

GCC Series - UC + Networking Convergence Solutions Overview and Basics



About the GCC Series

The GCC6000 Series provides an extraordinary all-in-one solution that redefines the communications experience by merging your unified communications and networking solutions into one platform. These state-of-the-art devices combine the functionality of 4 products to provide an all-in-one solution that includes a VPN router, next-generation firewall, IP PBX, and network switch or Wi-Fi access point. With the GCC Series, you can create and manage wired, wireless, and VPN networks, provide enterprise-grade network security, and utilize a market-leading communication and collaboration platform. These flexible devices provide unified management and centralized control of all Grandstream endpoint solutions, including Wi-Fi APs, network switches, IP Phones, and more. The GCC Series allows full UC, networking, and security solutions to be configured in minutes and managed through the cloud with the Grandstream Device Management System (GDMS), and can also be managed through our mobile app, local Web UI, and GWN Manager.

Product Positioning

Ideal for small-to-medium sized businesses, the GCC6000 Series provides an all-in-one platform that combines all business data, security, communication, and collaboration needs into one device – making it easier and more affordable than ever to build state-of-the-art communication solutions.



5 or 10 Gigabit ports and PoE/SFP ports on select models



Easy centralized configuration through GDMS



Built-in QoS for prioritization of network traffic

Competitive Features

- IP PBX capabilities provides voice and video communications for 12 users and 4 concurrent calls (upgrades available for purchase)
- Enterprise-grade firewall feature provides anti-virus, layer 3-7 IDS/IPS, DPI, SSL detection, and more
- VPN router solution supports 2.5Gbps or 3Gbps to allow easy remote access to private networks
- Multiple WAN ports with loadbalancing and failover to maximize connection reliability
- Provides advanced security protection with encrypted traffic, secure booth, unique security certificates, and more
- Managed through the cloud (GDMS), mobile app, local Web UI, and GWN Manager

GCC Key Technical Specifications

	GCC6010	GWN6010(W)	GWN6011
Gigabit Ethernet Ports	2 x 2.5 Gigabit SFP ports, 5 Gigabit Ethernet ports - 4 of which are PoE out ports	5x Gigabit Ethernet ports, WAN/LAN configurable, max 3x WAN	2 x 2.5 Gigabit SFP ports, 10 Gigabit Ethernet ports - 4 of which are PoE out ports
PoE / PoE+ Output	4 x PoE out ports, IEEE802.3af/at, Maximum PoE: 36W	n/a	4 x PoE out ports, IEEE802.3af/at, Maximum PoE: 36W
Routing / IPsec VPN	2.5Gbps / 1Gbps	3Gbps / 1Gbps	2.5Gbps / 1Gbps
Wi-Fi AP	n/a	Wi-Fi 6, 2x2:2 MU-MIMO	n/a
QoS Capabilities	VLAN, TOS, Support multiple traffic classes, filter by port, IP address, DSCP, and policing, app QoS: Application/protocol monitoring and traffic statistics; VoIP Prioritization		
Firewall	DDNS, Port Forwarding, DMZ, UPnP, DoS & Spoofing defense, traffic rules, NAT, DPI, Anti-Virus, IPS/IDS, SSL Proxy, Content Control: DNS filtering, web url/class/key words filtering; application identification and control		

GCC Series - UC + Networking Convergence Solutions

Features and Benefits



VPN Router and Firewall

One of the primary functions of the GCC series is its VPN Router and Firewall capabilities. The firewall module of the GCC series is a Next-Generation Firewall (NGFW) that secures users' network environments by providing defenses against advanced network attacks, supporting anti-virus and intrusion prevention with frequent signature library updates. VPN configurations allow for a wide array of VPN types, empowering networks with an encrypted connection that enables users to exchange data across shared or public networks.

- Secure Multi-WAN and Networking
 - Dynamic routing and multi-WAN Capabilities, NAT VLAN, performance-based WAN link selection and monitoring
 - DHCP server, DNS server, IGMP Proxy, TURN server, IPv4/IPv6 support
- High-Speed Virtual Private Network
 - Wireguard, OpenVPN® Clients and Servers, PPTP Clients and Servers, L2TP, IPSec Site-to-Site and Client-to-Site, Remote Users Management
- Advanced Firewall Filtering, Inspection, and Protection
 - Filter by source destination, protocol, and port
 - Stateful packet inspection and DoS attack protection (UDP/ICMP/SYN flood)
 - Enhanced Spoofing Defense
- Intrusion Detection and Advanced Threat Protection
 - Signature-based scanning, auto-rule update using configurable cron, real-time SSL deep inspection, SSL blacklist and whitelist, and GeoIP enforcement
 - Instant identification and immediate response to sophisticated attacks with support for application / protocol monitoring and traffic statistics with Deep Packet Inspection (DPI)

IP PBX

The integrated IP PBX module for Grandstream's series of GCC convergence devices provides a communication and collaboration solution for small-to-medium businesses. It offers the same features and capabilities as provided by Grandstream's other PBX solutions, and ensures a cost-effective and efficient collaboration experience.

- Supports 12 users/4 concurrent calls by default, and can be upgraded up to 200 users or 24 concurrent calls
- Rich IP PBX services, including call forwarding, transfer, parking, intercom/paging, IVR, emergency calls, etc - with built-in audio and video conferencing platform supports Wave Desktop/Web/Android/iOS
- Wide range of QoS features, CRM integration, protocols, multiple audio and video encodings, and more

Management

The GCC series also has an intuitive management system via Grandstream Device Management System (GDMS), GWN Manager, or its local web GUI.

- Centralized Management
 - Intuitive user interface with device management center, allowing for all nodes to be collectively configured, managed, monitored, and troubleshooted
 - GCC can be easily maintained via the GDMS system, with dynamic reporting and monitoring via multiple system performance charts and graphics

GCC Series - UC + Networking Convergence Solutions

Key Feature Highlights



VPN

A Virtual Private Network (VPN) is used to create an encrypted connection enabling users to exchange data across shared or public networks acting as clients connected to a private network. The benefit of using a VPN is to ensure the appropriate level of security for connected systems when the underlying network infrastructure alone cannot provide it. The most common types of VPNs are remote-access VPNs and site-to-site VPNs.

GCC convergence devices support a wide range of VPN configurations such as PPTP, IPSEC, OpenVPN®, LTP, and WireGuard®.

VLANs

VLAN provides a group of host devices with a common set of requirements that allows them to communicate as if they were attached to the same broadcast domain, regardless of their physical location. A GCC device's VLAN has the same attributes as a physical LAN but allows for endpoints to be grouped together even if they are not on the same access level or distribution level switch. This enables tighter network security, smoother IT infrastructure management, and better overall performance.

QoS

Quality of Service (QoS) is the name for a wide set of configurable options that are available on GCC devices. Overall, these settings allow for the prioritization of latency-sensitive traffic exchange between WAN and LAN hosts. Organizations get more control over limited bandwidth, ensuring the smooth operations of all application services.

IP PBX Features

The GCC series of convergence solutions has a staggering amount of communication and collaboration features. Comprehensive call handling, extension customization, IVR/call queue settings, voicemail, call parking lots, instant messaging, video meeting rooms, and more are all available straight out of the box. In addition, a wide set of CRM, PMS, and other integrations are available with API capabilities as well.

Firewall Policy

The GCC series has in-depth policy options to define how GCC devices handle inbound traffic. Rules policy, inbound rules, forward rules, advanced NAT rules, and global configuration are all available. This allows traffic to be thoroughly configured and vetted to ensure network operations remain uncompromised.

Content Control

Especially important for networks that provide public access to Wi-Fi, GCC content control features can filter (allow or block) traffic based on DNS, URL, keywords, and the overall application. Web filtering can be deeply defined to ensure users are not accessing malicious websites. Application filtering will prevent designated application categories from being usable, with optional AI recognition to help the GCC use learning algorithms to more accurately classify applications.

Other Features

Browse all of the GCC's technical features on our technical [user guide](#) located on the documentation center on our website.

GCC Series - UC + Networking Convergence Solutions Deployment Scenarios - Offices



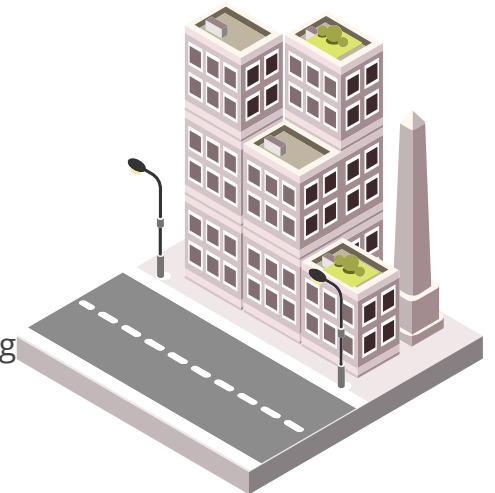
Offices

Small to medium offices can leverage the GCC series to create an all-in-one solution without the need for multiple devices, subscriptions, user interfaces, and other factors that come with having a separate device for UC, networking, and firewall needs. There are a variety of advantages that an office can leverage by using a GCC device, such as the affordability of an all-in-one device, simplified hardware infrastructure, and streamlined configuration and ongoing management. A GCC device would be deployed in the Core layer of an office's network, serving as a backbone for unified communications, security, and network node optimization operations. The device's 2.5 Gigabit SFP ports would connect to distribution/access layer switches that support higher-bandwidth nodes of devices, such as clusters of workstations, while the Gigabit ports could be organized in a LAG configuration to support additional high-bandwidth distribution/access switches, such as Wi-Fi access points, or connect to lower-bandwidth distribution devices such as clusters of IP phones.

Within an office deployment, the GCC state-of-the-art communication and collaboration capabilities can be leveraged to enhance the productivity of a workforce and enable them to work more efficiently with both clients and coworkers. The IP PBX function of the GCC Series provides a suite of powerful communication and collaboration features, including audio and video meetings, calls, conferences, chat, instant messaging, file sharing, whiteboard, recording, webinars, and more. Offices can take advantage of a suite of features to help direct calls, such as comprehensive inbound and outbound route customization, a highly configurable IVR with up to 5 layers, ring grounds, call queues, and more.

An office can benefit from the networking capabilities of the GCC Series as well. The GCC Series offers a secure central admin interface to manage an organization's entire network in real-time; from high-level visual network topology all the way down to a fine granular level, for example, per network node, per endpoint device, per user, or per application. This can be entirely provisioned and managed either locally in the office or remotely through the cloud. VPNs, VLANs, policy-based routing, and Quality of Service (QoS) configurations allow small to medium businesses to take advantage of highly advanced network optimization features typically reserved for more expensive enterprise devices.

Finally, the GCC's firewall capabilities elevate an office's IT infrastructure with the latest in network security. Its state-of-the-art firewall has industry-renowned VB100 Grade-A anti-malware certification, advanced attack defense, adaptive intrusion detection and protection, market-leading AI-based DPI, and sophisticated content filtering and application control. This suite of capabilities provides organizations with comprehensive, end-to-end security protection against cyber threats.



GCC Series - UC + Networking Convergence Solutions Deployment Scenarios - Commercial and Retail



Commercial and Retail

Commercial and retail stores are an ideal choice for a GCC deployment. Larger, multifloor retail stores and malls can have upwards of 200 employees simultaneously working to keep a store functioning. Cashiers, stockers, customer support teams, section managers, and back-of-house managers are all examples of staff that can benefit from the GCC's networking, firewall, and PBX capabilities. Much like an office deployment, a GCC device would be deployed in the Core layer of a commercial network. The GCC would in turn function as the anchor for an IT infrastructure of distribution/access layer switches, Wi-Fi access points that serve both employees and customers, and IP endpoints such as desktop IP phones, speakers, paging devices, workstations, check-out stations, cordless Wi-Fi phones, item scanners, and more.



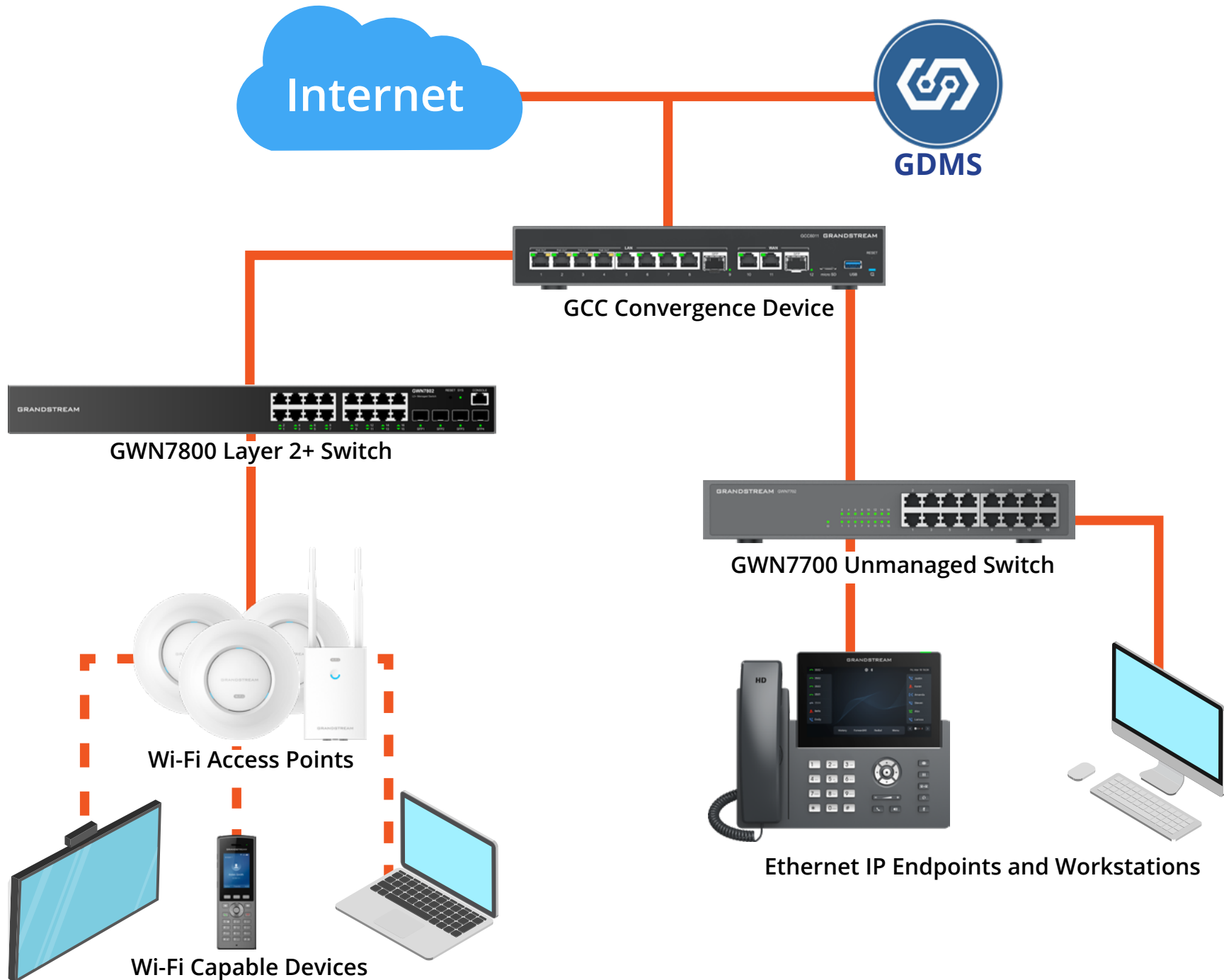
For this deployment, a GCC device's networking capabilities would allow for deep customization of how various nodes throughout the IT infrastructure utilize the network. No one device would require large amounts of bandwidth support, however, a vast amount of IoT devices and IP endpoints would be relying on both hardline ethernet and Wi-Fi connections to access the LAN. The GCC's Virtual Local Area Network (VLAN) capabilities would allow for device segmentation that will make the network easier to manage, separate network traffic based off of department/device type, and then use VLAN Quality of Service (QoS) features to optimize bandwidth utilization. Policy routing and load balance pools can also be leveraged to ensure smooth network performance throughout the entirety of a workday, despite customer/employee network usage.

Retail stores and larger commercial organizations alike will have a large amount of extensions and IP endpoints to manage. A GCC device's IP PBX capabilities can help streamline both internal organizational communication and incoming external customer calls. Mobile employees that are given cordless IP phones, wall-mounted desktop IP phones, paging speakers that are deployed across the entire store, and facility access solutions can all have their extensions customized and grouped, inbound/outbound routes set, paging/intercom groups and multicast settings configured, and be included into call queues. Additionally, internal and external IVRs can be composed so both customers who are calling into the commercial deployment and internal employees can be routed to the proper department/extension for assistance.

While firewall features aren't as critical as an office deployment, the GCC Series will still serve as a safeguard against malicious threats. This will ensure that the operations of critical equipment will not be compromised while also protecting back-of-house workstations from employees who unintentionally fall victim to fraudulent emails and downloads.

GCC Series - UC + Networking Convergence Solutions

Deployment Scenarios - Deployment Diagram



GCC Series - UC + Networking Convergence Solutions

Grandstream Integration

GWN Wi-Fi Access Points

- QoS features and VLAN segmentation on GCC devices can be used to put Wi-Fi access points within their own network while also optimizing their performance
- Both GWN Wi-Fi access points and a GCC device within a single deployment can be fully managed, configured, and monitored via Grandstream's GDMS platform
- For smaller deployments, access points can connect directly to a GCC device via its Gigabit network ports



Cloud Management

- Grandstream Device Management System (GDMS) allows installers and system integrators to easily add, configure, and monitor GCC convergence devices, entirely from the cloud. Entire deployments of Grandstream devices can be managed from this free, comprehensive system
- GCC convergence devices also have network maintenance features that can be used to monitor an entire deployment of devices and ensure a network is operating smoothly

GWN Network Switches

- For larger deployments that have more devices than a single GCC can support, GWN switches can be used as access/distribution level nodes that then connect back to the GCC device
- With a comprehensive onboard networking hub, a GCC device can be used to manage network quality, bandwidth settings, VLAN creation, VPNs, and more. This means only unmanaged switches are needed for endpoint nodes in the deployment, making it more affordable



IP Phone Endpoints

- Grandstream's IP phones can connect to a GCC device deployed in the same network, with the GCC functioning as the network's IP PBX
- PoE-capable IP phones can also be powered by the PoE models within the GCC series in smaller deployments
- Auto-detection, VoIP prioritization, and QoS features can be used to ensure Grandstream endpoints always have a stable connection in busy networks

