Networking Solutions for VoIP

Table of Contents

VoIP has become a mainstream technology. Today, the question for business telephony at any scale is no longer whether to switch to VoIP, but when. This paper focuses on the internal networking aspects of making a successful transition to VoIP, with emphasis on network design and switching technology.

QoS: THE PRIME MOVER

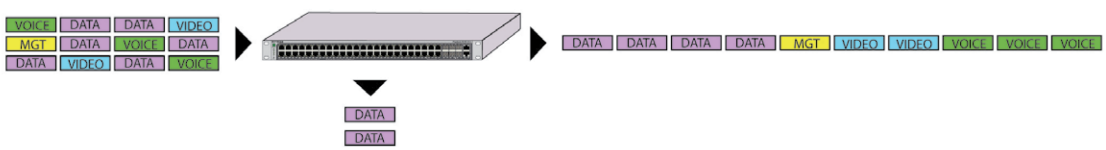
The most important factor that has moved VoIP into the mainstream is improved quality of service (QoS)[1]. Businesses that have held back because of VoIP's early reputation for poor voice quality need no longer be concerned that important transactions (such as sales) will be impeded by poor QoS, or that their company will make a less than fully professional impression on callers with VoIP.

Today, excellent quality of service can always be achieved with VoIP, but it's not guaranteed. QoS ultimately depends on the switches that control the VoIP traffic, and of course, the network over which that traffic travels. It's understandable that the focus of attention in a transition to VoIP is typically on the service provider, the delivery model (onsite vs. hosted) and the IP phones, but the switches have the most important impact on the user experience. With NETGEAR switches, VoIP traffic can be automatically prioritized to maintain the desired QoS, even when the network is saturated.

The key factors required to ensure a successful VoIP network with reliable QoS are as follows:

- **Voice packet prioritization**. The switch(es) that manage the traffic must be able to prioritize voice traffic when necessary to maintain QoS.
- **Adequate bandwidth**. The network and the switch(es) that control it must be able to handle the additional load imposed by a VoIP deployment.
- **Resilience**. The network switch(es) must have access to an alternate power supply should the main source of power fail.
- **Security**. The network must be protected from hacking, including physical hacking.

The first factor – packet prioritization – deserves more explanation. VoIP streams are not forgiving when it comes to dropped packets, signal delay and other factors that don't affect data traffic. Therefore, to ensure a consistently high level of QoS, the switches must be able to prioritize network traffic, giving voice packets top priority. NETGEAR switches accomplish this automatically.



NETGEAR switches automatically analyze packet traffic and give priority to voice packets, eliminating jitter, echo and delay to ensure high QoS.

BENEFITS OF VoIP

This guide will help you understand the basics of VoIP so you can successfully plan and specify a VoIP network. It includes reference designs for VoIP networks with 20, 200 and 1,000 IP phones. Before covering design issues, however, it's worth reviewing just why VoIP has become the solution of choice for organizations of all sizes.

[1] The term "Quality of Service" and its abbreviation, QoS, has long been used in the literal sense of voice quality, i.e. how closely what the user hears matches the original. Recently, however, the term has begun to be used to describe the voice packet prioritization technology that is used to ensure high QoS even during periods of network congestion. In this document, QoS refers only to the original meaning of the term.

VoIP's packet-switched solutions are winning the marketing battle over conventional circuit-switched telephony because they offer advantages that conventional POTS ("Plain Old Telephone Service") just can't match. These include:

- **Price.** VoIP is substantially less expensive than circuit-switched telephony. In fact, online services like Skype enable individual users to international calls of unlimited duration for free. VoIP for business purposes isn't free, but it is dramatically cheaper than today's circuit-switched options.
- **Quality of service (QoS).** In the past, the reduced cost of VoIP came with a penalty: reduced QoS. Today's VoIP technology can provide voice quality that equals or even exceeds what conventional circuit-switched systems offer.
- **Complexity.** Switching to VoIP typically reduces the complexity of dealing with "the phone company" and its arcane pricing structures, which even highly-paid consultants can't always understand.
- **Features.** VoIP can now match conventional telephony feature-for-feature, ranging from basics like voice mail to emerging capabilities like presence sensing.
- **Integration.** More and more of today's business applications, including CRM and call center applications, are grounded in internet-related technical standards. VoIP technology can be integrated with these applications much more easily than the analog technology of conventional telephony.
- **Ease of administration.** Adding, removing or changing internal numbers is a simple process with VoIP's web-based interfaces, and with auto discovery features, activating a new phone is virtually automatic.
- **Deployment advantages.** VoIP can be piggy-backed on an existing network infrastructure, including the physical cabling. This means lower initial cost (with no new wiring) and lower maintenance cost as well.
- **No risk of obsolescence**. VoIP is the wave of the future. Companies who adopt VoIP have no risk of ending up with a "dinosaur" phone system that can't operate efficiently in an all-digital world.

VoIP NETWORK COMPONENTS AND PROTOCOLS

No matter what the size of a VoIP network, it will always include one or more of the following components:

- **User agents.** These may be commercial IP phones, or "soft phones" residing in a desktop or laptop PC.
- **Voice gateway.** The gateway acts as the bridge between a VoIP network and the PSTN network of the "outside world."
- **IPBX.** The IPBX (sometimes referred to as an IP PBX) replaces the conventional PBX of the past, and performs all its functions (voice mail, call forwarding, conference calling and many, many more). It connects to the PSTN network via the voice gateway. The IPBX is available in three deployment options:
    - – a dedicated, on-site hardware device
    - – software that runs on a standard on-site server
    - – a managed service via the cloud
- **Switches to manage network traffic.** The switches are crucial, because if they lack the appropriate capabilities or bandwidth capacity, QoS will suffer, leading to user complaints, poor customer service and problems with external telephone communication in general.
- **Cabling.** For adequate performance, Cat5E or better cabling is recommended.

Decisions involving these components can directly affect QoS, based on which protocols they support. For example, some IP phones use protocols that deliver higher voice quality, but also require more bandwidth. Before reviewing those protocols, it's worth taking a moment to examine QoS in a little more detail.

QoS is ultimately a subjective measurement, because different individuals will invariably disagree as to how well a system can reproduce a voice that's known to them. However, one decades-old attempt objectify QoS does exist. Developed initially for evaluating circuit-switched equipment, it provides a measure of quality known as Mean Opinion Score (MOS) based on individuals sitting in quiet rooms and rating voice quality. MOS can range from 1.0 (unintelligible) to 5.0 (ideal). Normally a score above 4.0 is considered to be acceptable, but what's most important is that QoS can be quantified, and components/protocols can be evaluated based on the MOS score they promise as well as their bandwidth requirements.

There are numerous protocols that govern VoIP systems, but three are of primary concern for VoIP networks:

- protocols for the CODECs that govern analog/digital conversion and the signal compression that takes place in the VoIP gateway (inbound) and the user IP phones (outbound)
- signaling protocols that govern the voice packets and their transmission
- The LLDP-MED protocol extension, used by network devices such as IP phones for advertising their identity, capabilities, and neighbors

CODECs

Popular protocols include G.711, G.729, G.723.1 and G.722. There are others as well, some of which are proprietary. These protocols are important because they differ in their sensitivity to various frequency ranges (e.g. voice only vs. voice and music), offer different levels of QoS, and impose different bandwidth requirements. It's not necessary to understand their details, but it is important to know that they represent options. As would be expected, the higher the QoS, the greater the bandwidth required. Many IP phones support multiple protocols, but that is not always the case.

Signaling Protocols

The signaling protocols govern the set-up and tear down of calls, as well as many other related call management functions. There are three major signaling protocols:

- **H.323.** This is the "oldest" protocol – it is actually a set of protocols – and it is widely distributed. H.323 was designed for multimedia communication services such as real-time audio, video, and data communications over packet networks, including IP networks. Based on binary encoding, is it considered somewhat harder to program than its "competitor," SIP.
- **SIP (Session Initiated Protocol).** This slightly younger protocol accomplishes most of the functions available under H.323, but is somewhat lighter (i.e. requires less bandwidth). It is text-based. The industry consensus is that SIP will eventually come to dominate VoIP communication, with the caveat that multiple protocols are likely to exist into the foreseeable future.
- **SCCP (Skinny Client Control Protocol).** This is a proprietary CISCO signaling protocol used by CISCO IP phones and the CISCO call manager. It is a stimulus-based protocol which achieves its "skinniness" by transferring functions to the call manager.

The LLDP-MED Protocol

LLDP-MED stands for Link Layer Discovery Protocol with Media Endpoint Discovery. When IP phones are LLDP-MED enabled, NETGEAR switches can automatically configure them so that they "know" which VLAN to join and what their QoS assignment is[2]. This protocol also enables automated power management of PoE-powered IP phones – virtually all IP phones are powered this way – as well as other convenience features such as device inventory management.

Security

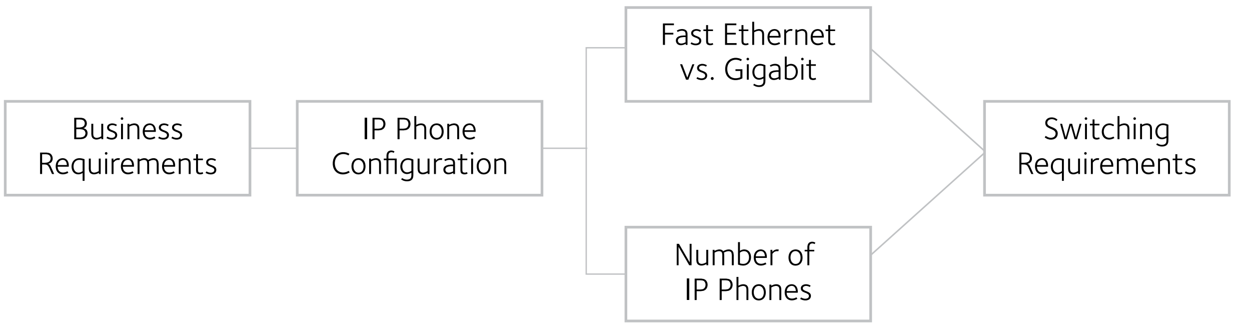
A separate, but extremely important consideration that requires some explanation is network security in an IP network. Obviously, any network will be protected through access control, e.g. support for role-based access with authentication and passwords. In addition, IP networks have a physical vulnerability. An attacker could easily disconnect a IP phone and put a PC in its place, thus obtaining unauthorized access to the network.

To prevent this, NETGEAR switches make use of the unique Media Access Control or MAC address for each physical IP phone. NETGEAR switches can sense this address, and be programmed to block any unauthorized device. The ultimate in protection can be achieved through the use of the Radius (Remote Authentication Dial-In User Service) protocol associated with an authentication server, or a Windows Server 2008 Network Policy Server (NPS) that can block access to ports even if hackers succeed in spoofing and emulating MAC addresses during an attack.

[2] The IP phones must tag their traffic using the correct VLAN tag, and mark their traffic using the correct Layer 2 802.1p or Layer 3 QoS values.

NETWORK PLANNING – GENERAL CONSIDERATIONS

The planning of a VoIP network has several steps, as show below:



Business requirements – QoS, number of users, types of user devices and the like – will determine the number of IP phones and their configuration (e.g. presence or absence of a soft phone connection or use of mobile devices).

The number of IP phones, combined with the need for a Fast Ethernet vs. Gigabit connection, will in turn determine bandwidth and power requirements for the switches. The following section will focus on the details of choosing the appropriate switch(es).

CHOOSING A SWITCH: BANDWIDTH & PORTS

NETGEAR recommends two lines of managed switches for VoIP networks:

- The NETGEAR Intelligent Edge M4100 series. These are Fast Ethernet (10/100) and Gigabit Ethernet (GigE) access layer switches with several Gigabit ports for uplink functions.

- The NETGEAR Next-Gen Edge M5300 series. These are Gigabit Ethernet (GigE) switches with embedded 10 Gigabit ports (10GbE) for uplink functions and virtual chassis stacking.

Determining which switch within these two families requires answering four questions.

1. *Will the IP phones require a Fast Ethernet port (at the switch) or a Gigabit Ethernet port?* Most entry-level desktop IP phones have only one port, which is a Fast Ethernet port. In this case, cost-effective NETGEAR Fast Ethernet switches may be adequate, based on the total bandwidth requirement. (See question 4.) Note that these Fast Ethernet switches, in spite of their name, do include a Gigabit port for uplink purposes in a two-tier network. Sometimes, however, even a deployment with only single port Fast Ethernet IP phones may require 10 Gigabit uplink capabilities.

   Today's high-end, state-of-the-art phones often have two ports, one that connects to the switch and another that connects to a co-located PC. If the co-located PCs on the network require Gigabit speed, then of course a Gigabit switch is required.

2. *What is the average bandwidth required per IP phone?* As explained above, VoIP bandwidth requirements depend on a number of factors, primarily the protocol/compression algorithm used by the codecs (the "G-number") and, to a lesser extent, the signaling protocol (SIP, H.323 or SCCP). Calculating this figure can be quite complicated, and the best way to determine it is simply to consult with the IP phone vendor. Best practice in calculating the bandwidth load on the network is to assume 100 percent usage by every IP phone. This will ensure that the network will be able to handle peak usage periods.

3 *How many IP phones will be on the network?* This determines how many ports the switch(es) will need – one port per IP phone. Note that all of the NETGEAR Fast Ethernet switches are equipped with several Gigabit ports for uplink purposes.

4. *What is the total bandwidth required per switch?* This is a simple calculation:

   Average bandwidth per IP phone x total number of IP phones = total bandwidth required (Gbps)

   The total Gbps that the switch can transfer – the "switching fabric" of that switch – must exceed the answer to this equation. And if the switch must be connected to an upper layer (such as a Core or Distribution Layer), then the uplink connection must support the total bandwidth required for that uplink without creating a bottleneck.

CHOOSING A SWITCH: POWER OVER ETHERNET

Virtually all IP phones are designed to accept Power over Ethernet (PoE). There are two versions available, PoE and PoE+. For IP phones, the 15.4W per port (12.9W to the IP phone) provided by PoE is adequate.

To determine which switch in the M4100 or M5300 family is required for a particular installation from a PoE perspective, ask the following questions:

1. *How many watts are required per IP phone?* This information can easily be obtained from the vendor.

2. *How many IP phones will be on the network?*

3. *What is the total wattage requirement?* It can be calculated as follows:

   Average watts per IP phone x total number of phones = total PoE budget required

   Obviously, the power capacity of the switch – its "PoE budget" – must exceed the total power requirements of the IP phones on the network.

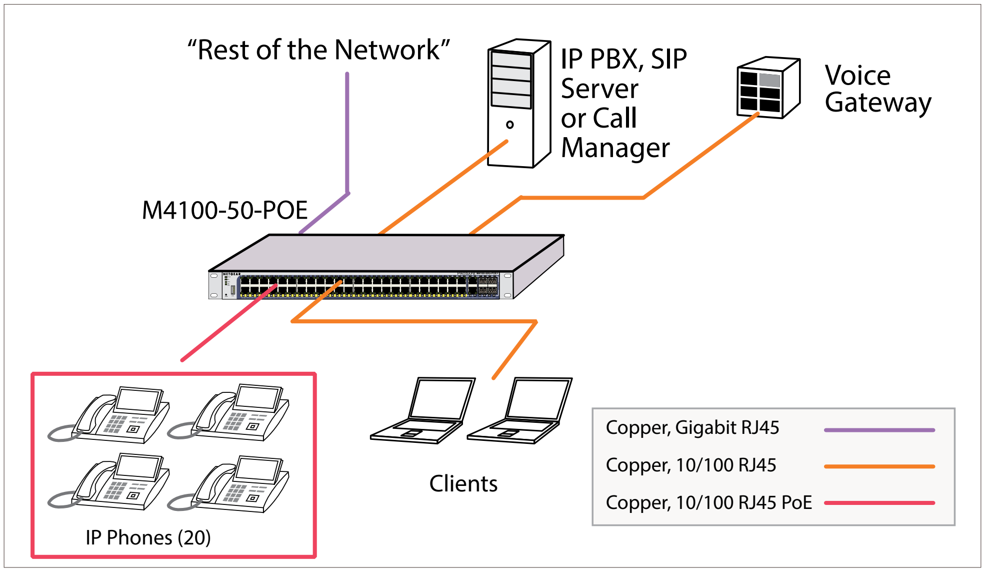
REFERENCE DESIGNS

The following reference designs will provide general guidance on how to plan a highly reliable and cost-effective VoIP network. Each network was designed with four criteria in mind:

- simplicity, to enable easy installation and management
- voice packet prioritization, to ensure that a high level of QoS will always be available
- resilience, to ensure the 24/7 coverage that's a requirement for a business-critical function like telephone service
- security

Reference Design: 20 Phones

The diagram below shows a typical installation with 20 IP phones. It is a complete solution compatible with all major signaling protocols, and is ideal for a small business or branch office that wants to enjoy the benefits of VoIP with maximum simplicity. The IP phones and the IP PBX/voice gateway are all on the same subnet and same VLAN. All the traffic is managed by a single switch, and that switch automatically applies QoS policies to ensure high QoS at all times, even when the network is congested.



The benefits of this design include the following:

Simplicity

- The switch can be configured with a unique, easy-to-use web-based interface as well as the industry-standard command line interface (CLI).
- The IP phones' IP configuration (including every kind of VoIP DHCP option setting) is automatic via a DHCP server or the NETGEAR switch, with no manual intervention required.
- QoS is handled automatically to maintain a constant high level.
- A separate cabling system for telephone service is no longer required, which vastly simplifies the process of adding or changing phone service for employees.
- The IP phones can keep their default configuration for VLAN and QoS settings.
- The switch will automatically set up a voice VLAN and tag the traffic accordingly, without requiring specific manual configuration on the IP phones.

Packet Prioritization

- The switch handles packet prioritization to deliver high QoS automatically. This Automatic Voice over IP prioritization (Auto-VoIP) feature simplifies the most complex multi-vendor IP telephone deployments, when based on any of the major signaling protocols (SIP, H323 or SCCP) .
- Auto-VoIP ensures that both data and signaling VoIP streams receive priority service over other ordinary traffic by classifying that traffic and enabling correct egress queue configuration with automatic 802.1p remarking.

Resilience

- Redundant Power Supply (RPS) protection. The switch can be connected to a back-up power supply to provide redundancy and ensure 24/7 reliability.

Security

- The switch provides for MAC-based security to prevent physical hacking, e.g. replacing the phone connection with a connection to a PC.
- Assuming the IP phones support the IEEE 802.1x authentication standard for port-based Network Access Control, a higher level of security can be implemented using a RADIUS server, or Windows Server 2008 Network Policy Server (NPS). With this approach, access to ports can be blocked even if hackers succeed in spoofing and emulating MAC addresses during an attack.
- The switch also supports MAB bypass for IP phones that don't support RADIUS 802.x authentication.

Bandwidth and Power Calculations: 20 IP Phones	
Average bandwidth per per IP phone	64 kbit/s
Total bandwidth for twenty phones	64 x 20 = 1.3 Mbit/s
PoE Class	1 (maximum 4W)
Total PoE budget	4 x 20 = 80W
All of these figures are well within the capabilities of the M4100-50-POE switch recommended below	
Key NETGEAR Components	
Switch	M4100-50-POE (48 ports Fast Ethernet PoE 802.3af, Layer 2+)
Redundant Power Supply	RPS5412 (Optimal Power one-to-one RPS unit) or RPS4000 (RPS unit up to four switches)
External Power Supply	RPS4000 (supplemental PoE power up to four switches)

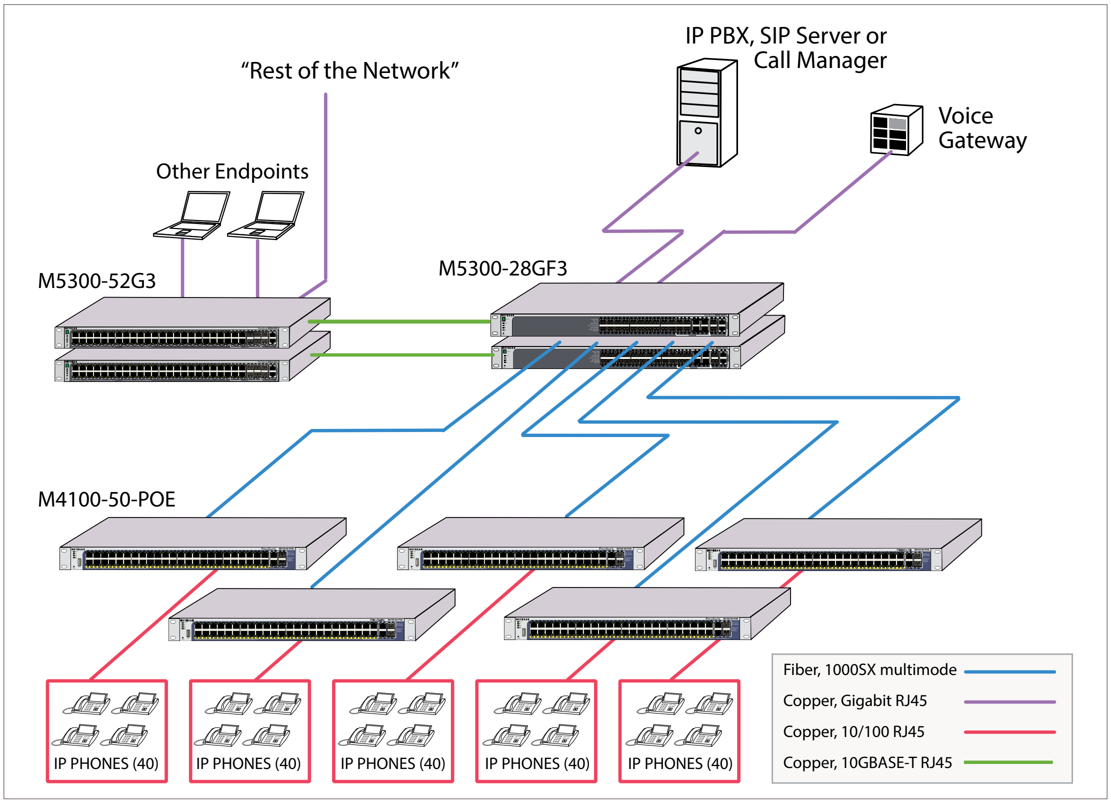
Reference Design: 200 IP Phones

This 200-phone installation would be typical for a mid-sized business or an enterprise-scale call center. At the access layer, each switch connects forty phones, and also powers them via PoE. At the distribution layer, virtual stacking technology is used to stack two M5300-28GF3 managed switches for high performance, highly redundant distributed link aggregation (one 10 Gigabit link per physical switch) for a 20Gbit/s connection to the rest of the network, where other clients may be located.

This installation consists of several IP subnets and associated VLANs, but without Layer 3 routing complexities. The telephony infrastructure components that manage the IP phones (the IP PBX, SIP server or Call Manager, and voice gateway) are all on a dedicated telephony VLAN and in a specified subnet. All the IP phones are also on a dedicated voice VLAN and in a specified subnet. Communication between the various VLANs is accomplished by inter-VLAN routing, i.e. by creating Layer 3 interfaces (IP addresses assigned to VLAN interfaces) and using simple, straight-forward Static Layer 3 Routing on the NETGEAR switches.

The phones receive their IP configuration, their VLAN configuration and their QoS priority settings from the infrastructure components, with no need for manual intervention. QoS settings are enforced by the switches across the entire VLAN network.

This design delivers a highly available network that provides uninterrupted connectivity. It incorporates a level of redundancy such that there are no points of hardware failure. Further, critical components can be swapped without interruption of service.



The benefits of this design include the following:

Simplicity

- The switches can be configured with a unique, easy-to-use web-based interface as well as the industry-standard command line interface (CLI).
- The IP phones' IP configuration (including every kind of VoIP DHCP option setting) is automatic via a DHCP server or the NETGEAR switch, with no manual intervention required.
- The IP phones are auto-discovered and automatically receive their VLAN configuration and QoS priority settings from the IP PBX/SIP Server or Call Manager via the IP telephony vendor-specific mechanisms.
- This network design avoids the use of the Spanning Tree Protocol, which is complex and difficult to configure. The network's highly resilient distribution layer allows for the best of both worlds with redundant links to the servers and access layer switches, as well as advanced load balancing and seamless failover capabilities – made as simple as "trunking."

Packet Prioritization

- The switches handle packet prioritization to deliver high QoS. In fact, the network (all the switches) in this reference design is assigned the task of implementing and enforcing the QoS priority settings determined by the telephony infrastructure (at the IP PBX, SIP Server or Call Manager level), so that the voice traffic is prioritized across the entire network. In addition to simplifying administration, the avoidance of the Spanning Tree Protocol also enables more efficient use of bandwidth, since all links are active and load balancing is enabled.

Resilience

- Redundant Power Supplies (RPSs). In this design the switches are all equipped with an RPS in the unlikely event that a switch power supply should fail. This approach can be implemented on a one-to-one basis with the NETGEAR RPS5412 redundant power supply if all the switches are in different buildings. If the switches are on the same rack, a NETGEAR RPS4000 can be used to provide redundant power to as many as four switches. The internal power supply of the switches at the distribution layer is modular and can be "hot swapped" with no interruption to service.
- Redundant Switches. This design features redundant, stacked distribution switches (two M5300-28GF3 switches and two M5300-52G3 switches) with sub-second network failover protection.

Security

- This design has a dedicated management VLAN for access layer and distribution layer switches, with an additional control plane ACL to better refine the IP/MAC/protocol through which management access to the network is controlled.
- MAC-based port security (MAC address table locking) provides a minimum level of security by preventing an attacker from disconnecting a phone and connecting a PC in its place for hacking purposes.
- Assuming the phones support the IEEE 802.1x authentication standard for port-based Network Access Control, a higher level of security can be implemented using a RADIUS server or Windows Server 2008 Network Policy Server (NPS) with or without MAC authentication bypass (MAB). With this approach, access to ports can be blocked even if hackers succeed in spoofing and emulating MAC addresses during an attack.
- NETGEAR switches support MAB bypass for non-RADIUS-aware phones, and will authenticate such phones when they submit their MAC address to the RADIUS or NPS server.

Bandwidth and Power Calculations: Distribution Layer	
BANDWIDTH	
Average bandwidth per phone	64 kbit/s
Total bandwidth for 40 phones (per switch)	64 kbit/s x 40 = 2.6 Mbit/s
When there is no bridge on the phone for connected to the users' PCs, then the overall bandwidth requirement for VoIP streams is very low.	
POWER	
PoE Class	1 (maximum 4W)
Total PoE budget per switch	4 x 40 = 160W
Key NETGEAR Components	
Distribution Layer Switch	M5300-28GF3 (24 ports Gigabit Ethernet Fiber with 10 Gigabit uplinks, Layer 3)
Access Layer Switch	M4100-50-POE (48 ports Fast Ethernet PoE 802.3af, Layer 2+)
Rest of the Network Switch	M5300-52G3 (48 ports Gigabit Ethernet with 10 Gigabit uplinks, Layer 3)
Redundant Power Supply	RPS5412 (Optimal Power one-to-one RPS unit) or RPS4000 (RPS unit for up to four switches)

Reference Design: 1000+ IP Phones

This 1,000-plus IP phone reference design assumes that telephone service needs to be provided for 12 separate buildings, such as might be the case in a small office complex or a medium-sized campus environment.This design further assumes that each IP phone is equipped with a bridge to the user's PC. For simplicity and ease of installation, it is configured as a two-tier network.

Switches and Cabling

Each building is equipped with two stacked 48-port M5300-52G-POE+ Gigabit switches using virtual chassis stacking technology. These stacked switches provide IP connections for 96 IP phones in each building (1,152 phones total), and also power those phones via PoE. Each switch has one 10GB fiber uplink to the distribution layer for a 4.8:1 oversubscription to the rest of the network, which is acceptable for normal to intensive office environments. Fiber optic cabling is used between each building and the aggregation layer due to the relatively long distance separating them.

At the distribution layer, virtual stacking technology is also used to stack four XSM7224S 24-port, 10 Gigabit managed switches for high performance, highly redundant distributed link aggregation (one 10 Gigabit link per physical switch) for a 40Gbit/s connection to the rest of the network, where other clients may be located.

Network Architecture: VLANs

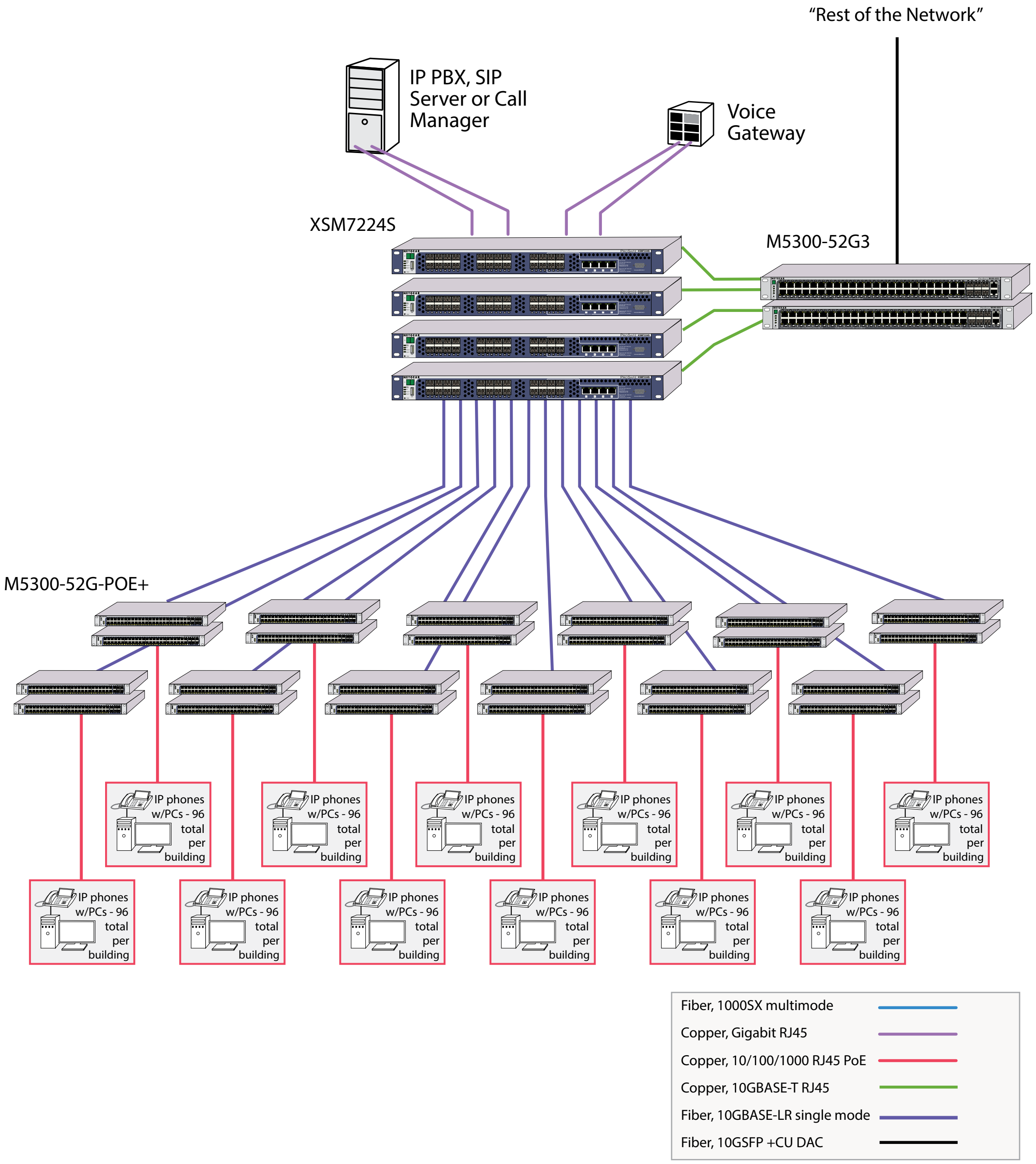
The installation comprises several dedicated VLANs. The telephony infrastructure components that manage the IP phones (the IP PBX, SIP server or Call Manager, and voice gateway) are all on a dedicated telephony VLAN, and in one specified subnet. All the IP phones are also on a dedicated voice VLAN and in another specified subnet. There is a third dedicated management VLAN. The PCs are connected to yet another (existing) VLAN such as a production data VLAN.[3] In other words, the PCs and the IP phones are on separate VLANs, even though they are connected to the network via the same port.

[3] It's assumed that the PCs are unaware of VLAN tagging. The traffic from the PCs will be untagged, but the NETWORK switches will perform this function by adding and removing the production data VLAN tag from packets as appropriate.

Communication between the various VLANs is accomplished by inter-VLAN routing, i.e. by creating Layer 3 interfaces (IP addresses assigned to VLAN interfaces) and using OSPF for unicast routing on the NETGEAR switches.

The phones receive their IP configuration, their VLAN configuration and their QoS priority settings from the infrastructure components, with no need for manual intervention. QoS settings are enforced by the switches across the entire VLAN network (at the VLAN level).[4]

This design delivers a highly available network that provides uninterrupted, high quality telephone service. NETGEAR switches strictly enforce Layer 2 and Layer 3 QoS parameters throughout the network for perfect VoIP prioritization. This design also incorporates a level of redundancy such that there are no points of hardware failure, and quick fault recovery is ensured. Furthermore, critical components can be swapped without interruption of service.



[4] Voice traffic packets can be classified with either Layer 2 802.1p priority or Layer 3 DiffServ priority. If the IP phones support both, we advise using Layer 3 DiffServ prioritization.

The benefits of this design include the following:

Simplicity

- The switches can be configured with a unique, easy-to-use web-based interface as well as the industry-standard command line interface (CLI).
- The IP phones' IP configuration is automatic via a DHCP server or a NETGEAR switch with no manual intervention required, and including every kind of VoIP DHCP option settings.
- The IP phones' IP configuration (including every kind of VoIP DHCP option setting) is automatic via a DHCP server or the NETGEAR switch, with no manual intervention required.
- Without any manual intervention, the IP phones know which VLAN tag and which QoS tag they must use for VoIP streams.
- This network design avoids the use of the Spanning Tree Protocol, which is complex and difficult to configure. The network's highly resilient distribution layer allows for the best of both worlds with redundant links to the servers and access layer switches, as well as advanced load balancing and seamless, sub-second failover capabilities – made as simple as "trunking".

Packet Prioritization

- The switches handle packet prioritization to deliver high QoS. In fact, the network (all the switches) in this reference design is assigned the task of implementing and enforcing the QoS priority settings determined by the telephony infrastructure (at the IP PBX, SIP Server or Call Manager level), so that the voice traffic is prioritized across the entire network.
- In addition to simplifying administration, the avoidance of the Spanning Tree Protocol also enables more efficient use of bandwidth, since all links are active and load balancing is enabled.

Resilience

- Switch redundancy. In every building, the two M5300-52G-POE+ switches connect to a different XSM7224S switch at the distribution layer for perfect redundancy in the unlikely event of a switch failure at either the access or distribution layer. The two switches in each access layer stack at the various buildings are connected to different physical switches at the distribution layer so there is complete redundancy at both layers in the unlikely event that a switch should fail. The four stacked distribution layer switches provide redundancy with < one second failover.
- Redundant Power Supplies (RPSs). This design assumes that each two-switch stack in the access subnet is deployed in a different location. Therefore, each stack is provided with a separate RPS – the NETGEAR RPS4000 – in the unlikely event that a switch power supply should fail. (Each RPS4000 can provide redundant power to as many as four switches.) The internal power supply of the four stacked switches at the distribution layer is augmented with an additional APS300W power module for server-like redundancy. It can be hot swapped if required.
- Redundant links. There are two 10 Gigabit links from each access layer stack to the distribution layer switches, and one of them alone has adequate bandwidth to carry all the aggregated voice streams. Adding a second enables load balancing and also provides redundancy should one of the access layer or distribution layer switches fail – an unlikely event.

Security

- This design has a dedicated management VLAN for access layer and distribution layer switches, with an additional control plane ACL to better refine the IP/MAC/protocol through which management access to the network is controlled.
- MAC-based port security (MAC address table locking) provides a minimum level of security by preventing an attacker from disconnecting a phone and connecting a PC in its place for hacking purposes.

- Assuming the phones support the IEEE 802.1x authentication standard for port-based Network Access Control, a higher level of security can be implemented using a RADIUS server or Windows Server 2008 Network Policy Server (NPS) with or without MAC authentication bypass (MAB). With this approach, access to ports can be blocked even if hackers succeed in spoofing and emulating MAC addresses during an attack.
- IMPORTANT: If the phones support RADIUS or NPS authentication but the PCs connected to them don't, NETGEAR switches will authenticate the PCs by submitting their MAC addresses to the Radius or NPS server using MAB. NETGEAR switches support up to 48 different RADIUS authentications per port, but for this application only two are needed.
- NETGEAR switches support MAB bypass for non-RADIUS-aware phones, and will authenticate such phones when they submit their MAC address to the RADIUS or NPS server.

Bandwidth and Power Calculations: Access Subnet	
BANDWIDTH	
Average bandwidth per phone	64 kbit/s
Total bandwidth for 40 phones (per switch)	64 kbit/s x 40 = 2.6 Mbit/s
POWER	
PoE Class	1 (maximum 4W)
Total PoE budget per switch	4 x 40 = 160W
Key NETGEAR Components	
Distribution Layer Switch	XSM7224S (M7300-24XF 24 ports 10 Gigabit SFP+ with 10GBASE-T uplinks, Layer 2+) and its XSM7224L Layer 3 license upgrade
Access Layer Switch	M5300-52G-POE+ (48 ports Gigabit Ethernet with 10 Gigabit uplinks, Layer 2+) and its GSM7252PL Layer 3 license upgrade
Rest of the network Switch	M5300-52G3 (48 ports Gigabit Ethernet with 10 Gigabit uplinks, Layer 3)
Redundant Power Supply	RPS4000 (RPS unit up to four switches)

MANAGED INFRASTRUCTURE

NETGEAR Managed Switches offer a secure, future-proof networking infrastructure for VoIP deployments in mid-size organizations and campus networks. NETGEAR Managed Switches come with industry-leading lifetime warranties; lifetime advanced technical support; and included 3-year onsite advance replacement service in most of North America, Europe and Australia cities. More detailed information is available at www.netgear.com/managed.

	L3	Chassis 1G/10G	**M8800** series	**Core**
	L2+ L3	Stackable 10G	**M7300** series	**10G Aggregation**
	L2+	Standalone 10G	**M7100** series	
	L2+ L3	Stackable 1G/10G	**M5300** series	**Access**
	L2+	Standalone 100M/1G	**M4100** series	

NETGEAR SWITCHING SOLUTIONS						
Product Name	**M8800-06**	**M8800-10**	**M7300-24XF**	**M7100-24X**	**M5300-28G**	**M5300-52G**
Order Number	**XCM8806**	**XCM8810**	**XSM7224S**	**XSM7224**	**GSM7228S**	**GSM7252S**
RJ45 Ports	Up to 240 x 10/100/1000	Up to 432 x 10/100/1000	4 x 10GBASE-T	24 x 10GBASE-T	24 x 10/100/100 2 x 10GBASE-T (Max: 4)	48 x 10/100/100 2 x 10GBASE-T (Max: 4)
Fiber SFP+ (1000/10G)	Up to 40 x XFP	Up to 72 x XFP	24 x SFP+	4 x SFP+	2 x SFP+ (Max: 4)	2 x SFP+ (Max: 4)
Fiber SFP (100/1000)	Up to 128 x SFP	Up to 224 x SFP	-	-	4 x SFP	4 x SFP
Power over Ethernet	Up to 240 x PoE 802.3af	Up to 432 x PoE 802.3af	-	-	-	
PoE Budget (Watts)	Up to 5,000W	Up to 5,000W	-	-	-	
Redundant Power Supply	N+1 modular PSUs	N+1 modular PSUs	Dual hot swap PSUs	Dual hot swap PSUs	RPS + Modular PSU	RPS + Modular PSU
Feature Set	Full Layer 3 Optional Core License	Full Layer 3 Optional Core License	Layer 2+ (static routing) Optional Full L3 License	Layer 2+ (static routing)	Layer 2+ (static routing) Optional Full L3 License	Layer 2+ (static routing) Optional Full L3 License
Form Factor	Chassis 10U	Chassis 14U	Rack 1U Stackable	Rack 1U Standalone	Rack 1U Stackable	Rack 1U Stackable
Product Name	**M5300-28G-POE+**	**M5300-52G-POE+**	**M5300-28G3**	**M5300-52G3**	**M5300-28GF3**	**M4100-D10-POE**
Order Number	**GSM7228PS**	**GSM7252PS**	**GSM7328S**	**GSM7352S**	**GSM7328FS**	**FSM5210P**
RJ45 Ports	24 x 10/100/100 2 x 10GBASE-T (Max: 4)	48 x 10/100/100 2 x 10GBASE-T (Max: 4)	24 x 10/100/100 2 x 10GBASE-T (Max: 4)	48 x 10/100/100 2 x 10GBASE-T (Max: 4)	4 x 10/100/100 2 x 10GBASE-T (Max: 4)	8 x 10/100 2 x 10/100/1000
Fiber SFP+(1000/10G)	2 x SFP+ (Max: 4)	2 x SFP+ (Max: 4)	2 x SFP+ (Max: 4)	2 x SFP+ (Max: 4)	2 x SFP+ (Max: 4)	
Fiber SFP (100/1000)	4 x SFP	4 x SFP	4 x SFP	4 x SFP	24 x SFP	2 x SFP
Power over Ethernet	24 x PoE+ 802.3at	48 x PoE+ 802.3at	-		-	8 x PoE 802.3af
PoE Budget (Watts)	380W/720W EPS	380W/1,440W EPS	-		-	66W
Redundant Power Supply	RPS + Modular PSU	RPS + Modular PSU	RPS + Modular PSU	RPS + Modular PSU	RPS + Modular PSU	-
Feature Set	Layer 2+ (static routing) Optional Full L3 License	Layer 2+ (static routing) Optional Full L3 License	Full Layer 3	Full Layer 3	Full Layer 3	Layer 2+ (static routing)
Form Factor	Rack 1U Stackable	Rack 1U Stackable	Rack 1U Stackable	Rack 1U Stackable	Rack 1U Stackable	Desktop

Product Name	**M4100-26-POE**	**M4100-50-POE**	**M4100-D12G**	**M4100-D12G-POE+**	**M4100-12GF**	**M4100-12G-POE+**
Order Number	**FSM7226P**	**FSM7250P**	**GSM5212**	**GSM5212P**	**GSM7212F**	**GSM7212P**
RJ45 Ports	24 x 10/100 2 x 10/100/1000	48 x 10/100 2 x 10/100/1000	12 x10/100/1000	12 x 10/100/1000	12 x 10/100/1000	12 x 10/100/1000
Fiber SFP (100/1000)	2 x SFP	2 x SFP	2 x SFP	4 x SFP	12 x SFP	4 x SFP
Power over Ethernet (PoE/PoE+)	24 x PoE 802.3af	48 x PoE 802.3af		10 x PoE+ 802.3at out	4 x PoE+ 802.3at	12 x PoE+ 802.3at
PoE Budget (Watts)	380W	380W/740W EPS		125W	150W	380W
Redundant Power Supply	RPS	RPS	PD Mode	PD Mode	RPS	RPS
Powered by PoE+ (Passthrough)	-	-	1 x PoE+ 30W port in	2 x PoE+ 30W ports in Can redistribute 25W	-	-
Feature Set	Layer 2+ (static routing)	Layer 2+ (static routing)	Layer 2+ (static routing)	Layer 2+ (static routing)	Layer 2+ (static routing)	Layer 2+ (static routing)
Form Factor	Rack 1U Standalone	Rack 1U Standalone	Desktop	Desktop	Rack 1U Standalone	Rack 1U Standalone
Product Name	**M4100-26G**	**M4100-50G**	**M4100-26G-POE**	**M4100-24G-POE+**	**M4100-50G-POE+**	**RPS/EPS Unit**
Order Number	**GSM7224**	**GSM7248**	**GSM7226LP**	**GSM7224P**	**GSM7248P**	**RPS4000**
RJ45 Ports	26 x 10/100/1000	50 x 10/100/1000	26 x 10/100/1000	24 x 10/100/1000	50 x 10/100/1000	For up to 4 switches
Fiber SFP (100/1000)	4 x SFP	4 x SFP	4 x SFP	4 x SFP	4 x SFP	For up to 4 switches
Power over Ethernet (PoE/PoE+)			24 x PoE 802.3af	24 x PoE+ 802.3at	48 x PoE+ 802.3at	APS1000W combination
PoE Budget (Watts)			192W/380W EPS	380W/720W EPS	380W/1,440W EPS	Up to 2,8880W budget
Redundant Power Supply	RPS	RPS	RPS	RPS	RPS	RPS EPS
Feature Set	Layer 2+ (static routing)	Layer 2+ (static routing)	Layer 2+ (static routing)	Layer 2+ (static routing)	Layer 2+ (static routing)	Connects M4100 series and M5300 series
Form Factor	Rack 1U Standalone	Rack 1U Standalone	Rack 1U Standalone	Rack 1U Standalone	Rack 1U Standalone	Rack 1U Four Slots