provide reliable and secure traffic access, help optimize and manage data flow and assist in capturing and analyzing network data of interest. With a portfolio of high-end network packet brokers, the most diverse TAP portfolio on the market, and award-winning ProfiShark® 1G and IOTA®, Profitap sets new standards in an industry where the definition of excellence is constantly being challenged.

With more than 1,000 clients, many of which are among Fortune 500 companies, from 60 countries, Profitap has become a must-have partner to achieve reliable network visibility and analytics.

PROFITAP HQ B.V.
HIGH TECH CAMPUS 84
5656 AG EINDHOVEN
THE NETHERLANDS

sales@profitap.com
www.profitap.com

Profitap

@Profitap

Profitap-international

2021-10-06