BEIJING

603, CLP Information Building,

6 Zhongguancun South Street,

Haidian District, Beijing, China

Tel: +86 10 6870 9986

Email: sales@greenet.com.cn

HONG KONG

Unit 1001, Mira Place Tower A,

132 Nathan Road,

TST, Hong Kong

Tel: +852 2824 8753

Email: sales@greenet.co

WUHAN

Fl 4, Building E2, 4 Middle Software Park

Road Optics Valley Software Park, East Lake

High-tech Development Zone, Wuhan, China

Tel: +86 27 8780 9610

Email: sales@greenet.com.cn

UZBEKISTAN

Uzbekistan Tashkent City,

Mirabad District, 14 Oybek ko'chasi

Tel: +998 93 001 2248

Email: sales@greenet.co

Super Intelligent Network Element White Paper

GREENET MANAGING CONNECTIONS SMARTER

Super Intelligent Network Element White Paper——Catalogue

CATALOGUE

1 PREFACE

Super Intelligent Network Element, SINE, offers a rich portfolio of innovative SDN/NFV network solutions, along with giving granular visibility of traffic in fixed,mobile, and new networks.

1.1 PURPOSE

This document targets for any audience who are interested in learning more about GreeNet's SINE solutions. In this whitepaper, we analyze broadband and mobile data market requirement, and how to take advantage of SINE's unique functionalities and give in-depth network visibility and analytic data to Communication Service Providers.

1.2 GLOSSARY

Abbreviation	Explanation
SINE	Super Intelligent Networking Element
MSE	Multi-Services Edge
SDN	Software-Defined Network
NFV	Network Function Virtualization
SR	Service Router
BRAS	Broadband Remote Access Server
MEC	Multi-Access Edge Computing
PPPoE	PPP over Ethernet
PAP	Password Authentication Protocol
CHAP	Challenge-Handshake Authentication Protocol
VXLAN	Virtual eXtensible LAN
DPI	Deep Packet Inspection
PCRE	Perl Compatible Regular Expressions

2 INDUSTRY BACKGROUND AND SOLUTIONS

2.1 INDUSTRY BACKGROUND

2.1.1 MARKET DRIVEN

According to S&B Market Intelligence, July 2019, the Broadband speeds are increasing, especially in countries where operators are moving to install more fiber in their networks. The average global broadband speed measured between May 2018 and May 2019 was 11.03 Mbps, up 20.65% over the previous year, according to recent data from the broadband comparison site Cable.co.uk. Dan Howdle, a consumer telecom analyst at cable.co.uk, noted that some countries are seeing much faster increases than others, especially in places where there is a push to install fiber to more homes and businesses[1]. There are more and more countries are introducing and commercializing fiber services, with speed up to 1Gbps, to home and enterprise users. In China alone, it estimates that more than 3 billion devices are connected to the network at any given time. The market potential for network equipment and accessing solutions is significant.

2.1.2 BUSINESS DRIVEN

The continuous expansion of broadband networks drives the rapid growth of data services. The high use of P2P services, online games, VoIP and other applications brings a large number of customers to operators. However, it brings some network troubles that the CSPs are required to manage.

Network Security becomes very critical in the CSPs business. In recent years, cyberattacks gradually expand to high-value applications. From what we learn from our customers, more than 70% of current attacks are concentrated on the application layer. This number is growing.Content security is also becoming a key issue in information security. The customer sturn to their service providers for security solution support.

Following the continuous development of new networking technology, many new application solutions are emerging. It gives many operational challenges to CSPs, especially for network visibility and control management, such as extra resources used for P2P malicious, stealing of personal information, illegal use of VOIP, and unauthorized NAT operations.

The biggest challenges currently faced by traditional network operators are how to conveniently and quickly deploy new applications on their networks, and how to flexibly update and upgrade their applications to meet rapidly changing business needs.

2.1.3 CHALLENGES FOR LEGACY BRAS

CSPs are expected to roll out new services regularly. Therefore they would like to have full flexibility to develop and deploy new services in time. Today, CSPs is limited by its legacy MSE/BRAS solutions because of:

- Weak traffic awareness: cannot identify and sense traffic above the L3 layer;
- Slow launch of new business: new business development cycle is long, and deployment costs are high. It is difficult to go online for application, lagging behind market demands;
- Uneven utilization of network resources: most current MSE / BRAS is using vertical integration of software and hardware. It is a closed architecture. The control plane and forwarding plane resources do not match. It is challenging to achieve resource sharing and flexible scheduling of services. The utilization rate is uneven and difficult to improve;
- Complexed configuration management: Network equipment from different manufacturers deployed in distributed end nodes; they do not have unified management capability. It creates a huge workload from operation to maintenance for different configurations of different manufacturers.

2.1.4 INDUSTRY SOLUTIONS

Broadband Remote Access Server (BRAS) is also commonly called Broadband Network Gateway (BNG). It

sits at the edge of the internet core network. It performs a wide range of system functions from subscriber management, routing, policy enforcement, content filtering to IP address management. BRAS is commonly used in broadband service providers' environments worldwide. However, the continued high growth of internet traffic such as video, IoTs, and gaming raises a challenge to the service providers to continuedly upgrade their capacity, improve the overall user's QoE at the edge. As a result, virtualization is a logical resolution for network expansion and preserve a better ROI.

vBRAS is the virtualization of BRAS with SDN/NFV architecture. It offers flexibility, scalability, and cost-effectiveness for service providers to optimize any BRAS functions on a universal X86 server with Supervisor and DPDK. vBRAS decouples control from the user plane, or it is called Control-User-Plane-Separation (CUPS), to allows a full acceleration of data plane at the edge.

In the mobile environment, Multi-access Edge Computing (MEC) brings a similar architecture to the mobile edge – flexibility and scalability - that enables flexible and rapid deployment of new applications and services. Typical use cases are Converged DPI, content caching, bandwidth management, application-level QoS, Internet of Things, video optimization, and so on.

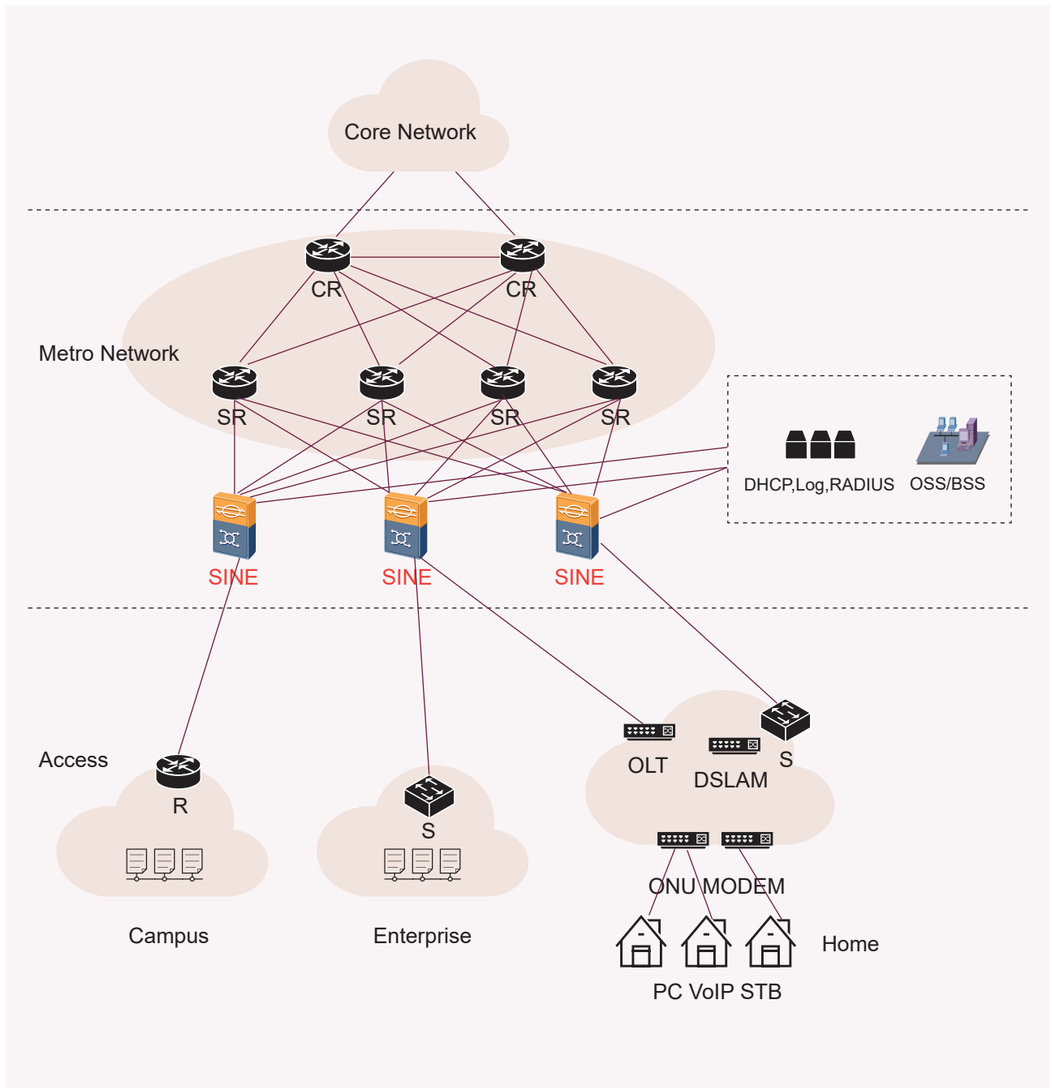
2.2 SOLUTIONS

GreeNet' Super Intelligent Network Element, or in short it is called SINE, offers a rich portfolio of innovative SDN/NFV network solutions, along with giving granular visibility of traffic in fixed and mobile networks. SINE combines with third-party caching and CDN systems to store hotspot resources closed to subscribers As a result it enhances user's online experience. SINE also stores a large number of original CDR data records, that use to provide relevant, accurate, and granular data for use in systems of :

- LTE service awareness and analytics system
- VoLTE end-to-end analytics system
- Personal Security System including anti-malware, anti-DDoS, anti-phishing, spyware, Trojan Horses attacks
- IoTs service stability system
- Edge Compute Systems including BRAS, MEC, Edge Storage
- UPF for 5G networks
- Provide interfaces to Integrate with broadband management, caching and network optimization systems

3 SYSTEM ARCHITECTURE

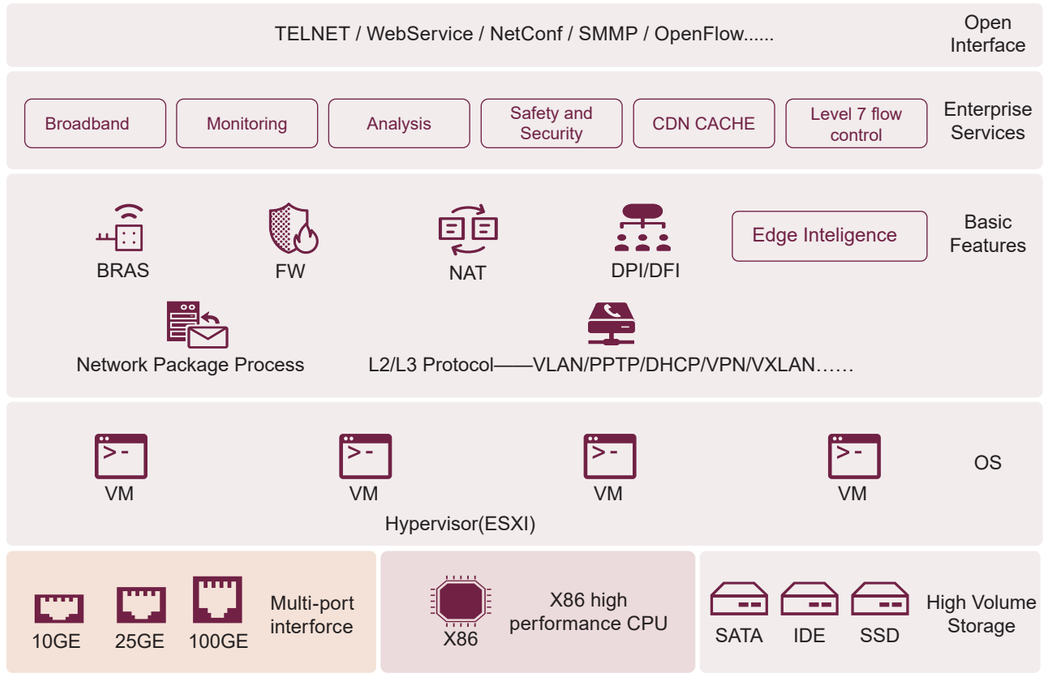
SINE deploys at the network access side. It supports intelligent edge access to realize user authentication, network interoperability, data analysis, data storage, edge computing, and other functions. A typical deployment is as below:



3.1 SOLUTION BLOCK DIAGRAM

SINE is developed and deployed on the industry's standard x86 architecture for system flexibility. GreeNet's patented software solution of the network protocol stack, visibility engine and analytics subsystems are developed on open standard operating systems.

The overall software architecture is as below:



SINE's unique features are:

1. Zero copy technology to optimize the IP protocol stacks to reduce network driver's workload. (Diagram 1)
2. Direct memory read-write for forwarding traffic. Reduce CPU cycle by 90%
3. Dynamic and strategic data mapping to reduce system resources (Diagram 2)
4. Improve forwarding strategy with FIFO priority queue algorithm (Diagram 3)
5. Rule-based intelligent matching engine (RME) to enhance the detection and filtering rules (Table 1)

Diagram 1 Zero Copy Methodology

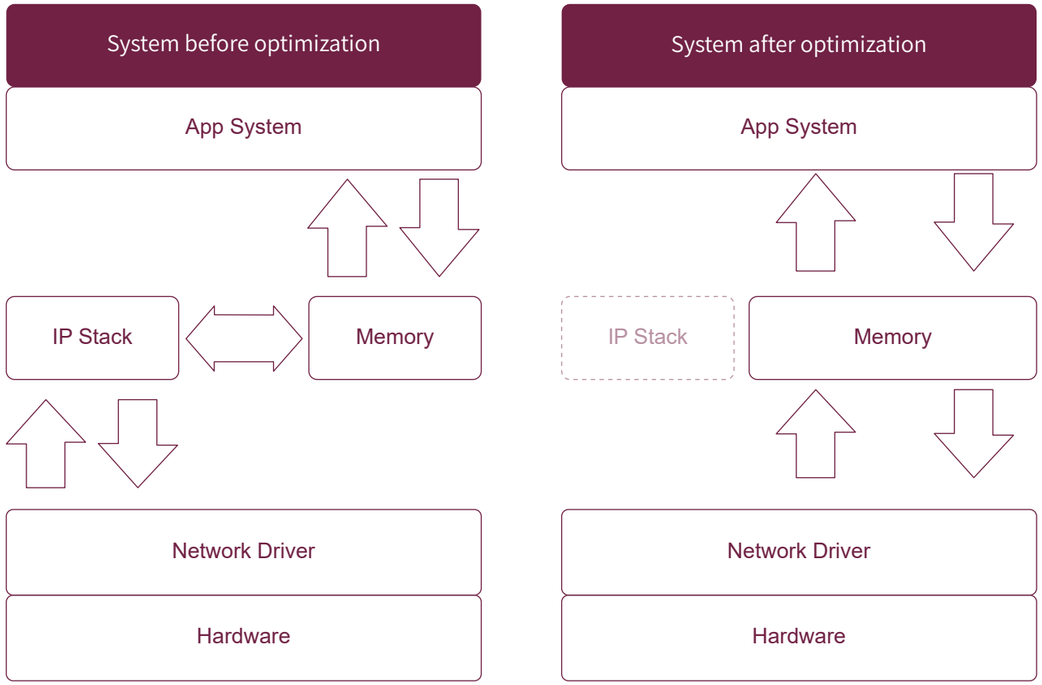
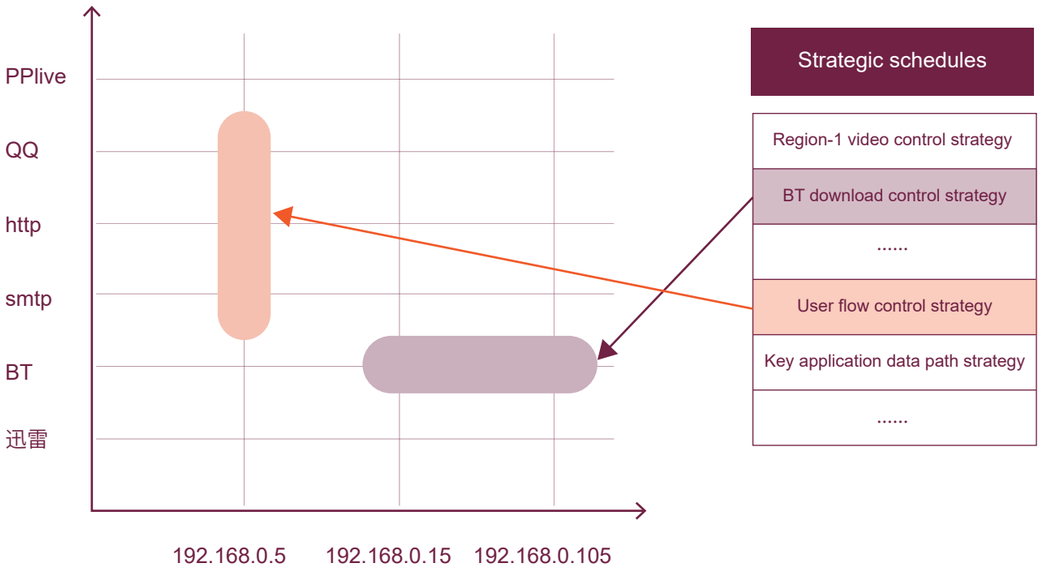
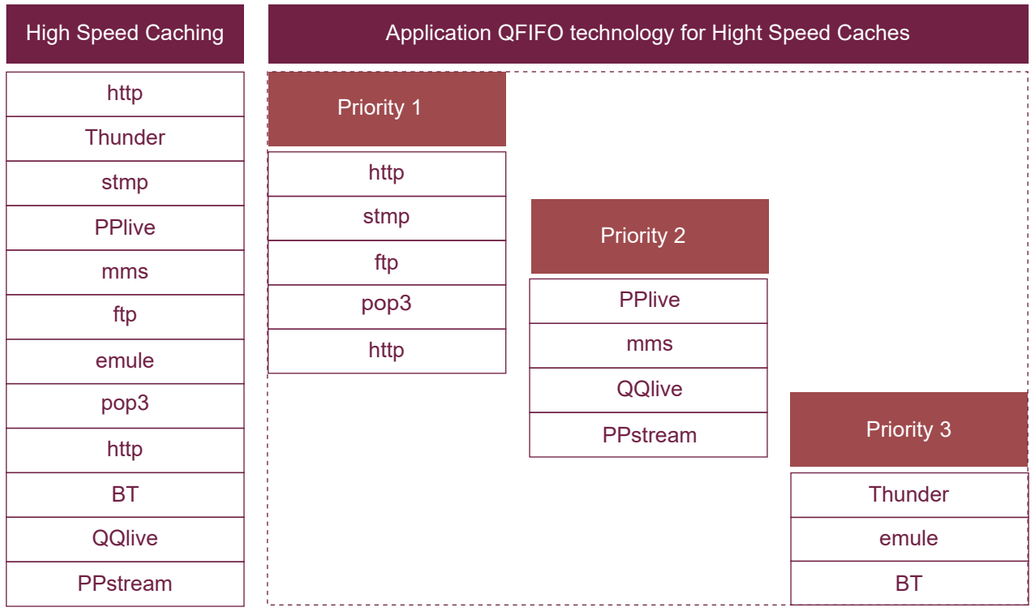


Diagram 2 Dynamic Data Mapping



Super Intelligent Network Element White Paper——System Architecture

Diagram 3: SINE optimizes the caching queue, divides the original simple single queue into multiple priorities of the same type. High bandwidth applications such as webpage loading, real-time application, video, and online games are set to the high-priority queue. Network data received by SINE are processed according to their queue priority.



Rule-Based Intelligent Matching Engine (RME)

In traditional DPI technology, the detection or filtering rules are all in the form of plain text. A rule in the form of a text is a character string representing a type of harmful data packet or a characteristic character contained in an application protocol. However, due to the sharp increase in the types of unhealthy data packets or the update of application software versions and the generation of a large number of variants, this plain text filtering rule has been unable to adapt to the new network environment. Need more flexible and universal rule syntax to support matching, RME (Rule Matching Engine) rule matching engine came into being

The RME is a set of matching rule using DPI algorithm that provides the following key capabilities:

1. Compatible with Wireshark packet analyzer for ease of use
2. Using C-style structural data set for easy creation of rule-based description
3. Configurable and scalable expansion
4. Multiple protocols support such as HTTP, HTTPS, RTP, FTP,H.323 and MGCP and its parameters and functions
5. Support PCRE regular expression. It can also achieve sophisticated string matching

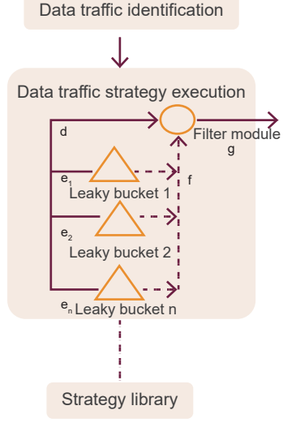
3.2 BUSINESS FUNCTION ORCHESTRATION

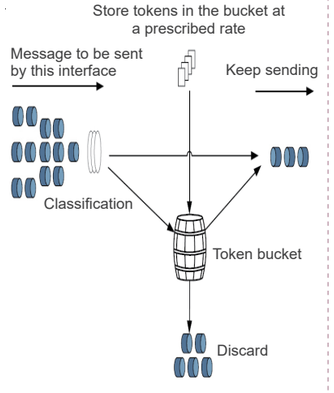
SINE is designed and developed with modular architecture. It provides both modular integration and flexible plug-in design from traditional access device features, DPI business rules to complex but rich software functions that give great flexibility for software development to meet the constant changes of market demands.

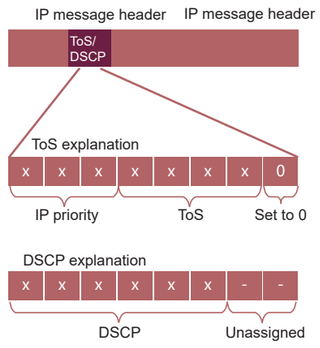
3.2.1 MESSAGE CONTROL TECHNOLOGY

SINE uses protocol identification to capture and manage all key data from the network, such as user information, time of use, bandwidth, historical traffic. The management method includes normal forwarding, blocking, limiting bandwidth, shaping, and remarking priority.

Filtering Packet Loss	Speed Limited	Priority Mark
• Use DPI to build the flow mechanism • Use filtering bucket to determine the flow logic • Use Filtering logic to determine the priority	• Use DPI to set max speed limited per link • Set upper limit • Use token to determine the flow speed at a given time	• Use DPI to set priority, transfer capability • Achieve QoS with priority strategy







SINE's flow control achieves the followings:

1.Packet Loss Filtering

a.Inline DPI filtering rules engine to deposit packets with different criteria into different buckets

2.Limiting throughput speed

a.Inline DPI engine to control bandwidth and guarantee throughputs

3.Prioritization

a.Inline DPI engine to set flow priority and optimize performance to achieve QoS

MAIN BUSINESS FUNCTION

SINE integrates modular designs of edge access, edge computing, edge storage, and DPI technology to build solutions that the market needs. Because of the modular design structure, new and enhanced applications can be developed with the minimal development effort.

4.1 NETWORK FEATURES

The following are the key features and protocol support by SINE:

Features	Description
Certification	• PPPoE authentication • Web Portal authentication • Direct connection (no authentication) • Record authentication logs, including online, Offline, and authentication failure logs

Features	Description
Billing	• RADIUS • Diameter • No billing
Authorization	• bandwidth • Time to allow network access
Access	• VLAN/QinQ/PPPoE/DHCP • DHCP Server • DHCP Relay • Captive Portal
Routing	• IPv4, IPv6 • Static routing • RIP • OSPF • ISIS • BGP • Policy routing • Application routing • IGMP • PIM-SM, PIM-SSM • RPF • ECMP
VPN	• BGP MPLS L3VPN • VPDN • local VPN • VXLAN
Traffic control	• user-based speed limit • speed limit based on three layers • application-based speed limit
Load balancing	• Load balancing based on physical ports

Features	Description
Firewall	• ACL • VLAN ACL • System ACL • uRPF • Stateful ACL • ACL hit count • Static ARP • Proxy ARP
Attack protection	• Anti-virus DoS / DDoS attacks, ARP spoofing attacks
Network monitoring	• Viewing interface bandwidth usage • viewing bandwidth usage history
Equipment Network Management	• stand-alone WEB network management • business configuration function • system parameter configuration
Deployment mode	• mixed access methods such as bypass, bridge, routing, NAT, etc.

4.2 DPI AND COMPLIANCE INSPECTION

SINE has its regulatory compliance solution. It includes the following functions:

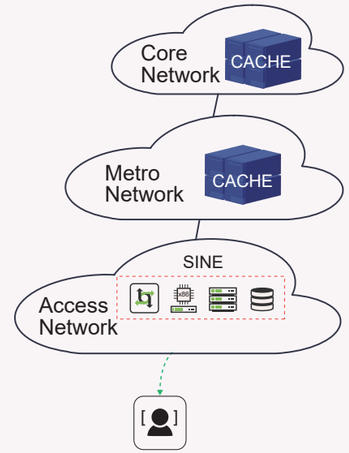
Features	Description
DPI function	• flow control, blocking, monitoring, mirroring • blocking, monitoring, access log • statistics-level data reporting (general traffic statistics, traffic flow direction, website access analysis) • session-level data reporting (XDR bill, HTTP GET log), file restoration

Features	Description
Online user behavior audit	• retain user registration information • record and retain log between user's Internet and intranet network addresses used
User behavior management	• user's online time, terminal, phone number, website access, online search, etc. • analysis of user's activities since online • support URL blacklist
Shared Detection	• able to identify the user terminal type, including browser, operating system, mobile phone model, pad model • Support real-time monitoring of users' Internet access • illegal user's detection and control
Log retention	• Retain log for WLAN user and home broadband user's online behavior such as online and offline access logs, retention, query, and reporting
Anti-Malware Monitoring and disposal	• Control and management of illegal web content such as unlawful propaganda • Anti-malware analysis and statistic management • Support both local signature and online databases • Configurable to update and upgrade automatically • Support self-defined detection rules and display monitoring results

4.3 CONTENT ACCELERATION

Video traffic continues to consume more than 80% of all internet traffic. And at the same time, the user continues to demand higher video quality after coming from HD to 4K and now 8K videos. The Caching system is not more a viable solution because of his it's cost and deployment difficulties. One of GreeNet's SINE functions is to provide caching at the network side that can be activated to use a different part of the network. By doing so, it will reduce the total cost and increase the overall video performance. This will give a better QoE for VIP users who demand the highest video quality.

SINE Caching function to determine CDN Cache Sinks

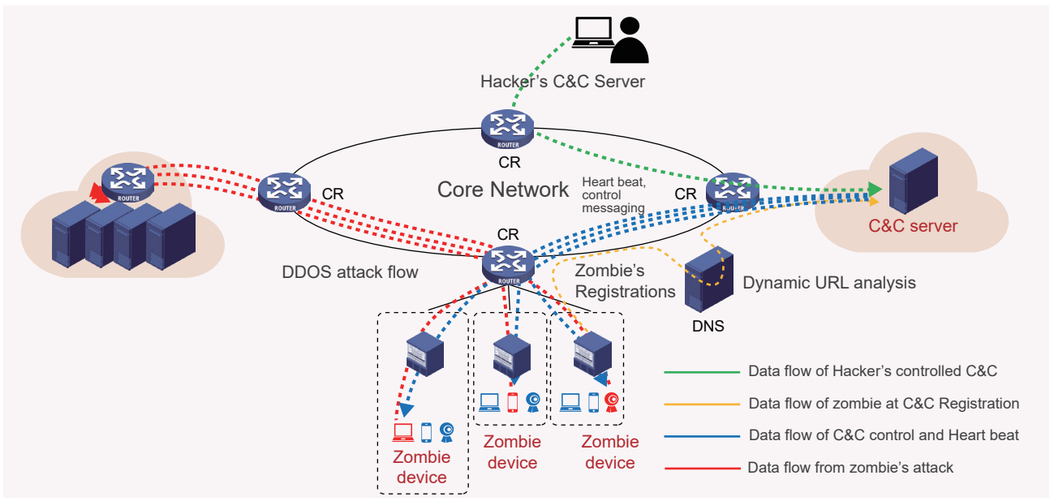


1.Sink cache node, to determine user awareness issue
2.Reduce bandwidth pressure from the core network
3.Unify network elements with Cache equipment to remove duplicated setups

4.4 DDOS NEAR-SOURCE SUPPRESSION

The typical DDoS defense strategy in the industry is near-end cleaning. That is, deploying cleaning equipment is in a network location closed to the destination, and it cleans troubled traffic before reaching the destination. One of the critical disadvantages is that the concerned traffic consumes a lot of network bandwidth and system resources before it is cleaned.

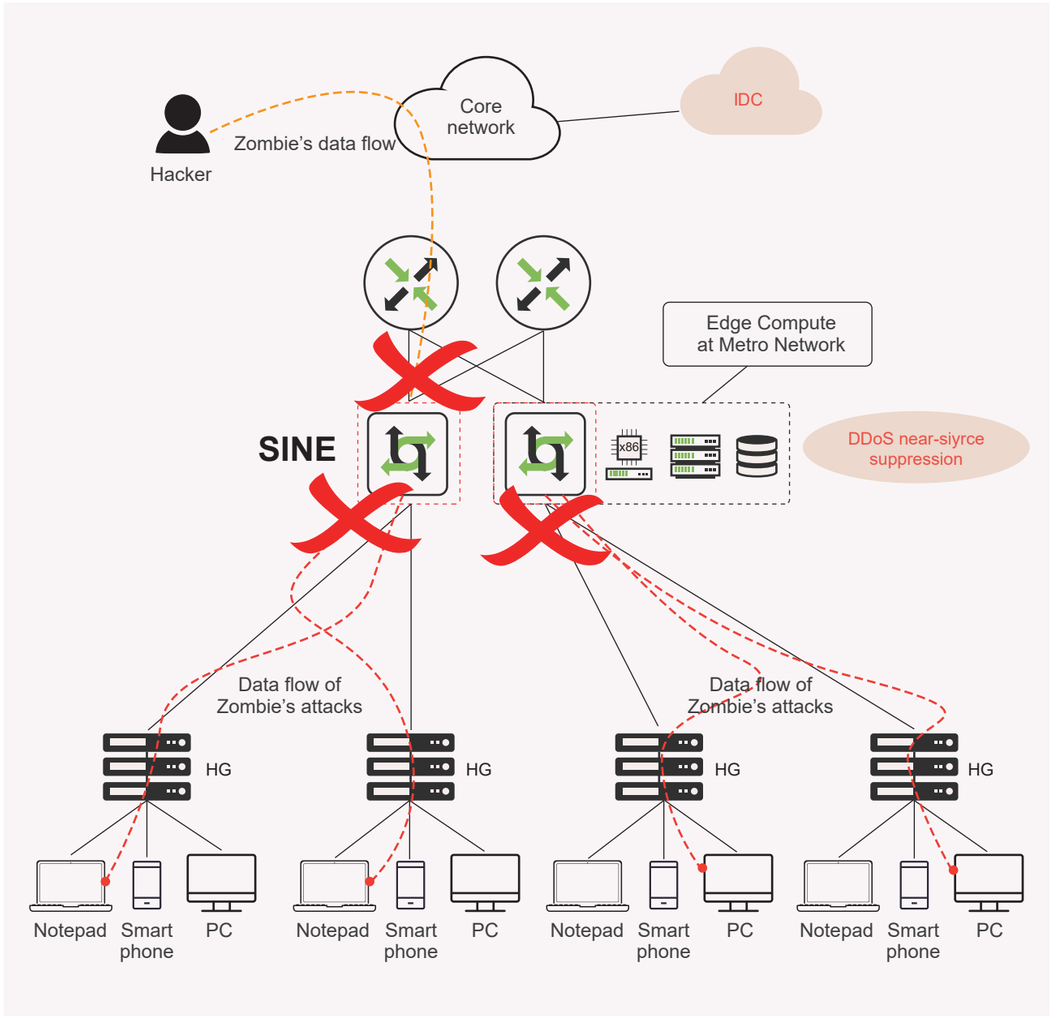
The principle of BOT infection and DDoS attack is shown in the following figure:



By taking advantage of large scale deployment at all the key gateway links in the network, SINE can integrate any DDoS detection subsystem (our own or any 3rd party) to achieve DDoS near-source suppression. It will not only reduce network resources earlier but also improve the resilience against any attack. The specific implementation method is as follows:

1. Use SINE's DPI technology to detect hacker-controlled C & C data flow characteristics, broiler-to-C & C registration data flow characteristics, C & C command issuance, and heartbeat link data flow characteristics.
2. Identify network abnormal behavior to filter attacked traffic.

The deployment method is shown below：



4.5 VALUE-ADDED SERVICES

SINE supports the rapid response to the following value-added services:

Value-added services	Description
Application acceleration	• protocol proxy to reduce application interaction process • stream cache to speed up service access
IPTV service	• BRAS function to provide user access and authentication • Support multicasting
VPN service	• Support L3VPN, VxLan, and other technologies to handle traffic for dedicated users.
Sponsor packages	• Support sponsored data usage management
Self-Provisioning	• Support self-managed user registration, login, view, and choose a package to use

5 PRODUCT ADVANTAGES

5.1 PRODUCT ADVANTAGES

Unlike traditional BRAS and other access devices, SINE chooses the "intelligent core" approach. Therefore an unified interface is developed to connect all subsystems and modules, although they are inhouse development or third-party subsystems. As a result, the upper layer business applications can be built, enhanced, adjusted and integrated without much new development. It will shorten the overall new product development time and launch effort.

6 TYPICAL USE CASE

6.1 BRAS SOLUTION FOR AN OPERATING COMPANY

6.1.1 BACKGROUND

Traditional BRAS carries only user access data, but not the corresponding data for analysis. Conventional DPI products have data collection and analysis capability, but they don't transmit user access data. To deploy these two products in the same network can be complicated and expensive.

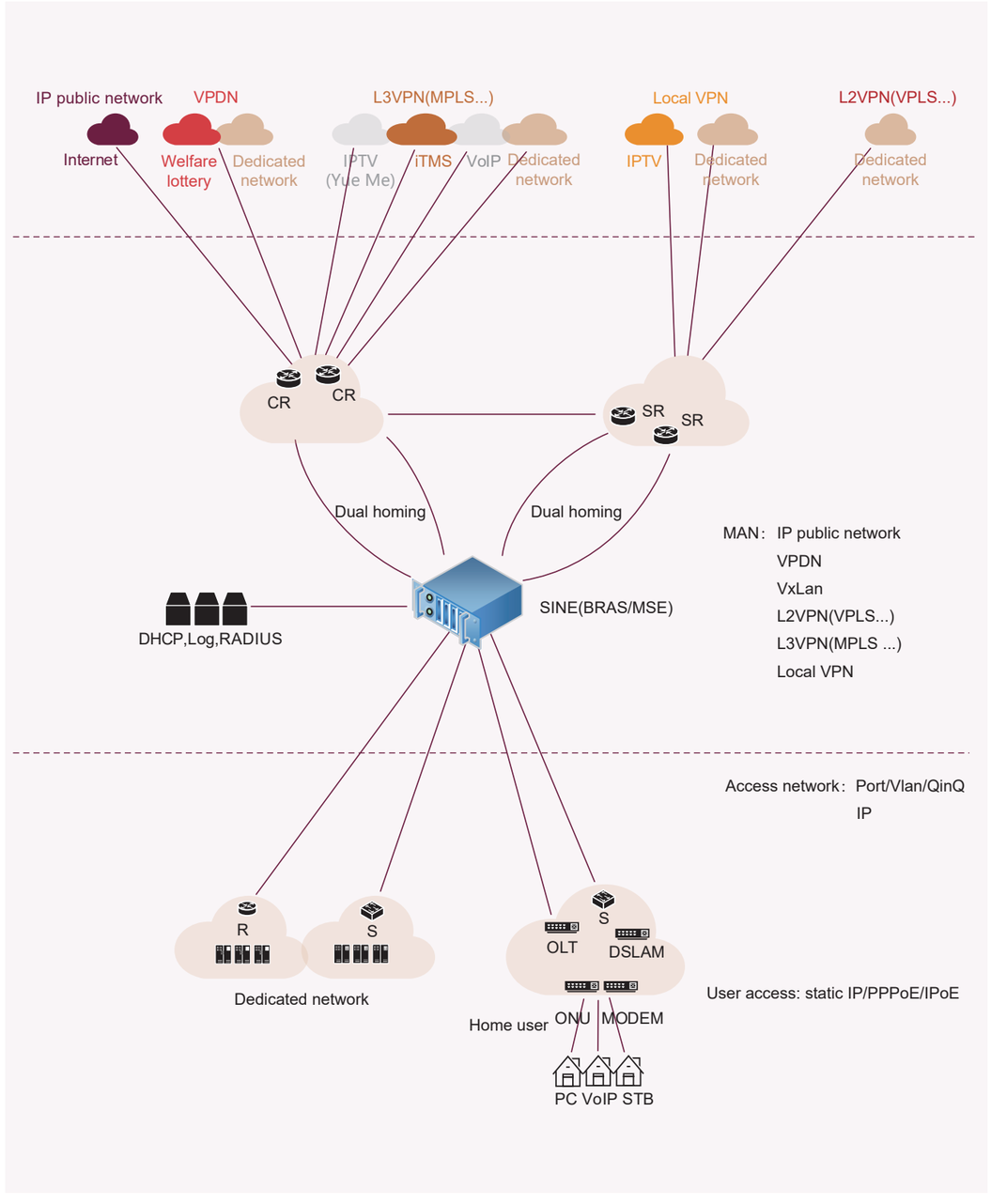
SINE is developed to combine these two functions in a single platform that carries not only the basic PPPoE user and AAA data, but also network visibility and analytics data. SINE implements and supports the following business functions:

- dynamic NAT, which can effectively improve address utilization;
- QinQ, enhance the scalability of VLAN and unique user identification;
- multi-link bundling, which improves bandwidth and redundancy;
- ACL for application-level control;
- policy-based QoS marking to distinguish contract and no-contract traffic;
- hierarchical bandwidth management, which can realize a reasonable mapping between business and bandwidth;
- OSPF to achieve agile infrastructure routing delivery;
- BGP to realize highly scalable user routing bearer;
- BGP / MPLS VPN to realize private network interconnection service;
- multicast technology to better support IPTV service forwarding;
- multicast VPN to realize multicast service in a private network;
- the conversion of multicast to unicast, taking into account the bandwidth saving and user experience;
- Change Over Acknowledge (COA) to provide intelligent speed-up services;
- correlates user info collected from multi-system to provide real-time renewal reminder;

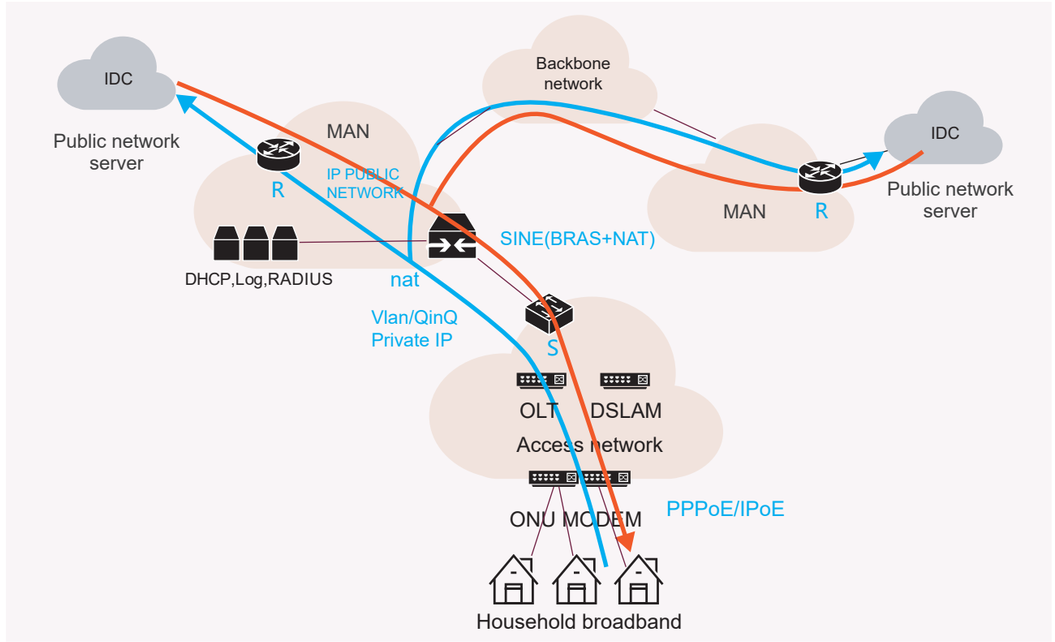
6.1.2 SOLUTION

SINE is deployed at the network access points. It is not only to provide the broadband access service, but also collect relevant traffic information for each user.

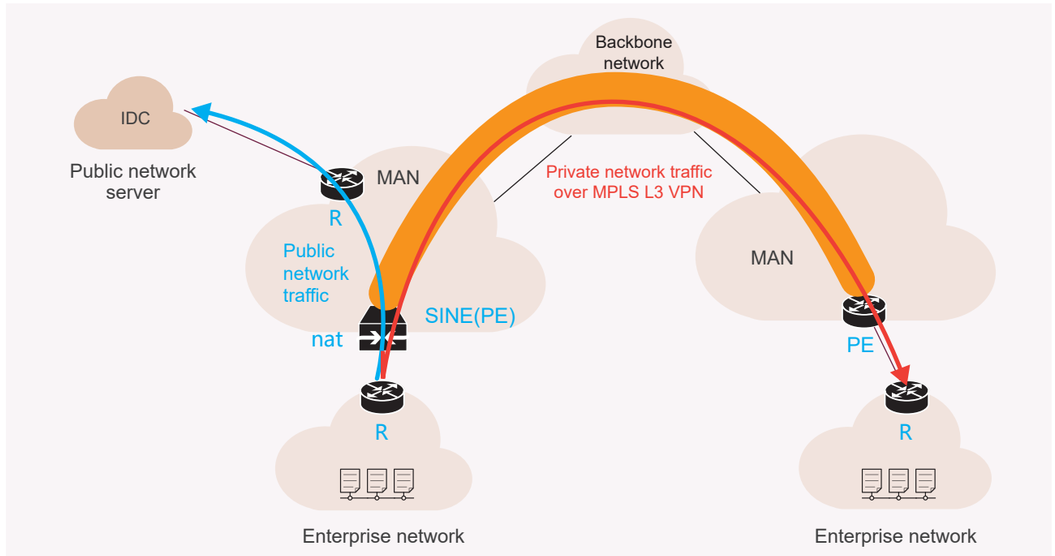
The overall deployment topology is shown below:



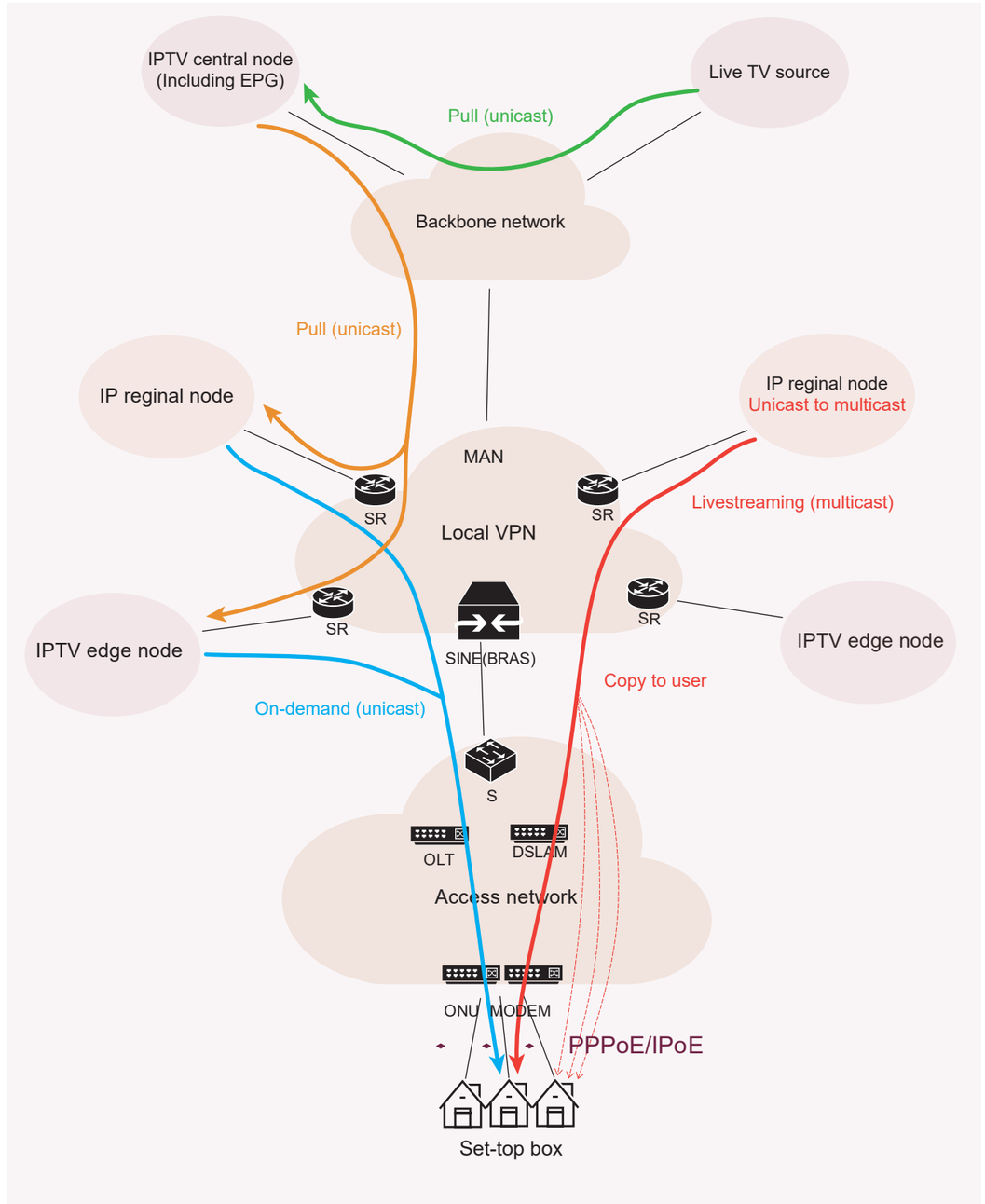
After authentication, authorization, and successful connection through PPPoE, the home broadband user's private address is converted to a public network address on SINE before the user can access the Internet, as shown below:



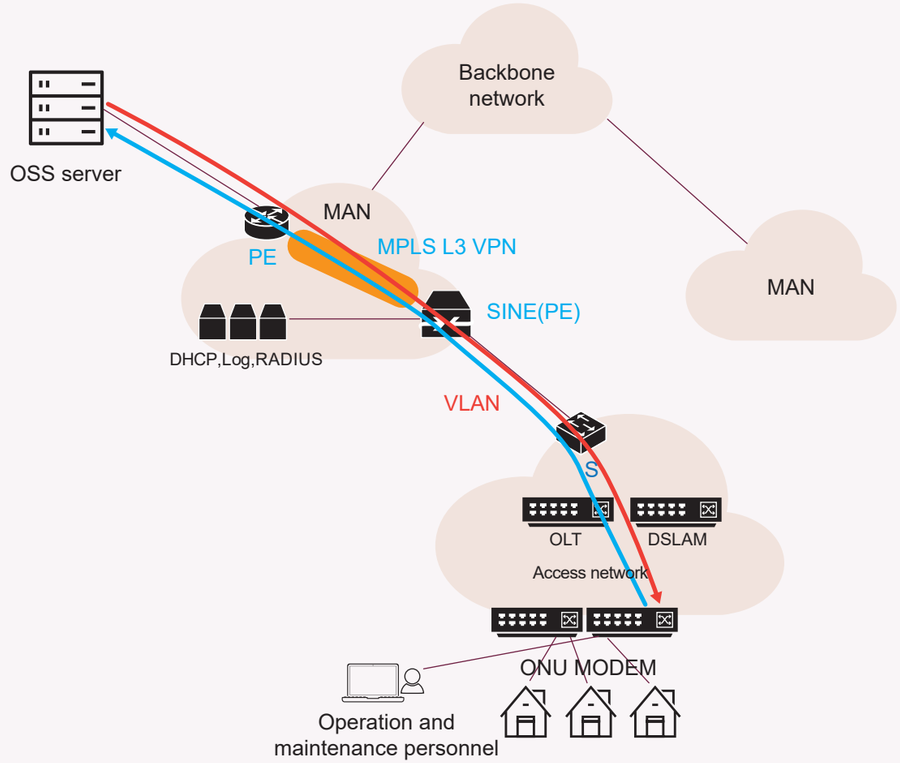
Users from a private network (at the same time, there is a need to access the public network) can achieve multi-branch interconnection through BGP / MPLS VPN. Also, they can access Internet through the local Breakout method, as shown below:



For IPTV, unicast and multicast are the technology used to provide on-demand and live broadcast services, respectively. The IPTV central node imports and stores video streams from live TV sources, whereas the IPTV regional center stores video streams to provide on-demand services. From live video to IPTV, protocol conversion is required. The overall business logic is as shown below:



The management of network elements, such as iTMS, uses a logical out-of-band MPLS VPN to separate its services from the public network services. As a result, it reduces unnecessary resources for NAT, that simplifies two-way communications, as shown below:



6.2 CAMPUS ACCESS SOLUTIONS

6.2.1 BACKGROUND

In a typical school environment, network equipment is provided by different vendors, which caused many maintenance issues from server accessibility to network abnormality. To address the issue, GreeNet provides the following resolutions:

- simplify the PPPOE authentication process, and achieve end-to-end network control with active network traceability to locate weak spot.
- Use SINE to separate the Internet and intranet access. At the time when internet access fails, the intranet will continue to provide accessibility to all resources within the campus.
- Design a new campus network with full SINE capability, as explained in the diagram below.

6.2.2 SOLUTION