SMB Networking Basics

Small Business Network

Building a Small Business Network

Small Business Network

Invest in a network that can grow over time, so you can add features and functionality.

Make sure your switches and routers are easy to install, use, and manage.

In today's global economy, small business networking is about reducing your operating costs. It's about reacting quickly to changing markets and customer needs. It's about being prepared for the future.

Routers and switches are the building blocks for all business communications as they can increase productivity, cut business costs, and improve security and customer service.

Small Business Network Benefits:

Routers and Switches allow your Small Business Network to:

Work Anywhere

A host of technologies such as virtual private networks (VPNs) enable mobile employees and teleworkers to work securely at home, on the road, or at customers' offices.

Improving security

Reduce risk and protect valuable business information by installing a networked solution with switches and routers. For example, routers can protect your network with a built-in firewall and Intrusion Prevention System (IPS) - specialised software that examines incoming data and protects against attacks.

Reducing operating costs

Routing and switching technologies can make a positive impact on your bottom line. You save expenses by sharing equipment, such as printers, internet access, servers, and services. A reliable network also can grow with your business, keeping you from having to replace it as your needs grow.

For additional SMB networking information visit Cisco. If you would like to talk to a Cisco Specialist regarding an upcoming project, then simply contact us

Speeding access to information

Accurate, timely information is essential for making business decisions. Routing and switching provides access to allow great visibility into real-time business information and provides a sound basis for effective decision-making.

Enhancing customer service

Today's customers expect rapid responses and personalised services whenever they're dealing with your business. A responsive, reliable small business network is an absolute necessity to give your employees speedy access to customer information.

Access Customer Data Wherever, Whenever

Secure small business networking allows you to input, update, and view information about customers in a database.

Be Prepared for the Future

Designing a secure, flexible small business network allows you to easily, cost-effectively add new applications such as voice and video. Therefore your business will be better positioned to keep ahead of competitors.

Adding voice and wireless to your secure small business network provides additional benefits:

- Streamline Network Management

Combining voice, data, and other applications into one network simplifies network installation and management.

- Communicate More Effectively

A secure voice and data network foundation lets you check email, voicemail, and faxes from one inbox. A single phone number will ring simultaneously on multiple devices, preventing callers from landing in voicemail. With enhanced communications, your company can more easily expand globally.

- Reduce Costs

Consolidating all your communications onto a single network saves companies an average of 46 percent in network costs, according to market research firm IDC.

- Use Your Phone as a Computer—and Your Computer as a Phone

Your employees can roam the sales floor, warehouse, office, or campus with their phones, so they're never out of touch. They can use their wireless phones to look up customer data, access the company directory, get stock quotes, and perform other tasks. When traveling, employees can use laptops to make and receive calls using your company's full phone system—just as they would if they were in the office.

Ten Tips for Making Your Business More Efficient

To cut costs, work more efficiently, improve customer satisfaction, and stay ahead of the competition

Efficiency is Key

To keep pace in an increasingly competitive world, your business needs to run as efficiently as possible. Sooner or later, any company not operating efficiently will be out of business. Efficiency is even more important for small and medium-sized businesses, because their resources are limited compared to large global companies.

Here are 10 tips for using network technology to help your business

1. **Give employees secure, consistent access to information.** You have an advantage over larger competitors because you can react quickly to business changes. But you can quickly lose this edge if your company network is frequently down, sluggish, or unsecured. A secure, reliable network based on intelligent routers and switches lets your employees access the information and tools they need to keep ahead of competitors.
2. **Deliver anytime, anywhere access to employees on the go.** To stay productive on the move, your employees need to be able to reach the people and information they need—anywhere, anytime. With tools like virtual private networks (VPNs), your employees can work outside the office and still enjoy safe access to the business network.
3. **Create effective business processes with partners.** Some large companies make efficient, secure business processes a prerequisite for doing business with them. To meet the business needs of your partners, you need a secure, reliable network.
4. **Make it easy to work together.** Smooth collaboration between employees, partners, suppliers, and customers is a sure-fire way to boost efficiency while also reducing costs. An intelligent network lets your business take advantage of interactive calendaring, videoconferencing, unified communications, and other technologies for easy collaboration.
5. **Enable employees to take their phone systems wherever they go.** Missed calls create project delays, wasted opportunities, and lost revenues. With a networked voice and data solution, your employees can have one phone number that rings simultaneously on multiple devices, so customers reach the

For additional SMB networking information visit Cisco. If you would like to talk to a Cisco Specialist regarding an upcoming project, then simply contact us

right person the first time. Your staff can access all their communications anywhere, from just one inbox.

6. **Streamline customer communications.** Delivering fast, knowledgeable service is the best way to keep customers satisfied. Linking your network phone system to a customer relationship management (CRM) solution is a great way to enhance customer communications. When a customer calls, a pop-up window with their records appears on an employee's IP phone screen, computer screen, or both.
7. **Reduce unproductive travel time.** All too often, time spent on the road is time lost. A networked phone solution that offers video calls and Web conferencing can help reduce the time and expense of traveling to offsite meetings. Instead of spending time traveling, you can use the time to get work done with technology.
8. **Employ a managed service provider.** Is managing a network the best use of your employees' time? In some situations, it is advantageous to hire a managed service provider for network administration. Working with a managed service provider can free your IT staff to focus on other IT tasks and use their time more effectively.
9. **Improve employee satisfaction.** Ageing phone systems and slow networks can frustrate your employees and customers. In some cases, an employee might become burned out and decide to move on. To help ensure that employees are productive and satisfied, your business needs a secure, reliable, and fast network.
10. **Develop a long-term technology plan.** The process of replacing obsolete hardware can bring the office to a standstill. You can minimise such disruptions by carefully determining short- and long-term business objectives and working with your network vendor to deploy technology that matches them.

Solutions from Cisco

Cisco and Cisco Certified Partners, value-added resellers (VARs), and managed service providers offer a variety of solutions tailored specifically to the needs of businesses like yours:

- Intelligent small business routers and small business switches, for a secure, reliable network foundation
- Voice and conferencing, for merging voice, video, and data into one phone system
- Security for small and medium-sized businesses, to safeguard against network threats and give employees highly secure network access from home
- Wireless mobility solutions, enabling workers to stay connected while on the go
- Advanced applications, such as Cisco Unified CallConnectors, linking your networked phone system to CRM solutions

Cisco and its partners work closely with you to identify business goals and map them to specific solutions. And Cisco Capital offers flexible leasing and financing options designed for your needs.

Begin exploring Cisco solutions for small and medium-sized businesses.

The Network & Its Key Components

Switches, Routers & Wireless

What is a Network?

The network operates by connecting computers and peripherals using switches, routers, and access points. These devices perform very different functions, and within the network they communicate with one another, as well as with other networks.

Switches

Switches are used to connect multiple devices on the same network within a building or campus. For example, a switch can connect your computers, printers, and servers, creating a network of shared resources. The switch serves as a controller, allowing devices to share information and communicate. Through information sharing and resource allocation, switches save you money and increase productivity.

There are two basic types of switches to choose from as part of your networking basics, managed and unmanaged:

An unmanaged switch works right out of the box. It's not designed to be configured, so you don't have to worry about installing or setting it up correctly. Unmanaged switches have less network capacity than managed switches. You'll usually find unmanaged switches in home networking equipment.

A managed network switch is configurable, offering greater flexibility and capacity than an unmanaged switch. You can monitor and adjust a managed switch locally or remotely, to give you greater network control.

Routers

Routers are used to connect multiple networks together. For example, you would use a router to connect your networked computers to the Internet and thereby share an Internet connection among many users. The router acts as a dispatcher, choosing the best route for your information to travel so that you receive it quickly. Routers analyse the data that is sent over a network and send it to another network or to a different type of network. They connect your business to the outside world, protect your information from security threats and can even decide which computers get priority over others.

Routers include different capabilities. Features include:

- Firewall: Specialised software that examines incoming data and protects your network against attacks.
- Virtual private network (VPN): A way for remote employees to safely access your network.

For additional SMB networking information visit Cisco. If you would like to talk to a Cisco Specialist regarding an upcoming project, then simply contact us

- IP phone network: Combines your company's computer and telephone network, using voice and conferencing technology, to simplify and unify your communications.

What Is a Network Switch versus a Router?

Switches create a network. Routers connect networks. A router links computers to the Internet, so users can share the connection. A router acts as a dispatcher, choosing the best path or route for information to travel so it's received quickly.

What Is a Network Switch to My Business?

Switches and routers are the building blocks for all business communications. They can increase productivity, trim expenses, improve security and customer service.

Wireless

An access point allows wireless devices to connect to the network. Having a wireless network makes it easy to bring new devices online and provides flexible support to mobile workers. An access point takes the bandwidth coming from a router and stretches it so that many devices can go on the network from farther distances away. But an access point does more than simply extend Wi-Fi. It can also give useful data about the devices on the network, provide proactive security, and serve many other practical purposes.

Access points support different IEEE standards. Each standard operates on varying frequencies, delivering different bandwidth, and supporting different numbers of channels.

There are four different types of deployments that an organisation can choose from to create a wireless network. Each deployment has its own attributes that will work better for different solutions. They are:

- Cisco Mobility Express: A simple, high-performance wireless solution for small or medium-sized organisations. Mobility Express has the full complement of advanced Cisco features. These features allow for a quick and effortless deployment that can be operational in minutes.
- Centralised deployment: The most common type of wireless network, traditionally deployed in campuses where buildings and networks are in close proximity. This deployment consolidates the wireless network, allowing for easier upgrades and enabling advanced wireless functionality. Controllers are based on-premises and are installed in a centralised location.
- Converged deployment: A solution tailored for small campuses or branch offices. This deployment consistently converges wired and wireless on one network device—an access switch—and performs the dual role of both switch and wireless controller.
- Cloud-based deployment: A system that uses the cloud to manage network devices deployed on-premises at different locations. The solution requires Cisco Meraki cloud-managed devices, which have full visibility of the network.

Wireless Network

Why you need to go Wireless

What is a Wireless Network?

A wireless local-area network (LAN) uses radio waves to connect devices such as laptops to the Internet and to your business network and its applications. When you connect a laptop to a WiFi hotspot at a cafe, hotel, airport lounge, or other public place, you're connecting to that business's wireless network.

What Is a Wireless Network vs. a Wired Network?

A wired network connects devices to the Internet or other network using cables. The most common wired networks use cables connected to Ethernet ports on the network router on one end and to a computer or other device on the cable's opposite end.

Catching Up with Wired Networks

In the past, some believed wired networks were faster and more secure than wireless networks. But continual enhancements to wireless networking standards and technologies have eroded those speed and security differences.

The Benefits of a Wireless Network:

A business can experience many benefits from a wireless network, including:

Convenience. Access your network resources from any location within your wireless network's coverage area or from any WiFi hotspot.

Mobility. You're no longer tied to your desk, as you were with a wired connection.

Productivity. Wireless access to the Internet and to your company's key applications and resources helps your staff get the job done and encourages collaboration.

Easy setup. You don't have to string cables, so installation can be quick and cost-effective.

Expandable. You can easily expand wireless networks with existing equipment, while a wired network might require additional wiring.

Security. Advances in wireless networks provide robust security protections.

Cost. Wireless networks reduce wiring costs.

For additional SMB Wireless information visit Cisco. If you would like to talk to a Cisco Specialist regarding an upcoming project, then simply contact us

Other reasons to go Wireless:

Enhanced guest access

- Give secure network access to customers and business partners
- Offer a value-added service

A wireless network allows your business to provide secure wireless access to the Internet for guests such as customers or business partners.

Improved responsiveness

- Connect to the information you need when you need it
- Provide better customer service

A wireless network can improve customer service by quickly connecting staff to the information they need. For example, a doctor in a small medical office can access online patient files while moving between exam rooms, or a retail sales person can check on available inventory necessary to write up orders on the showroom floor.

Better access to information

- Connect hard-to-reach areas
- Improve your processes

Wireless LANs allow a business to bring network access to areas that would be difficult to connect to a wired network. For example, adding wireless access points to a warehouse can make it easier to check and manage inventory, providing the company with accurate inventory figures in real time.

Wireless Networking: Getting Started

Ready to get started with wireless networking? Consider these steps:

1. Make Sure Your PCs Are Wireless

Most laptops today have built-in wireless networking connections. If yours doesn't, you'll need to install a wireless network adapter card, which is typically inexpensive and easy to use.

2. Get a Router Capable of Wireless Networking

Many network routers today act as wireless networking access points. They let you connect multiple computers to a single wireless network. And they connect your network to the Internet.

You can extend wireless networking throughout your office, store, or campus by placing additional wireless access points in various locations. The additional access points extend the wireless signal's range and strength over a wider geographical area, so that it's available in more places, such as conference rooms.

3. Pay Attention to Location

The signal generated from each wireless access point or router extends up to approximately 300 feet. Walls, metal (such as in elevator shafts) and floors can negatively affect range. And the wireless signal's strength weakens the longer it has to travel. For best results, space out your access points and position them in central areas. Tip: Access points can provide stronger signals when installed on or near ceilings.

4. Don't Overshare Access Point

For best results, don't share any single wireless access point with more than 20 users. Typically, the more users sharing an access point, the slower the wireless network can become. If your business network supports a voice over Internet Protocol (VoIP) or Unified Communications system, limit each access point to 8-12 users.

5. Secure Your Network

Security is vital to wireless networking. Some security methods to consider for your network include:

- Data encryption, so only authorised users can access information over your wireless network
- User authentication, which identifies computers trying to access the network
- Secure access for visitors and guests
- Control systems, which protect the laptops and other devices that use the network.

Cisco Aironet 1815 Access Point Series - A Wireless SMB staple in your business network

Network Security Checklist

Helping You Keep Your Network Safe

Network Security Checklist

Many small and medium-sized businesses do not have adequate network security. Here's how to make sure you do.

Now more than ever, you depend on your network for your most important business operations, such as communication, inventory, billing, sales, and trading with partners. Yet up to now, you might have held off on protecting your network, for several reasons:

- Network security might seem too complex, and tackling it might seem like too much work. But you can take a step-by-step approach as described in the checklist below, and then get an outside consultant to help you complete your security plan.
- You might think network security is an expense that won't help your business grow. Instead of thinking about network security as a technical concern, consider it a business continuity issue. Networks have become a basic part of doing business today, making security as important as sales and marketing.
- You may believe that smaller companies are less likely to be a target of attacks. But as large companies beef up their network security, hackers are increasingly focusing on small and medium-sized businesses.

General Security Planning Tips

The following tips can help you develop and win support for an effective network security plan:

- Focus on return on value rather than return on investment. Consider the harm a network security breach could do to your business, such as lost revenue or customer litigation.
- Never assume that network attacks will come only from outsiders. Your employees can accidentally create security vulnerabilities, or former employees can cause damage.

For additional SMB security information visit Cisco. If you would like to talk to a Cisco Specialist regarding an upcoming project, then simply contact us

- Don't be tempted to confront security concerns with a piecemeal approach rather than a single, unified strategy that protects your whole network.
- Work with others in your company to develop and roll out security strategies, focusing on technology, training, and physical site security with tools like surveillance cameras.
- Find the right balance between security and usability. The more secure your network is, the more difficult it can be to use.

Network Security Checklist

Every business should have a thoughtfully prepared network security plan. A thorough policy will cover topics such as:

- Acceptable use policy, to specify what types of network activities are allowed and which ones are prohibited
- E-mail and communications activities, to help minimise problems from e-mails and attachments
- Antivirus policy, to help protect the network against threats like viruses, worms, and Trojan horses
- Identity policy, to help safeguard the network from unauthorised users
- Password policy, to help employees select strong passwords and protect them
- Encryption policy, to provide guidance on using encryption technology to protect network data
- Remote access policy, to help employees safely access the network when working outside the office

Answering the following questions can help you develop your own policy:

Do you have any of the following?

- **Firewall**, to keep unauthorised users off your network
- **Virtual private network (VPN)**, to give employees, customers, and partners secure access to your network
- **Intrusion prevention**, to detect and stop threats before they harm your network
- **Content security**, to protect your network from viruses, spam, spyware, and other attacks
- **Secure wireless network**, to provide safe network access to visitors and employees on the go
- **Identity management**, to give you control over who and what can access the network
- **Compliance validation**, to make sure that any device accessing the network meets your security requirements

Identify Your Most Important Digital Assets and Who Uses Them

- Exactly what are your company's digital assets (such as intellectual property and customer records)?
- What are they worth?
- Where do those assets reside?
- Who has access to these assets, and why? Can all employees access the same assets?
- Do you extend access to business partners and customers?
- How do you control that access?

What Would a Security Breach Do to Your Business?

- What is the potential financial impact of a network outage due to a security breach?
- Could a security breach disrupt your supply chain?
- What would happen if your Website went down?
- Do you have e-commerce features on your site? How long could the site be down before you lost money?
- Are you insured against Internet attacks, or against the misuse of your customers' data? Is this insurance adequate?
- Do you have backup and recovery capabilities to restore information if necessary after a security breach?

Consider Your Current and Future Needs

- How do you expect your business plan to evolve over the next few years?
- How recently have you updated your network equipment? Software? Virus definitions?
- What type of security training do you provide to your employees?
- How will growth affect your digital assets and their value to your business as a whole?
- In the future, are you likely to have a greater need for remote employees, customers, or partners to access those digital assets?

Cisco's Next Gen Intrusion Prevention Systems (NGIPS) are a necessity for a SMB Network to ensure your business network is safe

Firewalls

Firewall solutions

Firewall Solutions

Firewall software and hardware solutions are both designed to block unauthorised access to computers. Firewalls help prevent hackers from intercepting private data or planting Trojan horses or other Internet threats on your networked computers.

Small business firewall software is one method used to protect computers against hacker attacks and other Internet threats. Another method is to deploy a hardware firewall (which also uses software).

Software vs. Hardware Firewalls

Software firewalls protect each individual PC they're installed on. But to protect all your company's computers, each must have a software firewall installed. That can get expensive and be difficult to maintain.

On the other hand, hardware-based firewall solutions for small business protect all computers on your network. A hardware-based firewall is easier to administer, too.

The ideal firewall solutions for small business integrate a hardware firewall with software controls into a comprehensive security solution that includes virtual private network (VPN) support, antivirus, antispam, antispyware, and content filtering capabilities.

Firewall Solutions for Small Business: Benefits

Firewall solutions for small business, when integrated with a comprehensive security device, offer many benefits. Among them are:

- Support for changing business needs. The best firewall solutions for small business let you safely deploy new applications. They provide advanced application-layer security for a wide range of applications, including email, voice over IP (VoIP), video, and multimedia programs.
- Controlled access to your company's resources. The most effective firewall solutions for small business block unauthorized access to applications or information assets.
- Increased employee productivity. By blocking unauthorised access from hackers, your firewall helps prevent the loss of employee productivity or valuable company data.

For additional Firewall information visit Cisco. If you would like to talk to a Cisco Specialist regarding an upcoming project, then simply contact us

- Improved business resiliency. The best firewalls prevent disruption of business-critical applications and services due to security breaches.

[Find out more about Cisco Next Gen Firewall Solutions]

Cisco ASA 5500-X FirePower Services

Small Business Phone System

What to consider when implementing a new small business phone system

What to Know When Buying?

Small business phone systems are available in a variety of configurations, offering an ever-growing range of features and benefits. Most modern small business phone systems today run on Internet Protocol (IP) networks—the same network they use to connect employees, devices, and information resources.

But how do you find the right small business phone system for your company? And what's the best way to deploy it?

Understand What Your Users Need

The right small business phone system can give your people the tools they need to be more efficient.

Features and capabilities available include:

- Mobile softphones, for using a computer as a phone
- The ability to make and receive calls from smartphones or tablets
- Video or web conferencing support
- Automated attendant
- Paging and intercom

You can also get unified messaging, with notifications by email, text message, or phone. Instant Messaging and Presence technology, help you quickly identify the people available within your organisation and reach them at any given time.

Benefits Include:

- **Improve Customer Relationships** – Adding customer contact centre technology to your small business phones gives customers multiple ways to reach you—via phone, fax, email, or click-to-chat. This helps your support team provide faster, more targeted service.
- **Free Your Workforce** – Today's small business phones aren't bound to a desk, and neither are employees. Workers can consolidate all incoming business calls to mobile, home office, or other phones with a single phone number and immediately receive calls wherever they're working.
- **Simplicity** – For employees, an IP network-based phone system can be as easy to use as a traditional landline phone, yet offer far more features and capabilities.

For additional SMB Phone System information visit Cisco. If you would like to talk to a Cisco Specialist regarding an upcoming project, then simply contact us

- **Flexibility & Mobility** – Communicate your way, in the most effective way for the task at hand – a phone call, video call, or with instant messaging or chat. Offered on smartphone and tablet platforms – including those owned by employees.

Ultimately, Cisco small business phone systems offer you simplified communications that enhance key business relationships, reduce your communications costs, and improve productivity for you and your coworkers.

With the Cisco Unified IP Phones 7900 Series, small businesses can make employees more productive by giving them the voice and data communications they need.

Voice over IP (VoIP)

VoIP helps your business keep it simple while saving cash

What is VoIP?

With VoIP, analog voice calls are converted into packets of data. The packets travel like any other type of data, such as e-mail, over the public Internet and/or any private Internet Protocol (IP) network.

How VoIP works for your business is simple: By adding voice to a data network, you'll reduce costs, improve productivity, and enhance collaboration.

As a business owner, you've got to stay flexible-and that's why VoIP for business is such a great way to go. By switching to an Internet-based phone system on your own network, you'll stay connected at work and at home. You'll have better security. And you'll have easier access to the information you need, right when you need it.

- **Save money**
- **Reduce travel expenses** with Web conferencing, video calls, and other collaborative tools
- **Add extra phone lines** easily-VoIP allows you to send more than one phone call across the same Web-based network
- **Communicate better** with employees and customers
- Offer more ways for you and your employees to **stay connected**
- **"Presence" technology** allows you to see which employees are available and how to contact them
- **Unified communications** makes it easier for you to work from home-or from anywhere with an Internet connection

Enjoy lots of features **without** hidden fees:

- Call forwarding
- Voicemail
- Unlimited long distance
- Call conferencing
- Caller ID

Voice over IP Facts:

The Range of Services

VoIP is available in a wide range of services. Some basic, free VoIP services require all parties to be at their computers to make or receive calls. Others let you call from a traditional telephone handset or even a cell phone to any other phone

For additional SMB VoIP information visit Cisco. If you would like to talk to a Cisco Specialist regarding an upcoming project, then simply contact us

Equipment

For VoIP, you need a broadband Internet connection, plus a traditional phone and an adapter; a VoIP-enabled phone; or VoIP software on your computer.

Security and Service Quality

Most consumer VoIP services use the Internet for phone calls. But many small businesses are using VoIP and unified communications on their private networks. That's because private networks provide stronger security and service quality than the public Internet.

Versus Unified Communications

Unified communications systems offer more features and benefits than VoIP. Unified communications brings together all forms of communication regardless of location, time or device. Faxes, e-mail, and voicemail are all delivered to a single inbox. You can integrate your phone and customer relationship management (CRM) systems to improve your customer service, and much more.

How to Protect Your Voice: Tips on IP Phone Security

Cybercriminals will happily tell you: IP telephony, known as VoIP, is a wonderful thing. As hacking voicemail is so lucrative; it exposes private business information and celebrity secrets.

Following are some IP phone security strategies and tips, from Cisco and two Cisco partners that provide VoIP security solutions and services.

Configure Dial Plans and User Profiles

Take advantage of features on your VoIP system that enable security. Essentially:

- Control voice network access by device certificate and/or user name and password.
- Restrict the types of calls allowed on the network, by device, user, and other criteria, such as time of day.

Protect Your Voice Systems

Apply physical and logical protection, such as:

- Set up a firewall and intrusion prevention system (IPS) to monitor and filter authorized and unauthorized VoIP traffic, and track unusual voice activities.
- Lock voice servers physically, and logically for administration.
- Centralise administration and use domain restrictions and two-factor authentication for administrative access, including to credentials, signaling data, and configuration files.
- Regularly install OS updates, and limit software loading on phones.

Use VLANs to Segment Voice Traffic and Separate It from Data Traffic

Some voice systems and switches support device discovery protocols and automatically assign IP phones to voice VLANs.

Encrypt Sensitive Voice Traffic

Apply encryption by segment, device, or user; encrypting indiscriminately can result in excessive network latency or introduce operational overhead and complexity.

Encrypt the signaling at your Internet gateway with Session Initiation Protocol (SIP) over Transport Layer Security (TLS); your service provider's switch fabric may do this.

Encrypt the media (packets) with protocols such as SRTP.

Use VPNs for network connections by remote phones. This is especially important when HTTPS or SRTP is unavailable. Cisco AnyConnect® Security Mobility Client and site-to-site VPNs also work well in this role.

Implement Strict Security Policies with Users.

- **Apply strong passwords to access the voicemail inbox**. Immediately change the default password to a strong password, then change it as often as your company's policy dictates for changing login and email passwords.
- **Delete sensitive voicemail messages as soon as users have listened to them**. Not storing voicemails is the easiest and most effective way to protect them.
- **Immediately report anomalies**. You may not know a phone has been hacked until an employee reports an odd occurrence.

The Cisco Business Edition 6000S is designed specifically to meet the needs of small businesses with up to 150 users. It provides all the essential communication and collaboration capabilities you need. With Business Editions 6000S, you get an easy-to-deploy, manage, and use IP phone system, plus much more.

PBX System

What is a PBX System?

What is a PBX System?

A PBX (Private Branch Exchange) shares and manages multiple lines within a company and automatically routes incoming calls to specific extensions.

IP-based small office PBX telephone systems are highly programmable and can perform sophisticated functions, such as automatic call conferencing, click-to-call, and more.

The Next Generation of Small Office PBX Telephone Systems

Small office PBX telephone systems aren't what they used to be. In fact, they're much more

A conventional PBX requires two networks, one for data and another for voice. However, today's small office PBX telephone systems are often part of an advanced unified communications solution. These small office PBX telephone systems run on Internet Protocol (IP) networks, the same network your company uses for data and Internet connectivity. Instead of requiring two networks, next-generation small office PBX telephone systems only need one—which simplifies network management and administration costs.

Unified Communications: IP PBX and More

Small businesses require specialised features to support their particular workflows. Unified Communications Manager Express from Cisco is designed specifically for small businesses. It combines an IP PBX with robust telephony features that traditional phone systems can't deliver.

The benefits of Cisco Unified Communications Manager Express include:

- Increased productivity with applications such as Cisco Unified CallConnector for Microsoft Office, a presence-based tool that provides call control, location, and status of other users
- Single number reach, which automatically forwards incoming calls to other phones based on your specifications
- An intuitive interface for easy installation and administration
- The ability to easily expand the phone system as business needs change
- A phone and communications solution in a single appliance that's low-cost, reliable, full-featured, and simple to deploy, administer, and maintain.

For additional information visit Cisco. If you would like to talk to a Cisco Specialist regarding an upcoming project, then simply contact us

5 Ways to Tune Your Network with a LAN Switch

Effective switching is essential to handling growing network traffic

Need Speed? Here are 5 Ways to Tune Your Network with a LAN Switch

Any small or midsized business can use LAN switching to sustain the speeds and availability that users need. This presents five ways to do it, from experts at two Cisco Certified Partners that do it every day.

1. Segment Your Network Logically, Using VLANs

A traditional flat network (which places all traffic in a single broadcast domain) can easily overload switch links. Instead, apply your switch's VLAN features to send traffic only where it needs to go, at the speed it needs to go.

You can use a variety of Layer 2 and Layer 3 VLAN types to segment traffic. Many Cisco switches for small and midsized businesses offer all of the following types of VLANs:

- **Protocol**, such as a VLAN dedicated to IP voice or video traffic
- **Devices**, such as a VLAN for wireless clients, a server or printer, or all the equipment on a building floor
- **Port**, such as a VLAN for a department or other group of users
- **Guest**, MAC address, and unauthenticated traffic
- **Dynamic VLAN assignment** that uses the end device's source MAC address to assign switch ports to VLANs
- **Multicast VLAN Registration (MVR)**, which organizes multicast traffic into a dedicated VLAN while maintaining the users' other VLANs. Internet Group Management Protocol (IGMP) Snooping limits the traffic to the devices that need it.

2. Provide the Needed Capacity

Deploy the processing power and bandwidth that your segments, applications, and users need. To reduce latency, congestion, and collisions, apply switch capacity capabilities such as:

- **A fast engine: Nonblocking wire-speed silicon chips.** Switches that forward traffic at wire speed sometimes cost more but can still make a difference in performance.
- **Link Aggregation Control Protocol (LACP).** This standard feature increases available bandwidth by trunking ports.

For additional SMB networking information visit Cisco. If you would like to talk to a Cisco Specialist regarding an upcoming project, then simply contact us

- **Gigabit bandwidth on LAN ports and uplinks.** It took a long time for links to go from 10/100 Mbps to 1 Gbps, but small and mid-sized businesses are now quickly moving to 10 Gbps, and soon it will be more. We recommend you review your infrastructure annually, and pace your CapEx by planning a five-year lifecycle.
- **Stack'em**. If you can, stack your switches to increase throughput and have them operate as one device with a single IP address. The throughput of a stack of Cisco Catalyst 3850 Series Switches can be up to 64 Gbps.

3. Apply Wire-Speed Routing Between VLANs

Inter-VLAN routing is necessary for any user or server that uses multiple VLANs.

Use your switch, not your router software, to route inter-VLAN traffic. A switch's hardware can do the routing, at wire speed. And offloading the router allows it to better handle its WAN connectivity and firewall functions, improving overall network performance.

Absolutely take advantage of both the static and dynamic IP routing capabilities in your switch.

4. Prioritise Applications and Apply Traffic Shaping

Make the best use of your bandwidth by controlling access to it.

You can use the following switch features to set performance parameters based on the traffic's importance and sensitivity to jitter and latency; also check to confirm that the connected devices support the feature:

- Prioritise applications by 802.1p/q tag (a Layer 2 switching capability)
- Prioritise applications by IP header (differentiated services code point (DSCP)/type of service (ToS), a Layer 3 switching capability).
- Shape traffic to delay packets, using criteria such as bandwidth throttling or rate limiting.

5. Set Endpoint Parameters, Preferably Automatically

Set the switch's endpoint ports for optimal performance, using parameters such as storm control, number of devices allowed, quality of service (QoS), and VLANs.

A switch with smart ports can detect new devices and use macros to configure many port parameters accordingly. Having automated QoS settings for IP phones and other devices really helps speed configuration, and you can always adjust the default settings.

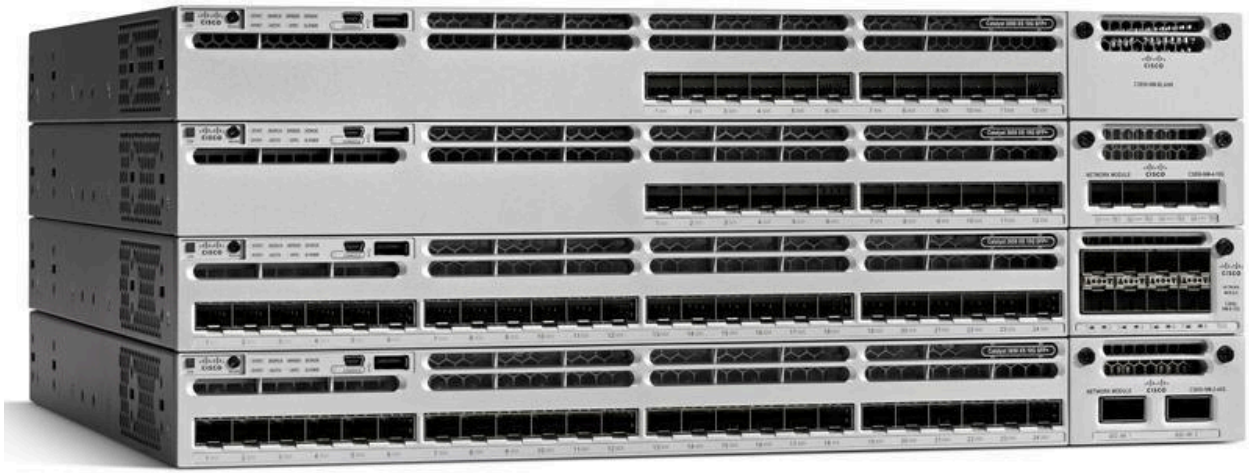
Cisco switches can also connect endpoints using the Cisco Discovery Protocol. It recognises Cisco devices and pulls the data relevant for optimal performance connections, fast problem solving, and efficient network management."

Integrate Your Switching, Reduce Expenses

Applying these five tips--in combination with Simple Network Management Protocol (SNMP) or other monitoring and management tools as well as switch security features such as dynamic Address Resolution Protocol (ARP) inspection, IP Source Guard, and Dynamic Host Configuration Protocol (DHCP) Snooping to thwart attacks--can produce awesome network performance. And help your company save money.

Move into the Fast Lane

When you need to speed up your network, Cisco Certified Partners can help you make adroit switching and infrastructure moves--including network assessment and design, solution financing and implementation, and onsite support and/or managed services.



Cisco Catalyst 3850 Switch

Thank you for reading

Cisco's SMB Networking Basics