Newer Cisco SBA for Government Guides Available

This guide is part of an older series of Cisco Smart Business Architecture for Government. To access the latest Cisco SBA for Government Guides, go to http://www.cisco.com/go/govsba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

IP Addressing Guide

SBA FOR GOVERNMENT

Revision: H2CY10

The Purpose of This Guide

This guide introduces you to the basics of IP addressing and prepares you to create an IP addressing plan for your network.

This guide is a concise reference on IP addressing best practices, including:

- The basic concepts of IP addressing
- The IP addressing plan used in the Smart Business Architecture (SBA) for Government Foundation lab network
- The steps you should follow to create your own IP Addressing Plan
- How to maintain your IP space as your network evolves

Who Should Read This Guide

This guide is intended for the reader with any or all of the following:

- An agency with 100-1000 connected employees
- Up to 20 remote sites with approximately 25 employees each
- IT workers with a CCNA® certification or equivalent experience

The reader will require any of the following:

- A general understanding of IP addressing and subnetting
- General IP addressing guidance while redesigning an existing network
- Guidance on how to add new services to an existing network
- Assistance planning for the acquisition of an agency that has a different IP address space
- A plan for expansion after running out of IP address space
- An IP address migration path for growth
- An IP addressing plan that can be used in midsize networks as a template for customer deployments

Before reading this guide

BN — Foundation Design Overview

BN — Foundation Deployment Guide

BN — Foundation Configuration Files Guide

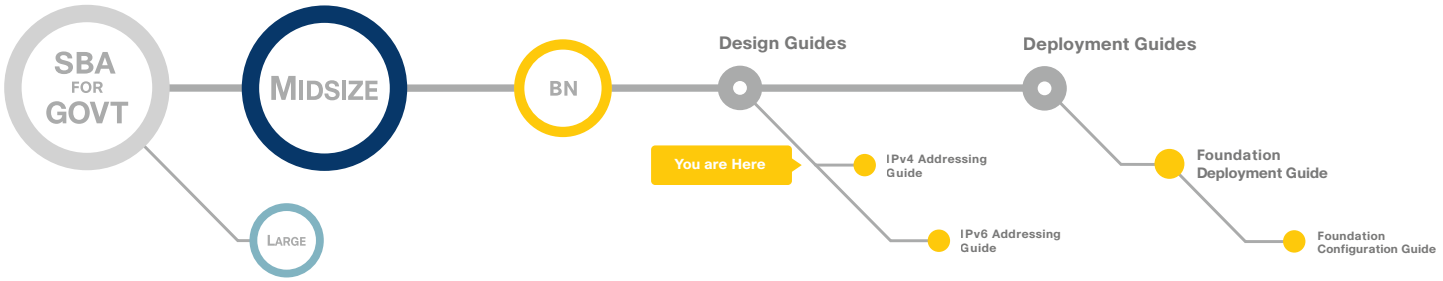


Table of Contents

Introduction

The Cisco® SBA is a comprehensive design for networks with up to 1000 users. This out-of-the-box design is simple, fast, affordable, scalable, and flexible.

The Cisco SBA for Midsize Agencies incorporates LAN, WAN, wireless, security, WAN optimization, and unified communication technologies tested together as a solution. This solution-level approach simplifies the system integration normally associated with multiple technologies, allowing you to select the modules that solve your agency's problems rather than worrying about the technical details.

We have designed the Cisco SBA to be easy to configure, deploy, and manage. This architecture:

- Provides a solid network foundation
- Makes deployment fast and easy
- Accelerates ability to easily deploy additional services
- Avoids the need for re-engineering of the core network

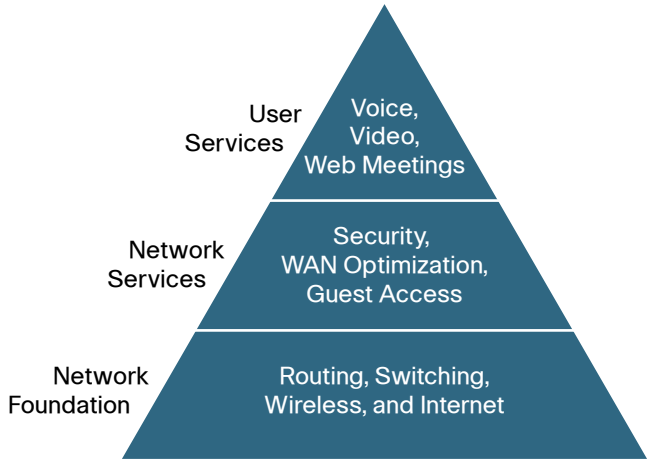
By deploying the Cisco SBA, your agency can gain:

- A standardized design, tested and supported by Cisco
- Optimized architecture for midsize agencies with up to 1000 users and up to 20 branches
- Flexible architecture to help ensure easy migration as the agency grows
- Seamless support for quick deployment of wired and wireless network access for data, voice, teleworker, and wireless guest
- Security and high availability for agency information resources, servers, and Internet-facing applications
- Improved WAN performance and cost reduction through the use of WAN optimization
- Simplified deployment and operation by IT workers with CCNA® certification or equivalent experience
- Cisco enterprise-class reliability in products designed for midsize agencies

Guiding Principles

We divided the deployment process into modules according to the following principles:

- Ease of use: A top requirement of Cisco SBA was to develop a design that could be deployed with the minimal amount of configuration and day-two management.
- Cost-effective: Another critical requirement as we selected products was to meet the budget guidelines for midsize agencies.
- Flexibility and scalability: As the agency grows, so too must its infrastructure. Products selected must have the ability to grow or be repurposed within the architecture.
- Reuse: We strived, when possible, to reuse the same products throughout the various modules to minimize the number of products required for spares.



The Cisco SBA can be broken down into the following three primary, modular yet interdependent components for the midsize agency.

- Network Foundation: A network that supports the architecture
- Network Services: Features that operate in the background to improve and enable the user experience without direct user awareness
- User Services: Applications with which a user interacts directly

IP Addressing Overview

An IP address uniquely identifies a device on an IP network.

Allocating, recycling, and documenting IP addresses and subnets in a network can get confusing very quickly if you have not laid out an IP addressing plan. A sound plan will help you prepare the network foundation to support additional services such as unified communications, wireless access, and enhanced network security.

IP addressing is a Network Foundation service, which makes it core to the network design. It provides the base for all other network and user services. Without the foundation, it would not be possible to interact with network and user services, from picking up the phone using the phone service to reading email using the email service.

By following recommended IP address management standards, you can avoid:

- Overlapping or duplicate subnets
- Nonsummarization in the network
- Duplicate IP address device assignments
- Wasted IP address space
- Unnecessary complexity

Notes

IP Addressing Basics

IP version 4 (IPv4) addresses, which uniquely identify a device on an IP network, are 32 bits in length and are typically communicated in a format known as dotted decimal.

The 32 binary bits are:

- Divided into a network portion and host portion
- Broken into four octets (1 octet = 8 bits)
- Each octet can be converted to binary.

Consider this IP address, which is presented in dotted decimal: **192.168.15.1**. The address breaks down into the following octets:

- 192
- 168
- 15
- 1

The value in each octet ranges from 0 to 255 decimal, or 00000000–11111111 binary. In binary, the same address is represented as: **11000000.10101000.00001111.00000001**.

IP Address Classes

IP addresses are split up into several different categories, including Class A, B, C, D (Multicast), and E (Reserved).

Address classes are defined, in part, based on the number of bits that make up the network portion of the address, and in turn, on how many are left for the definition of individual host addresses.

- In Class A addresses, the first octet is the network portion.
- In Class B, the first two octets are the network portion.
- In Class C, the first 3 octets are the network portion.

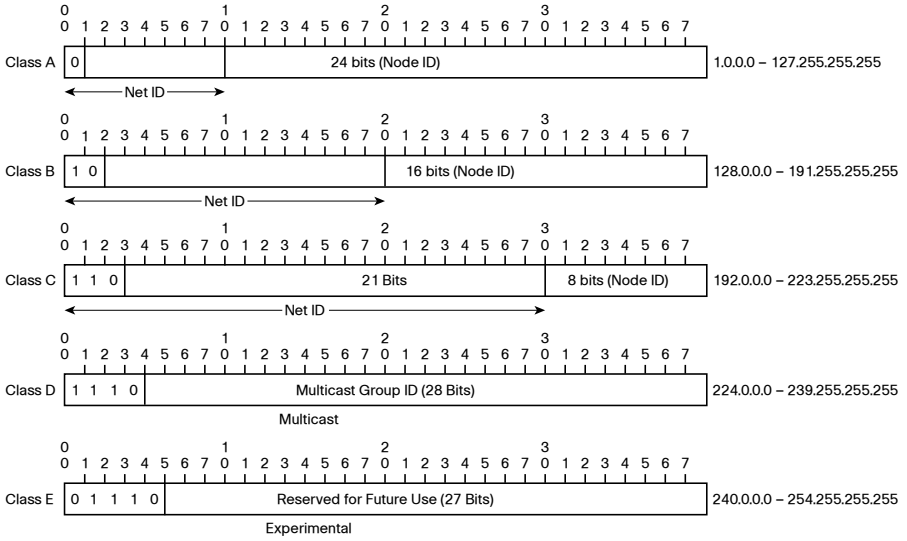
Figure 1 shows how the network and host IDs are different for each class of IP addresses.

Class A has 3 octets for the host portion of the address. Deployed as is, a Class A address represents a very inefficient use of address space, since available Layer 2 technologies cannot easily support this many hosts on a single subnet. Subnetting is utilized to use this address space efficiently.

Tech Tip

IP version 6 (IPv6) is the next generation of IP addressing. IPv6 quadruples the number of network address bits from 32 bits (in IPv4) to 128 bits, which provides enough globally unique IP addresses for every networked device on the planet. IPv6 is an important protocol for the future of IP networking. More information can be found at www.cisco.com/go/ipv6.

Figure 1. Classful Addresses



Private IP Addressing

The Internet Assigned Numbers Authority (IANA) has reserved a number of IPv4 network ranges as private. These network addresses are routed in the public Internet as defined in RFC 1918.

These network ranges, known as RFC 1918 spaces, are reserved for organizations that want to build an internal network infrastructure based on TCP/IP without using public IP space.

RFC 1918 space includes the following three blocks of IP address space:

- 10.0.0.0 – 10.255.255.255 (10.0.0.0/8), which allows the greatest flexibility with the equivalent of 255 Class B address spaces to be used as needed.
- 172.16.0.0 – 172.31.255.255 (172.16.0.0/12), which allows for 16 Class B address spaces.
- 192.168.0.0 – 192.168.255.255 (192.168.0.0/16), which allows for one Class B address space.

By universally recognizing these ranges as private and non-routable in the Internet, multiple organizations can use these ranges internally without causing a conflict with public Internet addresses. If an organization attempts to route these networks externally, the traffic is filtered and dropped by the Internet Service Provider.

Since RFC 1918 space is completely private it allows an incredible amount of flexibility when designing a network.

Tech Tip

To allow traffic from hosts that are using private addresses to access Internet hosts using a public address, Network Address Translation (NAT) is required. NAT allows internal hosts to use a few public addresses for Internet access. Public address space is difficult to get and can be expensive so the small pool of public addresses that an ISP allocates must be used sparingly.(Please see NAT in the *Cisco SBA for Midsize Agencies—Borderless Networks Foundation Deployment Guide*). Public addresses are also needed if a Demilitarized zone is required

Subnetting

Subnetting allows you to create multiple logical networks that exist within a single Class A, B, or C network. If you do not subnet, you can only use one network from your Class A, B, or C network, which is simply unrealistic.

Each data link on a network must have a unique network address, with every host on that link being a member of the same network. If you break a major network (Class A, B, or C) into smaller subnetworks, you can create a network of interconnecting subnetworks. Each data link on this network would then have a unique network/subnetwork ID.

To subnet a network, extend the mask using some of the bits from the host ID portion of the address to create a subnetwork ID. For example: given a network of 192.168.5.0/24, which has a mask of 255.255.255.0, you can create subnets in this manner:

```
192.168.5.0     - 11000000.10101000.00000101.00000000
255.255.255.224 - 11111111.11111111.11111111.11100000
-----------------------------------------[sub]------
```

The address on the left is in dotted decimal notation and the binary representation is on the right. When planning IP subnetting, sometimes it is easier to visualize the different portions of the network address when looking at the binary format. The subnet mask is also represented in dotted decimal and binary. Any address bits that have corresponding mask bits set to 1 represent the network ID. Any address bits that have corresponding mask bits set to 0 represent the host ID.

By extending the mask to be 255.255.255.224, you've taken three bits (indicated by sub) from the original host portion of the address and used them to make subnets. With these three bits, you can create eight subnets. With the remaining five host ID bits, each subnet can have up to 32 host addresses. A single subnet can be split up into eight 32-host subnets. Eight 32-host subnets, however, may not be flexible enough. For example:

```
192.168.5.0 255.255.255.224 address range 0 to 31
192.168.5.32 255.255.255.224 address range 32 to 63
…
192.168.5.224 255.255.255.224 address range 224 to 255
```

Tech Tip

There are two ways to denote subnet masks:

- Since you are using three bits more than the originally specified 255.255.255.0 mask, the mask is now 255.255.255.224.
- The mask can also be denoted as /27 as there are 27 bits that are set in the mask and is denoted with the notation prefix/length. For example: 192.168.5.32/27 denotes the network 192.168.5.32 with a mask of 255.255.255.224.

When appropriate, the prefix/length notation is used to denote the mask throughout the rest of this document.

Variable Length Subnet Masks (VLSMs)

Variable Length Subnet Masks (VLSMs) allow you to use different masks for each subnet, and thereby use address space efficiently. With private address space, it is rarely necessary to shrink below a /24 subnet mask as space is plentiful. Use VLSM to:

- Create a larger subnet of more than 255 host addresses
- Create very small subnets for WAN links
- Configure loopback addresses

VLSM Example

Given the 192.168.5.0/24 network and requirements below, develop a subnetting scheme with the use of VLSM:

- netA: must support 330 hosts
- netB: must support 6 hosts for a point-to-point WAN link supporting Hot Standby Router Protocol (HSRP)
- netC: must support 2 hosts for a T1 circuit to a remote site
- netD: must support a single address for a router loopback

The first step is to determine what mask allows the required number of hosts.

- netA: requires a /23 (255.255.254.0) mask to support 510 hosts
- netB: requires a /29 (255.255.255.248) mask to support 6 hosts
- netC: requires a /30 (255.255.255.252) mask to support 2 hosts
- netD*: requires a /32 (255.255.255.255) mask to support 1 address

*Note: This is a special configuration reserved for loopback addresses.

The easiest way to assign the subnets is to assign the largest first. For example: You can assign in this manner:

- netA: 192.168.5.0/23 address range 5.0 to 6.255
- netB: 192.168.7.0/28 address range 0 to 7
- netC: 192.168.7.8/28 address range 8 to 11
- netD:192.168.7.12/32 address of 12

Reader Tip

For specific information on IP addressing and variable length subnet masks, please reference "IP Addressing and Subnetting for New Users," Document ID: 13788, http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800a67f5.shtml.

Voice Overlay Subnets

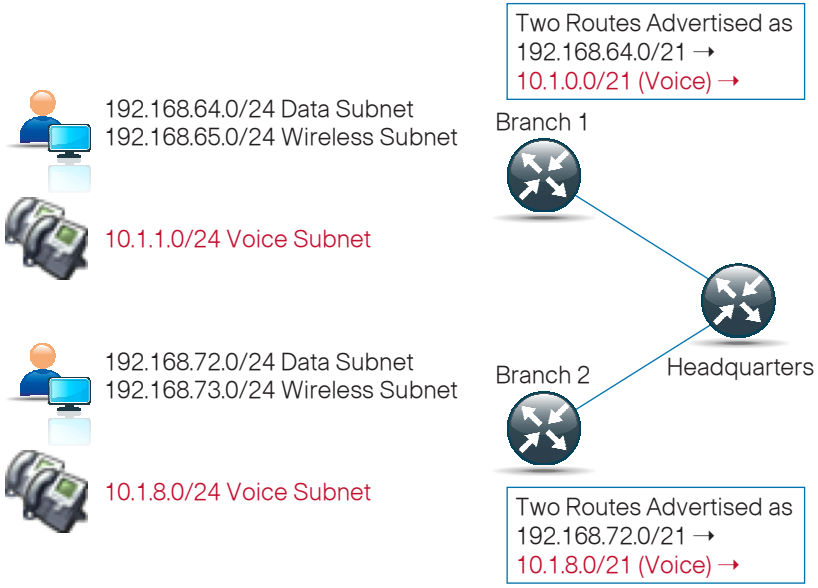
When adding a new service such as unified communications or quality of service, it is very helpful to overlay different private IP addressing on an existing IP addressing scheme. For example:

- All voice could be on its own subnet range from 10.0.0.0 or 172.16.0.0.
- A simple mask covering all 172.16 and 10.0.0.0 addresses could be used to classify voice traffic across all sites.

Such an approach can also help solve scalability issues with an addressing plan that was not designed to accommodate enough subnets and end hosts for each site to support the new service.

For example: Two existing branches have wired and wireless access and would like to add voice. They have reserved all of their 192.168 subnet space. The voice subnet is overlaid in a 10.X.X.X address range highlighted in red in Figure 2.

Figure 2. Voice Overlay Subnets



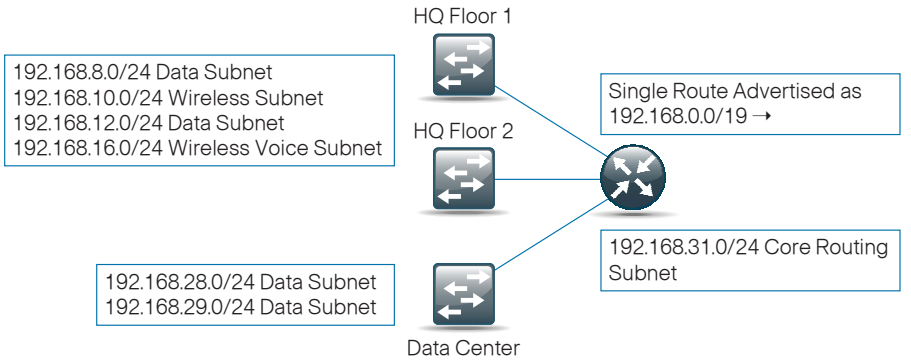
Summarization

Summarizing IP addresses ensures that there are no entries for child routes, which are routes that are created for any combination of the individual IP addresses contained within a summary address, in the routing table. This summarization reduces the size of the table and allows the router to handle more routes.

In a small network, summarization is often not necessary at first. However, as soon as the network starts to expand, it needs to scale. Summarization provides the ability to scale IP address space from a single-site headquarters to an additional remote site location and then include hundreds of remote sites.

An example of summarization from the network headquarters out to the remote site locations is shown in Figure 3. Normal IP routing advertisement would have sent out seven routes in the routing table. With summarization, all seven routes are summarized back to the headquarters as a single route.

Figure 3. IP Summarization at Headquarters



Summarization can be used on all spaces if the addressing is contiguous or specific to a location. If existing IP addressing does not allow for summarization, document it and leave it be while you deploy future IP space that can be summarized.

Tech Tip

Be sure to turn off auto-summarization in the Enhanced Interior Gateway Routing Protocol (EIGRP) if there are noncontiguous IP spaces.

IP Multicast

IP Multicast is a bandwidth conservation technology that reduces traffic and server loads by allowing a single stream of information on the network to be received by thousands of users.

Applications that take advantage of multicast technologies include:

- Video conferencing
- Corporate communications
- Music on hold
- Distance learning
- Distribution of software, stock quotes, and news

IANA has reserved the range of 239.0.0.0/8 as Administratively Scoped addresses for use in private multicast domains. These addresses are similar in nature to the reserved IP unicast ranges (such as 10.0.0.0/8) defined in RFC 1918 and will not be assigned by the IANA to any other group or protocol.

An agency multicast IP addressing plan, just like a unicast addressing plan, needs to be provisioned for the entire network.

Reader Tip

For more information on IP Multicast, please visit www.cisco.com/go/multicast.

Notes

Managing IP Addresses

With proper planning, the IP network can be more organized, easier to set up, and easier to troubleshoot than user and network services.

Before explaining how to create your own IP addressing plan, we will relate the technical concepts already described to an actual network design, using the SBA design as the network example.

IP Addressing in the SBA

Although SBA uses 192.168.0.0 as the example address range, you can apply these same principles to the other ranges. Your requirements will determine the range or ranges you implement.These same principles apply to a public address range, but most midsize agencies will likely deploy private addresses internally and use public addresses from a service provider when connecting to a public network such as the Internet.

The SBA IP addressing ranges are assigned from the 192.168.0.0/16 range of private addresses to cover the following main sections of the network:

- Headquarters
- WAN
- Remote Sites
- Data Center
- DMZ
- Disaster Recovery Site
- Security
- Voice

The chosen address space is allocated in contiguous IP address blocks to each of these areas to promote IP summarization.

- Headquarters is assigned addresses in the 192.168.0.0/19 block, allowing for 32 /24 subnets.
- The disaster recovery site is assigned a separate block.
- Branches are assigned an 8 subnet block 192.168.64.0/21.
- For the Network Foundation:
  - Data Subnets are required for wired and wireless users.
  - Wireless access may require additional subnets for guest access, quarantine of nonsecure devices, etc.
  - Subnets for end-user access are commonly specified as /23 or /24, and allow for 253 hosts or 509 hosts, respectively with a single router address being used.
  - Voice Subnets are separate from data networks to simplify configuration of quality of service, and to avoid having IP phones contributing to the lack of space on already congested data subnets.
  - One subnet for wired data and one subnet for wireless allows for flexibility. Subnets can be /24 or /23, and allow for 253 hosts or 509 hosts, respectively with a single router address being used.

Table 1 presents an example of IP address assignment and summarization.

Following the table, you can find a diagram of the SBA architecture with sample IP subnet assignment and summarization. Summarization can be extrapolated to each remote site and across a campus as required. To add another remote site, simply assign another block of eight addresses. For example: Branch two would be assigned 192.168.72.0/21.

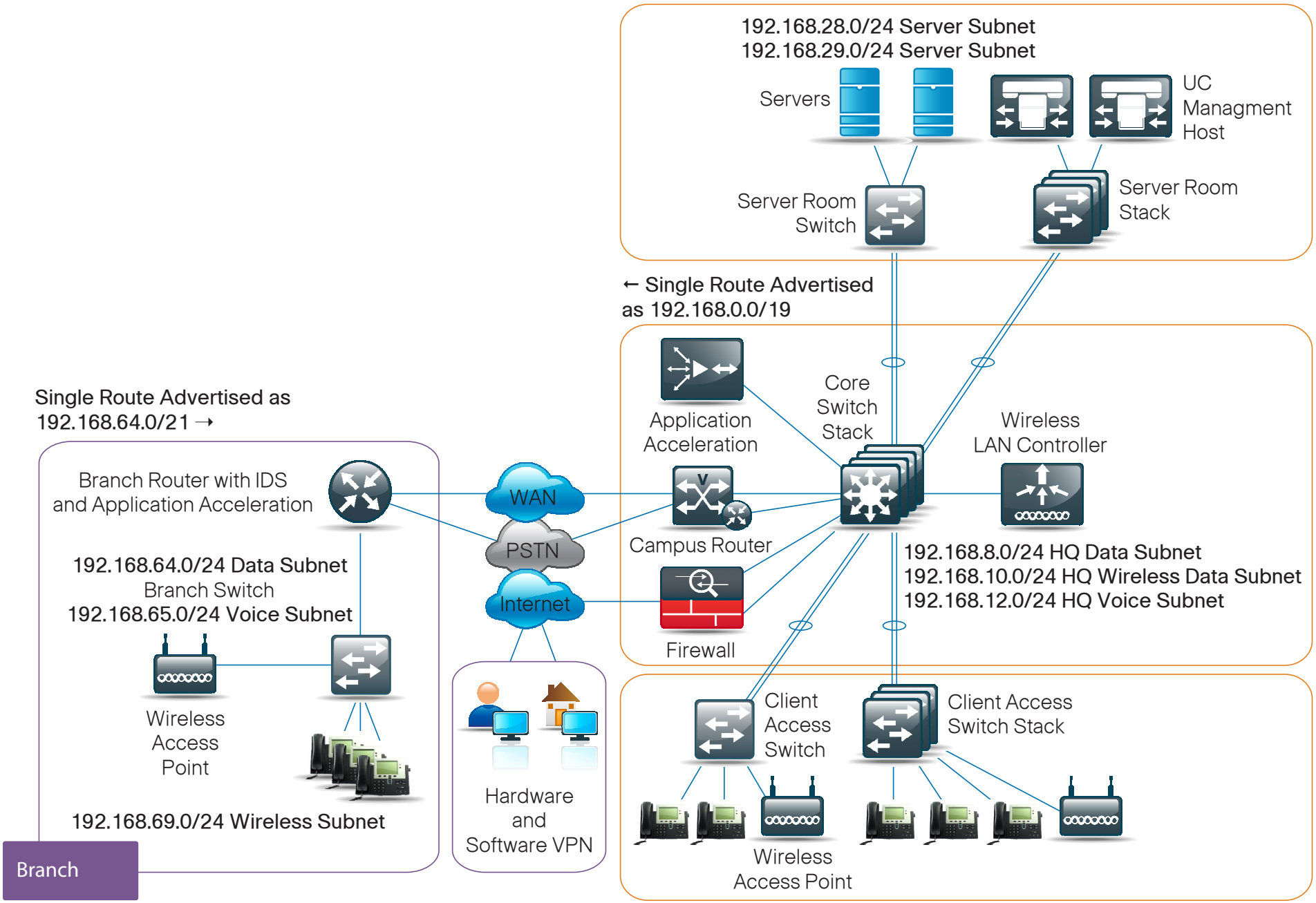
Table 1. SBA Assigned IP Addresses

Location	VLAN	Subnet	Department	Summary Address
Headquarters				102.168.0.0/19
	1	192.168.1.0/23	HQ Management	
	8	192.168.8.0/24	HQ Data	
	10	192.168.10.0/24	HQ Wireless Data	
	12	192.168.12.0/24	HQ Voice	
	14	192.168.14.0/24	HQ Wireless Voice	
	16	192.168.16.0/24	Wireless Guest	
	28	192.168.28.0/24	Server Farm A	
	29	192.168.29.0/24	Server Farm B	
	31	192.168.31.0/24	Core Routing	
Branch 1				192.168.64.0/21
	64	192.168.64.0/24	Branch 1 Data	
	65	192.168.65.0/24	Branch 1 Wired Voice	
	66	192.168.66.0/24	Branch 1 Reversed	
	67	192.168.67.0/24	Branch 1 Reversed Security	
	68	192.168.68.0/24	Branch 1 Reversed	
	69	192.168.69.0/24	Branch 1 Wireless Data	
	70	192.168.70.0/24	Branch 1 Wireless Voice	
	71	192.168.71.0/24	Branch 1 loop-backs in 32's	

The SBA design as seen in the SBA for Midsize Agencies — Borderless Networks Foundation Design Guide is shown in Figure 4 with the addition of IP address assignments and route summarization.

Notes

Figure 4. SBA Design with Assigned IP Addresses and Summarization



Process

Creating an Addressing Plan

1. Define Addressing Standards
2. Plan Range
3. Allocate IP Space
4. Document Plan

It's important to approach the IP addressing plan with the entire network in mind, not just the foundation. Proper planning of IP address space across each of the layers is critical to ensuring their interaction is seamless and integrated. Within each subnet range, the plan should account for:

- Subnet sizes
- Subnet assignment
- Static address assignments for network devices
- Dynamic address assignments

Well-planned and documented IP address space can yield many saved hours of troubleshooting time.

Procedure 1 Define Addressing Standards

Using consistent standards across the different locations simplifies overall maintenance and troubleshooting of the network.

Step 1: Create standards for IP address assignments within each subnet range. Some standards you may consider applying include:

- For ease of identification, VLANs can be created to match the third octet of the IP subnet. For example: VLAN 71 for x.x.71.x. This results in a self-documenting design.
- Routers, gateways and Hot Standby Router Protocol (HSRP) virtual addresses within a subnet are assigned the first available addresses within the range.
- Printers and other fixed address assignments.
- Dynamic address ranges for Dynamic Host Control Protocol (DHCP). For example: All user subnets may be /24 subnets with 253 available address assignments for end hosts.
- Routers may be assigned the .2 and .3 addresses, and the HSRP address assigned the .1 address.
- Printers may be assigned the .5 through .9 addresses.
- DHCP may range from .10 through .254 addresses.

Step 2: Define a consistent, structured naming convention and DNS for devices. This helps:

- Create a consistent access point to routers for all network management information related to a device.
- Reduce the opportunity for duplicate IP addresses.
- Create simple identification of a device showing location, device type, and purpose.
- Improve inventory management by providing a simpler method to identify network devices.

Step 3: Identify DHCP ranges and add them to DNS, including the location of the users. This range may be a portion of the IP address or a physical location. An example might be dhcp-bldg-c21-10 to dhcp-bldg-c21-254, which identifies IP addresses in building C, second floor, wiring closet 1. Alternatively, the precise subnet or variation thereof can be used for identification.

Step 4: Document all standards that you develop and reference them on all network engineering plan documents to help ensure consistent deployment.

Procedure 2 Plan Range

There is no incorrect private subnet to allocate, but some choices provide more flexibility than others.

Step 1: Determine which address space to use by evaluating all of the user and server requirements. Consider the following examples:

- The 192.168.0.0 range is a well used address range by many agencies and network equipment vendors. This address range has a lower number of host addresses available, which may become an issue as an agency grows or when a merger occurs with another agency using the same range.
- If you have the luxury of starting from scratch, consider the 10.0.0.0 range to allow for the most flexibility. The 10.0.0.0 range allows for many more hosts in the same range, which provides more flexibility when sub-netting. For example: each branch or building needs to have a consistent host range and the 10.0.0.0 network provides this flexibility.
- In many cases, organizations may have multiple different address RFC1918 spaces in their network. To simplify configuration and trouble-shooting, it is easier to work with one range from RFC1918 space and use summarization. Using multiple IP ranges from different address spaces is not a problem if the addressing plan is well documented.
- Whatever address space is selected or inherited, there may be an advantage to start somewhere other than the beginning of the range when choosing network numbering. In case of a merger with another agency that is using IP addressing from 10.0.0.0 or 192.168.0.0, it is advisable not to start at the beginning of the range, to decrease the chance of address conflicts.

Procedure 3 Allocate IP Space

Step 1: Carefully define the size of the IP space with public addresses as it is available only in a finite amount. Be sure to take into account that:

- Private addresses are not constrained
- For ease of use, a /24 mask should be used as a minimum for user subnets.
- End devices always grow in number, so there is no reason to set a low limit on the number of private addresses, since they are readily available.
- Wide-Area Network connections have much smaller requirements for IP addresses. In general, a point-to-point network connection between two sites has two IP addresses in use. If HSRP is used with redundant routes on each side, the number of addresses increases to six, three for each side of the link.
  - /30 subnet allows for two usable IP addresses
  - /29 subnet allows for six usable IP addresses

Step 2: Reserve a subnet for physical security. These requirements can be as simple as a subnet to control door access to a building or something more complex like video surveillance for the entire building. Even if physical security is not required at the initial setup, you should still complete this step.

Step 3: Reserve a subnet for facilities. This subnet addresses Physical Plant requirements such as remote power control, air conditioning, and facilities monitoring, which can now be monitored with new technology on the IP network.

Step 4: Allocate public addresses for all production networks in the Demilitarized Zone (DMZ), which is the network or networks situated between an ISP edge router and agency firewalls. An alternative is to utilize NAT.

Step 5: Allocate a subnet for Remote Access, which is generally set up as a Virtual Private Network (VPN).

Step 6: Allocate a subnet for Network Management to provide access to network devices such as Ethernet switches, firewalls, routers, etc. This subnet will allow for easy management with a separate logical network. SBA uses VLAN 1 for management of network devices.

Tech Tip

Where practical, a separate physical network can also be used for management.

Step 7: Create a loopback address to make it easier to manage a single address for a router with multiple interfaces.

Loopbacks:

- Are always up.
- Are reachable even if a single interface goes down when the router has multiple interfaces.
- Can provide a single source address for voice applications, network management, routing, etc.
- Give continuity, for example, to a voice gateway in a router. If the voice gateway is configured for the WAN interface and it goes down, the voice gateway also goes down. Loopbacks prevent these problems as they stay up as long as the router stays up and is reachable over an interface.
- Need to be advertised by the IP routing protocol.
- Can also be used for unnumbered interfaces. For example: The AIM-IPS modules use unnumbered interfaces that refer to a loopback interface for their IP addresses.

Loopback interfaces can be assigned an address of /24 or up to a single /32 (be sure to summarize if using /32 loopbacks). Configure loopback interfaces as the source IP address for traps, Secure Shell (SSH), and Simple Network Management Protocol (SNMP).

Note that WAAS modules use a special kind of loopback interface in the ISR that connects the module to a routed interface separate from the physical interfaces, and typically requires a /30.

Procedure 4 Document Plan

Step 1: Document the entire IP address space in a spreadsheet showing site-allocation, usage, and available subnets for each subnet size within the block, along with summary addresses for each particular block of addresses.

An example of a simple IP addressing worksheet is available in the Appendix of this guide.

Process

Maintaining and Growing Network Space

1. Resolve Overlapping Address Ranges
2. Increase the Number of IP Addresses
3. Merge with Another Agency

Once the IP addressing plan is in place, you are ready to resolve situations as they come up. The following procedures explain how to handle some of the special situations you may encounter.

Procedure 1 Resolve Overlapping Address Ranges

If two address ranges overlap, two scenarios may be in place.

The first possible scenario is that the ranges are the same but the subnets used within these ranges are unique to each site and there is no overlap as seen in Figure 5. This scenario is not optimal, but the networks should still be able to communicate. In this scenario complete the following steps:

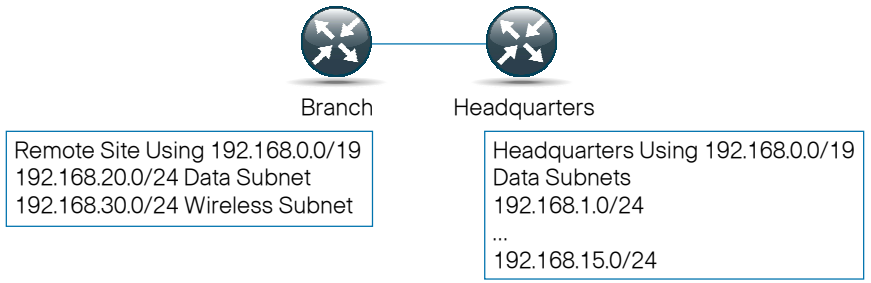
Step 1: Remove summarization from both sides if it contains any of the overlapping IP space.

Note: This step is enough to allow the networks to communicate while step 2 is being completed.

Step 2: Renumber the overlapping space.

Step 3: Reinstate the summarization.

Figure 5. Overlapping IP Address Space, Non Conflicting



The second possible scenario is that the spaces conflict, meaning they use the same subnets as seen in Figure 6. This is a real problem. Unlike the simple solution of the previous example, this one is more complex, but it can be overcome.

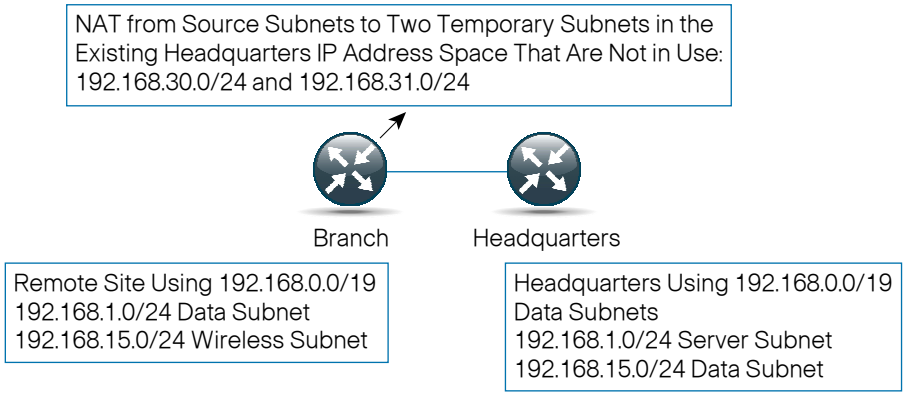
Complete the following steps to resolve the situation:

Step 1: Use NAT from the conflicting site in a new nonconflicting IP address space as a temporary workaround.

Step 2: Renumber the conflicting space.

Step 3: Once the hosts are renumbered into the new address space, turn NAT off.

Figure 6. Overlapping IP Address Space, Conflcting



Procedure 2 Increase the Number of IP Addresses

As an agency grows, so does its need for IP addresses. If your plan includes provisions for expansion, growth is not a problem.

If the hosts are all DHCP and the next available subnet has been reserved, complete the following steps:

Step 1: A data subnet may have had an adequate amount of IP addresses when it was first deployed, but as the agency grows it becomes apparent that the /24 assigned needs more room. One way is to expand the subnet by changing the mask to a /23 to double the IP addresses available. The router interface configuration will get reconfigured for the new mask and routing verified.

Tech Tip

This change of mask can only be done if the network IP planning took this future expansion into account when the network was designed. If it was planned, the hosts are all DHCP, and the next available subnet has been reserved..

Step 2: With the router configuration complete, address the hosts. With the hosts configured for DHCP, they receive their IP addresses and subnet masks from the DHCP server.

Step 3: Change the mask and add the additional range to the DHCP server. Note that the DHCP mask needs to be changed on the DHCP server and not on every host.

Step 4: Once the mask has propagated when DHCP renews to the existing hosts, they will now be able to have visibility to the expanded range in DHCP. At this point , expand the DHCP range to the larger set of IP addresses so they can be assigned.

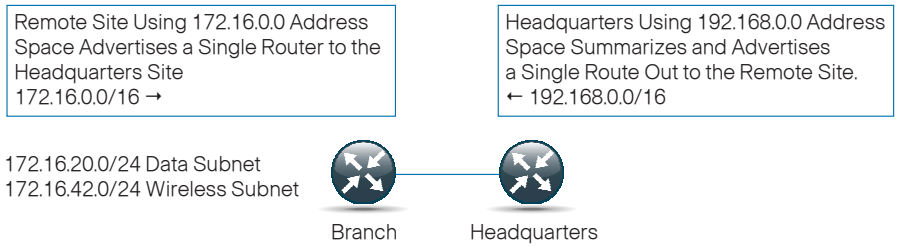
Tech Tip

If the hosts are not configured for DHCP, each host will have to be visited or they will not be aware of hosts and gateways on the subnet.

Procedure 3 Merge with Another Agency

Consider the example depicted in Figure 7. Assume a new location was acquired by an agency that already has a network with 172.16.20.0 and 172.16.42.0 address space in use. You would need to either renumber the address space to fit within the active 192.168.0.0 space currently deployed at the headquarters, or simply summarize the address space at the border to the remote site as 172.16.0.0/16.

Figure 7. Merging with Different IP Space



Reader Tip

For more information on IP addressing, please see the following resources:

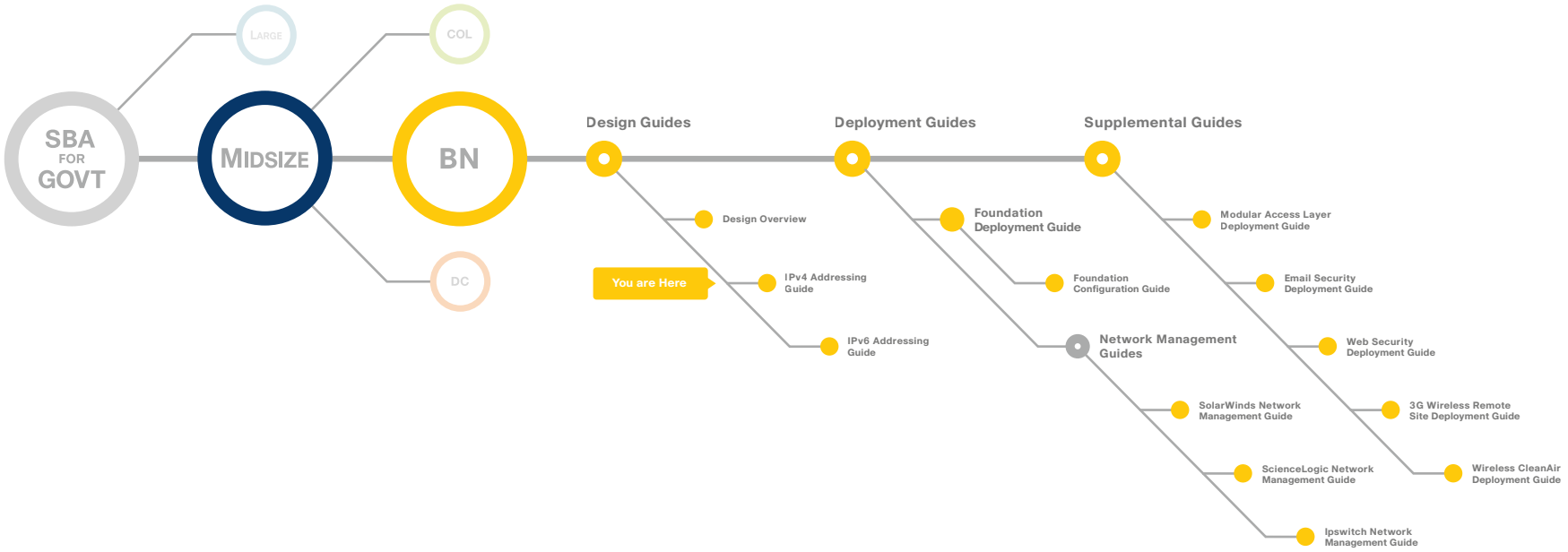
- Routing and Switching Best Practices: How Cisco IT Deploys IP Addressing in the Enterprise, http://www.cisco.com/web/about/ciscoitatwork/downloads/ciscoitatwork/pdf/Cisco_IT_IP_Addressing_Best_Practices.pdf
- Configuration Management: Best Practices White Paper http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a008014f924.shtml
- "General Design Considerations for Secure Networks", in ***Network Security Architectures***, a Cisco Press book.

Notes

Appendix A: Subnet Design Worksheet for SBA

Location	VLAN	Subnet	Department	Summary Address

Appendix B:
SBA for Midsize Agencies Document System



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

C07-641123-00 12/10