

Wi-Fi Access Gateway (WAG)



End users have high expectations these days when it comes to WiFi. In response, WiFi networks need to become more sophisticated in subscriber management and control, security, mobility, and quality of experience capabilities. To address these needs in a simple, unified, consistent manner across the WiFi network, businesses use a WiFi Access Gateway (WAG). A WAG also enables the use of cost-effective WiFi Access Points (APs) or multi-vendor WiFi networks without having to compromise on functionality.

Benu Networks' WAG is used in a variety of deployment uses cases including Public / Community WiFi, Mobile Network Offload, Smart Cities, Venue WiFi, Hospitality WiFi, Multi-Dwelling Units (MDU). All of these environments have a common theme: a large volume of guest WiFi users. While enterprise WiFi solutions primarily serve the needs of employees, they are not well-suited for serving large guest WiFi populations. The Benu WAG provides the market-leading solution for WiFi networks that have a large number of guest users as well as a diverse user base of employees, partners, and IoT devices.

Benu's WAG simplifies:

- Distributed WiFi networks in multiple physical locations
- Networks that require enhanced security
- Administration of subscriber policies
- Multi-vendor WiFi networks

The Benu WAG solution provides a rich feature set that adds to WiFi network capabilities and simplifies overall management:

- Multi-vendor WiFi aggregation via GRE, L2TPv3, or VLANs from the CPE/WiFi access points
- AAA proxy and load-balancing
- Policy enforcement per access point, per VLAN, or per subscriber
- Access controls and advanced Quality of Service (QoS)
- Best-in-class mobility for guest WiFi users
- Application and service steering
- Scalable routing
- Carrier-grade NAT and stateful firewall
- High-scale DHCP server
- Full IPv6 support and variety of dual IPv4/IPv6 combinations
- Content filtering and malware/phishing protection
- Service function chaining
- Lawful intercept support
- Analytics and statistics

Key Highlights

Guest users and IoT create unique challenges for WiFi networks. Benu Network's WiFi Access Gateway takes your WiFi solution to the next level:

Enhance Guest Experience

- Flexible authentication and authorization schemes
- Seamless mobility, fast and at-scale

Improve Security

- Network micro-segmentation
- Guest portal and walled garden protections
- Policies for connected but unauthorized users
- Denial-of-service prevention
- Firewall and content filtering
- Malware and phishing protection

Reduce Costs

- Consolidate subscriber gateway, DHCP, router, and firewall functions
- Simplified and centralized policy enforcement
- Unified and consolidated analytics

Bandwidth management

- Flexible traffic intelligence and Hierarchical QoS support
- Consistent per application, per user, per group performance

Avoid Proprietary Lock-in

- Use any vendor WiFi
- Standards-based open interfaces

Data Sheet | Wi-Fi Access Gateway

Use Cases

Benu Networks' WAG is used in a variety of deployment uses cases:

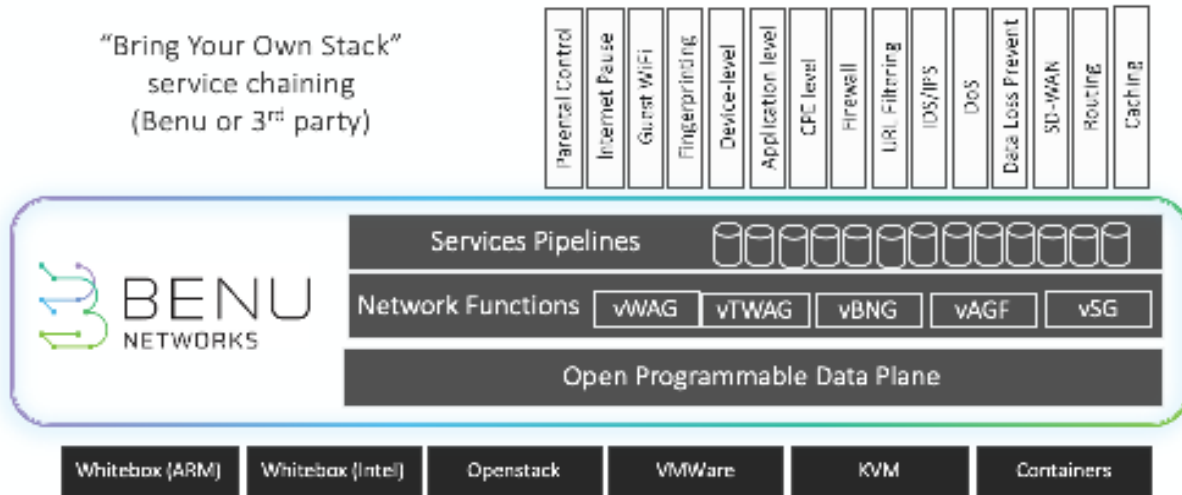
USE CASE	DESCRIPTION	BENEFITS
Public / Community WiFi	Service providers provide a WiFi hotspot network across existing home, business, and/or outdoor WiFi networks	<ul style="list-style-type: none"> • <i>Builds brand</i>: users see operator's SSID everywhere • <i>Increases subscriber retention</i>: subscribers benefit from easy, free out-of-home WiFi access • <i>Easy upsell to managed networks services</i>: guest WiFi, network security, LTE backup, etc
Mobile Network Offload	3GPP cellular network operators can offload mobile traffic to WiFi networks while maintaining subscriber visibility and management	<ul style="list-style-type: none"> • <i>Fill in coverage gaps</i>: particularly inside buildings • <i>Reduce network load</i>: improves subscriber network speeds
Smart Cities	Cities use WiFi to support Internet-of-Things (IoT) monitoring and automation related to utility billing, traffic, parking, public transport, public safety, and street lighting.	<ul style="list-style-type: none"> • <i>Reduces operations costs</i>: increased automation • <i>Improves constituent satisfaction</i>: more efficient delivery of city services • <i>Green</i>: reduces waste in transportation costs
Venue WiFi	Provide critical amenity for convention centers, stadiums, shopping malls, airports and train stations	<ul style="list-style-type: none"> • Improves customer satisfaction • <i>Reduces operations costs</i>: support IoT for automation • <i>Revenue opportunities</i>: enable commerce opportunities, location-based services, and sponsored WiFi opportunities
Hospitality WiFi	Consistent WiFi services in rooms, common areas, meeting rooms, and ballrooms.	<ul style="list-style-type: none"> • Improves customer satisfaction and retention • <i>Reduces operations costs</i>: support IoT for automation • <i>Revenue opportunities</i>: upsell enhanced broadband Internet support
Multi-Dwelling Units (MDU)	Apartment complexes, retirement homes, university housing, and military housing all need support for tenant WiFi, guest WiFi, staff WiFi, and often IoT.	<ul style="list-style-type: none"> • <i>Support wide user base</i>: create separate "networks" on single physical WiFi infrastructure • <i>Control and visibility of individual subscribers</i>: don't treat the MDU as just one large wholesale subscriber • <i>Improve tenant satisfaction</i>: seamless WiFi mobility and services • <i>Reduce operational costs</i>: IoT for automation

Data Sheet | Wi-Fi Access Gateway

Features

Service Function Chaining (SFC)

Benu Networks has a flexible traffic intelligence and service steering architecture that supports dynamic service chaining for value added services. This capability allows flexible provisioning of multiple services as well as the most efficient scaling of the service plane since only the required application servers are inserted in the path of IP flows, resulting in the conservation of application server resources as well as the minimization of latency.



In addition, the Benu Platform has privileged access to subscription policies and operator policies regarding services, and generates the necessary meta-data header. Network service headers (NSH) carrying policy information and device identification simplify integration of application servers (aka service functions) since it eliminates the need for the complex integration of a service provider's OSS/BSS middleware with standalone service functions in the data center, or in many cases, 3rd party software-as-a-service (SaaS) clouds. For a flexible orchestration of services, the Benu Platform architecture supports SFC provisioning interfaces via REST API. For realizing service paths towards service functions, the platform offers L2/L3 service overlays using VXLAN and NSH.

Features

Gateway Support

Business Access Gateway (BAG)
Trusted Business Access Gateway (TBAG)
WiFi Access Gateway (WAG)
Trusted WiFi Access Gateway (TWAG)

Tunnel Connectivity

GREv2, GRE over UDP
L2TPv3, L2TPv3 over IP, L2TPv3 over UDP
GRE over IPsec and IKEv2
VLAN as a Tunnel (Subscriber VLANs)
Mobile Offload S2A, Gn (GTPv1-U, GTPv1-C, GTPv2-C)

Authentication, Authorization, and Accounting (AAA)

RADIUS AAA client support
RADIUS accounting
EAP authenticator
EAP-AKA, EAP-SIM
802.1x
RADIUS AAA server groups
RADIUS AAA load balancing or primary/secondary scheduling
RADIUS custom dictionaries and VSAs

Management

CLI, Telnet, SSH
SNMPv1, v2c, v3; 400+ MIBs
FTP, TFTP, SFTP, FTP Client/Server
PING, traceroute, MTU Settings
Management ACLs
NTP
Syslog

High Availability

N+1 active / active, active / standby

VRRP (for Layer 2 networks)
BGP Anycast (for Layer 3 networks)
802.1ad Link Aggregation
Link Aggregation Group (LAG)
VLAN over LAG

Quality of Service (QoS) and Bandwidth Management

Rate Limiting (Subscriber/Device, VLAN, Tunnel)
DSCP classification and marking
802.1p classification
Queue Scheduling (Weighted Round Robin, and Strict Priority)
Hierarchical QoS

IP Addressing and IP Features

DHCP v4/v6 server
IPv4, IPv6, and dual stack
IPv4/v6 block fragmented packets
DNS v4/v6 Client/Resolver
DNS Server v4/v6 Options
DNS Bridge

L2/L3 Routing

Static
BGP
OSPFv4
IS-IS
MPLS
MPLS: BGP Add Path
BFD
Equal Cost Multi Path (ECMP)
Route Maps
1 Million IPv4 Routes
ARP

IP v4/v6 fragmentation handling
Static IP on CPE (B2B static IP)
L3VPN with B2B static IP

Security

VLANs
Standard & Extended ACLs, IPv4/v6
ACLs per port, per subscriber, per tunnel, per tunnel VLAN
IPv4 Firewall
Carrier-grade NAT (CGNAT)
CGNAT Port Block In-Use Syslog/
SNMP Alarm Threshold
FQDN DNS ACLs
Wildcard DNS ACLs
Tunnel Broadcast Prevention
Control plane DoS protection
Data plane DoS protection
Parental Controls
Content Filtering
Malware & Phishing Protection
Legal Intercept
Subscriber mirroring
WiFi AP mirroring

Guest User Services

Captive portal redirect
HTTP Enrichment
Splash page
Walled garden services
Guest user mobility
Un-auth and authorized user policies

Analytics

SNMP MIB stats
Port and VLAN utilization metrics
Subscriber Session Analytics (SSA)
Benu Operations Subscriber Simulator (BOSS) for performance monitoring

Data Sheet | Wi-Fi Access Gateway

Benu Networks WAG Product Portfolio

Within the WAG family of products, Benu has three solutions. The Business Access Gateway (BAG) and Trusted Business Access Gateway (TBAG) are low-scale versions of the WAG and TWAG with low starting entry price points. The BAG (or TBAG) is primarily for gateways up to 14Gbps bandwidth and 1000 tunnels, but licensing does allow for higher capacities. The WiFi Access Gateway (WAG) provides high scale at a cost-effective price point. Finally, the Trusted WAG (TWAG) is specifically for Mobile Network Offload (such as Hotspot 2.0) services.

PRODUCT	APPLIANCES	VIRTUAL SOFTWARE
BAG	xMEG-1	vMEG-SI 10K
TBAG	xMEG-1	vMEG-SI 10K
WAG	xMEG-10, xMEG-100, xMEG-200	vMEG
TWAG	xMEG-10, xMEG-100, xMEG-200	vMEG

The xMEG appliance solutions come at different scaling capacities ranging from 1 Gbps to 200 Gbps. All Benu products have software licensing based on the scale of deployment, enabling small deployments to pay less, and large deployments to benefit from economies of scale.

CAPACITY	x M E G - 1	x M E G - 10	x M E G - 100	x M E G - 200
Throughput (Mpps)	1.6	5	35	48
Throughput (Gbps)	14	40	100	200
Tunnels	1,000	100,000	1,000,000	1,000,000
CADs	20,000	100,000	1,000,000	1,000,000
CGNAT	10,000,000	50,000,000	512,000,000	512,000,000
ACLs (port or subscriber)	512	16,000	16,000	16,000
Rate limiting policies	21,000	200,000	2,000,000	2,000,000
DHCP transactions/sec	160	800	4000	4000
RADIUS transactions/sec	320	1600	24000	24000



Ordering Information

Business Access Gateway (BAG) & Trusted Business Access Gateway (TBAG)

CONFIGURATION	OPTIONS	PART NUMBER
Choose hardware (if desired)	xMEG-1 6x1GE and 2x10GE SFP+, AC Power	980-0080
Choose Standard Image (SI) OS	x/vMEG-SI 10K OS License	700-1210
Choose product type: BAG, TBAG or both	BAG Service - RTU	700-2600
	TBAG Service - RTU	700-2615
Choose capacity in 3 dimensions: <ul style="list-style-type: none"> Bandwidth Access Tunnels Concurrent Active Devices (CADs) 	BAG Bandwidth Capacity License 1G	700-1232
	BAG Bandwidth Capacity License 10G	700-1234
	BAG sGRE Tunnels 50	700-2620
	BAG sGRE Tunnels 1K	700-2603
	BAG sGRE Tunnels 10K	700-2604
	BAG L2TPv3 Tunnels 50	700-2621
	BAG L2TPv3 Tunnels 1K	700-2608
	BAG L2TPv3 Tunnels 10K	700-2609
	BAG CAD 250 devices	700-2622
	BAG CAD 1K devices	700-2605
	BAG CAD 10K devices	700-2606
BAG only: Firewall capacity (recommend 512 flows per CAD)	BAG 100K CGNAT Flows and Firewall	700-2601
	BAG 1M CGNAT Flows and Firewall	700-2602
	BAG 10M CGNAT Flows and Firewall	700-2607
TBAG only: Mobile core tunnel capacity (1 per CAD)	TBAG S2a 1,000 SAU License	700-2610
	TBAG S2a 10,000 SAU License	700-2611
Optional advanced security	Content Filtering 250 CAD, annual	710-1553
	Malware/Phishing Protection 250 CAD, annual	710-1554
	Content Filtering 1K CAD, annual	710-1555
	Malware/Phishing Protection 1K CAD, annual	710-1556
Optional optical transceivers (SFP+)	10GBASE-SR 300; SFP+	921-0023
	10GBASE-LR; SFP+	921-0024

Data Sheet | Wi-Fi Access Gateway

Wi-Fi Access Gateway (WAG) & Trusted Wi-Fi Access Gateway (TWAG)

CONFIGURATION	OPTIONS	PART NUMBER
Choose hardware (if desired)	xMEG-10 4x10 SFP+, AC Power	980-1001
	xMEG-10 4x10 SFP+, DC Power	980-1002
	xMEG-100 8x10GE SFP+, AC Power	980-1019
	xMEG-100 8x10GE SFP+, DC Power	980-1020
	xMEG-100, 2x100GE QSFP28, AC Power	980-1021
	xMEG-100, 2x100GE QSFP28, DC Power	980-1022
	xMEG-200, 4x100GE QSFP28, AC Power	980-1040
	xMEG-200, 4x100GE QSFP28, DC Power	980-1041
Choose optical transceivers (SFP+, QSFP28)	10GBASE-SR 300; SFP+	921-0023
	10GBASE-LR; SFP+	921-0024
	100GBASE-LR4; QSFP28	921-0016
	100GBASE-SR4; QSFP28	921-0009
Choose base OS: xMEG appliance or virtualized vMEG	xMEG-10 OS	700-1230
	xMEG-100 OS	700-1231
	vMEG-OS: 8-core or less	700-1340
	vMEG-OS: Over 8-core, under 48 core	700-1342
	vMEG-OS: Over 48 core	700-1344
Choose product type: WAG, TWAG or both	WAG Service - RTU	700-2400
	TWAG Service - RTU	700-2415
Choose capacity in 3 dimensions: <ul style="list-style-type: none"> • Bandwidth • Access Tunnels • Concurrent Active Devices (CADs) 	WAG Bandwidth Capacity License 1G	700-1232
	WAG Bandwidth Capacity License 10G	700-1233
	WAG sGRE 1,000 Tunnels	700-2403
	WAG sGRE 10,000 Tunnels	700-2404
	WAG sL2TPv3 1,000 Tunnels	700-2408
	WAG sL2TPv3 10,000 Tunnels	700-2409
	WAG CAD 1,000 Sessions	700-2405
	WAG CAD 10,000 Sessions	700-2406
WAG only: Firewall capacity (recommend 512 flows per CAD)	WAG 1 Million CG-NAT Flows - xMEG/vMEG	700-2401
	WAG 10 Million CG-NAT Flows - xMEG/vMEG	700-2402
TWAG only: Mobile core tunnel capacity (1 per CAD)	TWAG S2a 1,000 SAU License xMEG/vMEG	700-2410
	TWAG S2a 10,000 SAU License - xMEG/vMEG	700-2411
Optional advanced security	Content Filtering 250 CAD, annual	710-1553
	Malware/Phishing Protection 250 CAD, annual	710-1554
	Content Filtering 1K CAD, annual	710-1555
	Malware/Phishing Protection 1K CAD, annual	710-1556

Data Sheet | Wi-Fi Access Gateway

Related Products & Services Ordering Information

CONFIGURATION	OPTIONS	PART NUMBER
Benu Operations Subscriber Simulator (BOSS) for subscriber performance monitoring	BOSS Controller	710-1760
	BOSS - 1 simulated session	710-1761
	BOSS - 50 simulated sessions	710-1762
	BOSS - 100 simulated sessions	710-1763
Subscriber Session Analytics (SSA)	SSA - Analytics Module	710-1460
	Analytics CAD 1K sessions	710-1461
Support & Services	Benu Provider Plus	610-0002
	Benu Provider Plus - 3yr	610-0006
	Benu Provider Plus - 5yr	610-0010
	Onsite Implementation Services, per Day	620-0001
	Remote consulting services	620-0003
	Onsite config and ops training course up to 8 students***	630-0002

About Benu Networks

Benu Networks is a leading software and solutions provider, simplifying the industry's most complex edge networks. With a comprehensive set of products and innovative solutions, Benu Networks delivers solutions to instantly transform legacy networks, elastically manage services, and carve the path to 5G.

Data Sheet | Wi-Fi Access Gateway

CATEGORY	WIFI DEPLOYMENT CHALLENGES	BENU WAG SOLUTION	APPLICABLE SOLUTION	USER BASE
Mobility	Guest users must repeatedly access login portal at each Wi-Fi AP	Tracks each Wi-Fi connection so guest users must only authenticate once, enabling access across all APs but while still restricting access to guest resources. This enhances the user experience and decreases load on the authentication server. Flexible authentication policies allow access to be restricted after a configurable time duration or total data usage.	Public, Venue, Hospitality, MDU	Guests
	802.1x authentication takes too long for fast mobility across APs in different networks	Eliminates some of the 802.1x messages to enable fast roaming across APs, even when in different networks with different IP address scopes	Public	All users
	New IP address assigned at each AP	Maintains the same IP address for the user throughout the Wi-Fi network, so cloud-based applications, VoIP, and VPN connections will continue uninterrupted.	Public, Mobile Offload, Venue, Hospitality, MDU	All users
	Session mobility for guests not possible because they cannot use 802.11r fast roaming	Full mobility for guest Wi-Fi	Public, Mobile Offload, Venue, Hospitality, MDU	Guests
Visibility to users behind NAT or for Over-the-Top services	Wi-Fi users are behind NAT of CPE, so they cannot be identified	Has visibility to individual user devices (e.g. MAC addresses), so the service provider can distinguish private from public users	Public, Smart Cities, Mobile Offload	All users
	Layer 3 boundary in access network eliminates visibility to subscribers, so no per-user policies to address different user types and subscription levels	By tunneling traffic across the 3rd-party access network, the service provider, smart city, or business can implement per user and per device policies, such as network traffic micro-segmentation, per-user control and security, per-user content controls, etc.	Public, Smart Cities, Mobile Offload	All users
	Not possible to do "lawful intercept" as required by law enforcement for users behind NAT	Compliant to "lawful intercept" policies and associated interfaces	Public, Mobile Offload	All users
Cost savings	High-scale AAA server required	Maintains user authentication status so authentication messages to the AAA are minimized	Public, Venue, Hospitality	Guests
	High-scale DHCP server	Provides high-scale DHCP at 4000 trans/second	Public, Venue, Hospitality, MDU	All users
	Firewall & NAT (to Internet)	Provides carrier-class firewall and NAT to the Internet	All	All users
	Router (to Internet or internally)	Provides full router functionality (OSPF, BGP, IS-IS, RIP, MPLS, Static)	All	All users
Security	Captive portal can be attacked	Captive portal DoS protection	Public, Venue, Hospitality	Guests
	AP does not support walled garden access for unauthenticated users	Walled garden access for unauthenticated users but without exposing network to Denial of Service (DoS) or other attacks	Public, Venue, Hospitality, MDU	Guests
	Parental / content filtering, malware & phishing prevention	Parental / content filtering, malware & phishing prevention	Public, Mobile Offload, Venue, MDU	All
	Guests' network traffic overwhelms private network traffic, particularly cloud-based Internet applications used by the private network.	Hierarchical Quality of Support (HQoS) to provide advanced bandwidth management to Internet	All	All
CPE limitations	May not segment traffic from different SSIDs, exposing private network to public/guest users	Micro-segmentation of network traffic to keep user types separate	Public, Smart Cities, Venue, Hospitality, MDU	All users
	No portal redirect or poor performance of guest Wi-Fi authentication	High-performance guest Wi-Fi portal authentication	Public, Venue, Hospitality	Guests
	No support for device-specific policies based on authenticated vs unauthenticated, thereby exposing authentication platforms to attack	Specific policies and protections against un-authenticated users	Public, Venue, Hospitality	Guests
Analytics	Analytics vary in multi-vendor AP deployments, making it impossible to provide aggregate stats	Provides single source for standardized analytics	All	All users
	Must be collected from each AP, taking bandwidth away from end-users	No impact on end-user bandwidth	All	All users
	Individual subscriber stats spread across APs, so difficult to correlate	Consolidated stats for each subscriber	All	All users
	End-to-end subscriber application performance unknown	Benu BOSS tool provides subscriber application performance monitoring	All	All users