CHAPTER 4

Planning Phase

Chapter 3, "Large-Scale Enterprise Requirements for IP Telephony," presented the XYZ, Inc. current network scenario and its high-level requirements for its future IPT network. Typically, customers provide these requirements in the Request for Proposal (RFP); otherwise, you can gather the requirements by meeting the voice architecture group in the customer organization. Understanding these requirements is critical to planning and designing a scalable and optimized IPT network.

Before you begin studying the planning phase, you need to understand the approach that we have taken to analyze the network infrastructure of XYZ in the planning phase.

The network infrastructure topologies of XYZ that were presented in Figures 3-2 and 3-3 show that the network is designed with full redundancy, that all network elements are Cisco switches and routers, that all devices understand QoS, etc. This topology is 100 percent ready to deploy IP Telephony (IPT). You will not find a network like this in the real world; instead, you will see networks that pose many challenges. Some of the common challenges are the following:

- Networks that are deployed with non-Cisco switches—you are required to provide a solution to deploy Cisco IPT products
- Switches that do not understand Layer 3 QoS
- Switches that cannot provide inline power to Cisco IP phones
- Networks that are deployed without following the recommended designs/best practices

To provide you with answers to some of the preceding challenges, we could have introduced some of these problems into the XYZ network. However, doing so would have made it harder to keep up with the chapter flow. Hence, the approach taken is as follows:

- Describe the best practices in making the network infrastructure ready to support IPT
- Provide alternate solutions and suggestions for commonly faced problems and challenges, such as those described in the preceding list, at appropriate places in the chapter

This chapter guides you through various tasks involved in the planning phase and discusses the best practices and the steps you need to follow at every layer of the network to make the network infrastructure ready to run the Cisco IPT solution.

To complete the planning phase for XYZ, this chapter uses the information presented in Chapter 3 along with the input provided by the customer to the following two questionnaires:

- Network Infrastructure Analysis Questionnaire found in Appendix B, "IPT Planning Phase: Network Infrastructure Analysis Questionnaire".
- Telecom Infrastructure Analysis Questionnaire found in Appendix C, "IPT Planning Phase: Telecom Infrastructure Analysis Questionnaire".

Getting Started

The first step in the planning phase is to understand the high-level business and technical expectations and requirements for the future IPT network, which include the following:

- Company vision, goals, and forecasted growth
- The plan for voice and data networks over the next 3 to 5 years
- Solution expectations
- Deployment and timing
- Financial expectations

To simplify the discussion for this case study, assume that XYZ expects its workforce to grow 5 to 10 percent every year. XYZ requires that the new IPT system must emulate the functionality of the current PBX, voice-mail, and application systems, be scalable, and provide additional services and features that improve employee productivity. The new technology update project at XYZ received approval from the company's financial board to support the funding for the IPT project, and there are no major budget constraints.

NOTE When you are working with a customer, you might have to study some of these requirements carefully. For example, a customer might have limited funding available for the IPT project, in which case you might have to adjust the hardware needed in the infrastructure and size the other expensive equipment so that the total cost of the project falls within the approved budget. In some cases, you might also have to choose a phased migration to IPT to minimize the costs.

After you understand the high-level business and technical expectations of the customer, the next step is to conduct meetings with the engineers and architects in the LAN, WAN, IT, legacy PBX, legacy voice-mail, and applications network groups. During these meetings with the various groups, you should make sure that the high-level requirements that you received from the customer in the RFP are accurate. Most importantly, make sure that you understand how the customer's existing network infrastructure is built so that you can identify the gaps in the infrastructure that need to be filled to support the converged traffic.

Network Infrastructure Analysis

Appendix B includes a Network Infrastructure Analysis Questionnaire that you can use to complete the network infrastructure analysis. (Another term commonly used for this analysis is IP Telephony Readiness Assessment.) The purpose of this assessment is to check whether the customer's network infrastructure is ready to carry the converged traffic. The assessment covers basic LAN switching design, IP routing including power and environmental analysis, and so forth. As a network engineer, you are required to identify the gaps in the infrastructure and make appropriate recommendations before you move forward with the IPT deployment.

The network infrastructure analysis of XYZ is divided into eight logical subsections:

- Campus network infrastructure
- QoS in campus network infrastructure
- Inline power for IP phones
- Wireless IP phone infrastructure
- WAN infrastructure
- QoS in WAN infrastructure
- Network services such as Domain Name Service (DNS) and Dynamic Host Configuration Protocol (DHCP)
- Power and environmental infrastructure

After reviewing the preceding list, you might be wondering why planning for the IPT network includes analyzing campus infrastructure (Layers 1, 2, and 3), WAN infrastructure, LAN and WAN QoS, and network services. The analysis of the aforementioned network infrastructure components is required during the planning phase of the IPT network deployment to identify the gaps in the current infrastructure to support the additional voice traffic on top of existing data traffic. After identifying the gaps, you need to make the appropriate changes in the network, such as implementing QoS in LAN/WAN, upgrading the closet switches to support QoS, and supporting the in-line power.

Chapter 1, "Cisco IP Telephony Solution Overview," discussed how legacy voice and data networks are migrating to new-generation multiservice networks. Chapter 1 also briefly discussed some of the requirements of the migration to multiservice networks. This section describes the technologies, features, and best practices to design a scalable and optimized infrastructure, which caries in parallel over the same IP infrastructure both real-time, delay-sensitive voice and video traffic and nonreal-time, delay-tolerable data traffic (i.e. FTP, e-mail, and so forth).

When you introduce real-time, delay-sensitive voice and video traffic into ensuring that your infrastructure is hierarchical, redundant, and QoS enabled, it becomes even more important to provide a scalable and redundant network infrastructure with fast convergence. Large network infrastructures use the access, distribution, and core layers at Layer 2 and Layer 3 for isolation, with redundant links and switches at these layers to provide the highest level of redundancy.

This isolation helps you to summarize the IP addresses and traffic flows at different layers and troubleshoot the issues in a hierarchical manner when they occur.

TIP Small networks do not have to have access, distribution, and core layers at Layer 2 and Layer 3. Networks can collapse the core and distribution layer functionality in the same switch, depending on the size of the network. The redundancy and QoS requirements remain the same.

According to the International Telecommunications Union (ITU) G.114 recommendation, you need to achieve 0- to 150-ms one-way delay for the voice packet. You can achieve this delay value only by making sure that your network infrastructure is hierarchical, redundant, and QoS enabled. If you are transporting voice across the WAN links, you also should have adequate bandwidth to carry the additional voice traffic.

Campus Network Infrastructure

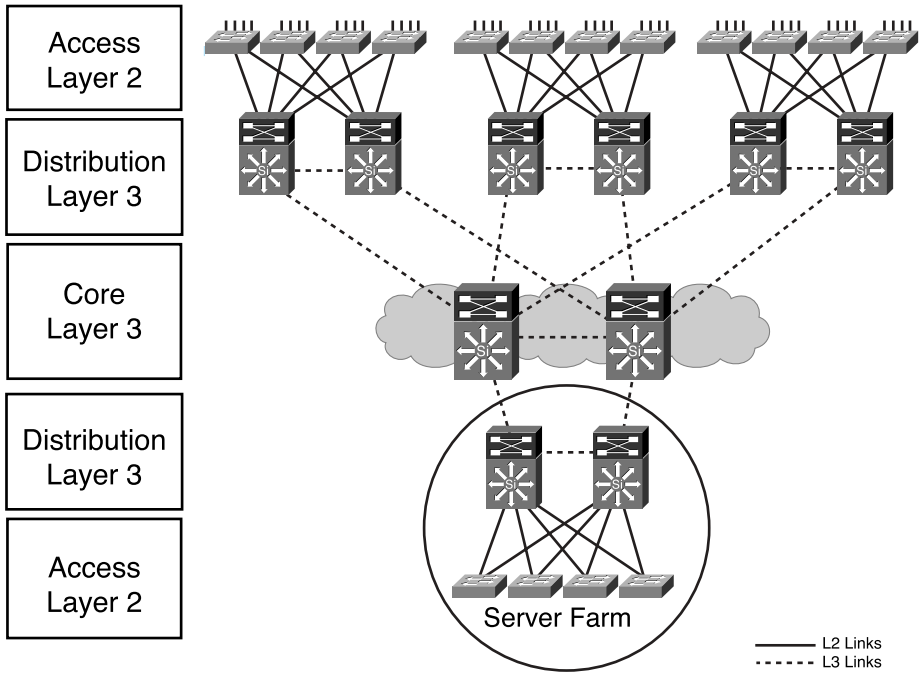
The best way to start the campus network infrastructure analysis of XYZ is by analyzing the XYZ current multilayer infrastructure. Figure 4-1 depicts a well-designed multilayer network, which provides redundancy and high availability. Access to the distribution layer of this network is Layer 2, and access to the rest of the network is Layer 3.

When you analyze this network, one of the main concerns you should have is the number of points of failure in this network. More points of failure in a network translates to a less highly available network.

As you can see in Figure 4-1, this network has one single point of failure, which is the access layer switch. If the access layer switch fails, you lose the devices connected to the access layer switch. On the other hand, if you lose an uplink to a distribution layer switch or if a distribution layer switch fails, you will be fine, because you have redundant links and redundant switches in the distribution layer. If you lose an uplink to the core layer switch or if a core layer switch fails, you can still reach the rest of the network, by using the redundant links and switches at the core layer, and continue the communications.

In IPT applications, voice traffic uses IP. If your primary path fails and you have another path to the destination, you can reroute these VoIP packets to the destination, and you will not necessarily lose the calls. You can achieve this goal if your IP network can converge fast enough and correct itself. The advantage of having an IP network with fast convergence and redundant links is that if someone pulls a link from a distribution layer switch or any other device in the network, IPT users will not notice a difference.

Figure 4-1 *XYZ Multilayered Campus Infrastructure*



The next few sections examine the access, distribution, and core layers of this network and highlight the key points to remember while planning for each layer.

Access Layer

The first thing you should plan for at the access layer is the virtual LANs (VLANs) in the network. A single VLAN should not span multiple access layer (wiring closet) switches in your network. You can have multiple VLANs in one wiring closet switch. By prohibiting a single VLAN from spanning across multiple wiring closet switches, you can limit the spanning tree into the wiring closet switch, which results in increased convergence time.

When you have multiple uplinks from the wiring closet switch to different distribution layer switches, you can use these multiple uplinks for faster convergence and load balancing, resulting in maximized use of redundant links.

The following features on the access layer switches help you to make the network infrastructure ready to support IPT.

Auxiliary VLAN

When you deploy IPT, you connect the IP phones to access layer switches. Some of the Cisco IP Phones also have a PC port on the back of the phone to connect the user workstations. The challenge to address in this scenario is to separate the traffic coming from the IP Phones with the data traffic coming from the user workstations. To address this scenario, Cisco switches support a feature called auxiliary VLAN, or voice VLAN, and the VLAN ID assigned to this voice VLAN is referred to as voice VLAN ID (VVID). In this approach, you create a new voice VLAN on the access layer switch and leave the original data VLAN (access VLAN) untouched.

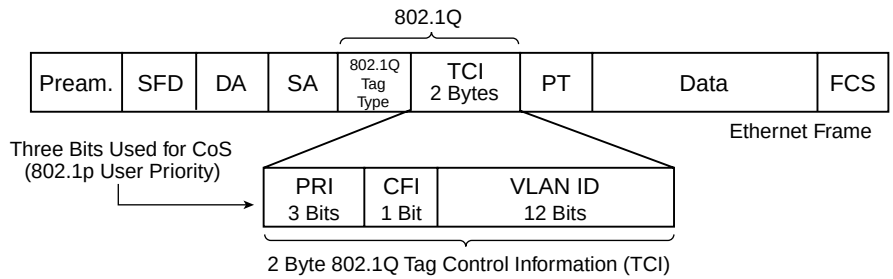
Some of the clear advantages of implementing separate data and voice VLANs are as follows:

- You can configure the differential treatments such as priority queuing for packets in the voice VLAN within network devices to guarantee the voice quality.
- Because the voice traffic will be on a separate VLAN, IP phones can use a separate IP address space altogether. Hence, you do not need to redesign the existing IP addressing scheme that is already deployed for the data network.
- When troubleshooting problems in the network, you can easily recognize and distinguish between data network and voice network traffic packets.
- Creating security policies and access lists is easy because the voice and data subnets are separate.
- Phones do not have to respond to broadcasts that are generated on the data network.

IEEE 802.1Q/p Support

The introduction of the IEEE 802.1Q standard (which defines a mechanism for the trunking of VLANs between switches) includes support for priority in an Ethernet frame. IEEE 802.1Q adds 4 bytes into the Ethernet frame, inserted after the MAC Source Address field, as shown in Figure 4-2.

Figure 4-2 *Layer 2 Classification 802.1Q/p*



The 4 bytes of the 802.1Q field incorporate a 2-byte Ethernet Tag Type field and a 2-byte Tag Control Information (TCI) field. Within the 2-byte TCI field are 3 bits that set the priority of the Ethernet frame. These 3 priority bits are often referred to as IEEE 802.1p or, more commonly, dot1p. Dot1p is a term used to identify support for this priority mechanism in a switch. Note that this is a MAC layer mechanism and, as such, has significance to all devices connected at the MAC layer (such as in a bridged or Layer 2 switched network segment); it does not imply that end-to-end QoS is supported.

These 3 priority bits, also called Class of Service (CoS) bits, can mirror the 3 bits used as the IP Precedence bits in the ToS (Type of Service) field in the IPv4 header, as shown in Figure 4-3. Because the ToS setting is a Layer 3 setting, it can support end-to-end QoS. Ideally, the matching of these fields will allow end-to-end QoS to be provisioned across a network that incorporates both Layer 2 and Layer 3 technologies by mapping CoS to ToS bits and vice versa.

Figure 4-3 *Layer 3 Classification IP Precedence/DSCP*

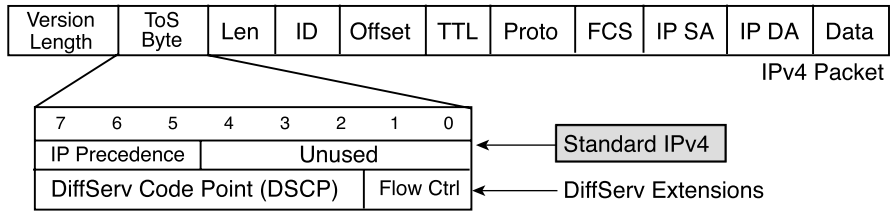


Figure 4-3 also shows Differentiated Services (DiffServ). DiffServ is a new model in which traffic is treated by intermediate systems with relative priorities based on the ToS field. It is defined in RFCs 2474 and 2475. As shown in Figure 4-3, the 6 most significant bits in the ToS byte are called Differentiated Services Code Point (DSCP). The last 2 bits are reserved for flow control and currently are not used. The intermediate devices in the network use the DSCP values set in the IP packet to determine the per-hop behavior (PHB).

When you turn on the auxiliary VLAN feature on an access port on a Cisco switch, two things happen:

1. The switch port is set to an 802.1 Q trunk port.
2. The switch starts sending the VVID information via the Cisco Discovery Protocol (CDP) on the switch port.

If a Cisco IP Phone is connected to a switch port that is configured with auxiliary VLAN, the IP Phone obtains the VVID configured on the switch via CDP. Cisco IP phones store this information in the Operational VLAN ID field.

However, when you are deploying Cisco IP Phones that are connecting to non-Cisco switches that do not have the auxiliary VLAN feature, you have to manually configure the voice VLAN on each Cisco IP Phone. This results in higher administrative and operational overhead and is not scalable for large networks. You can use the Admin VLAN ID field in the Cisco IP Phones to manually assign the VVID.

TIP To view the Operational VLAN ID and Admin VLAN ID settings on Cisco IP Phone model 7960G, click the Settings button and select the Network Configuration option. These two values are listed in items 19 and 20, respectively.

In many Cisco IPT networks, IP phones are connected to the access layer switches. User workstations are connected to the PC port on the back of the phone. However, you cannot use this method if you are in either of the following two situations:

- Wiring closet switches do not support 802.1p class of service.
- Wiring closet switches do not support 802.1Q VLANs on access ports, and IP address space limitations exist.

Instead of connecting the PC to the PC port on the back of the phone, connect the PC and phone on two separate switch ports. This method consumes additional switch ports in the wiring closet for each IP phone installed but provides a physical delineation between voice and data traffic.

PortFast

PortFast is a spanning-tree enhancement that is available on Cisco Catalyst switches. PortFast causes a switch or trunk port to enter the spanning-tree forwarding state immediately, bypassing the listening and learning states.

When you connect a Cisco IP Phone to a switch port, enabling PortFast on that port allows the IP Phone to connect to the network immediately, instead of waiting for the port to transition from the listening and learning states to the forwarding state. This feature decreases the IP Phone initialization time because it can send the packets as soon as the physical link is activated.

NOTE Do not enable PortFast on a switch port if it is connected to another Layer 2 device. Doing so might create network loops. Enable PortFast only on the ports that are connected to IP phones.

Spanning Tree Protocol (STP) is defined in the IEEE 802.1d standard. New standards that are enhancements to IEEE 802.1d are available:

- IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
- IEEE 802.1s Multiple Spanning Tree (MST)

UplinkFast

Like PortFast, UplinkFast is the spanning-tree enhancement on Cisco Catalyst switches. Typically, you connect the access layer switch to two distribution layer switches for redundancy and load balancing. When you have two uplinks, one uplink port on the access layer switch is in a blocked state and the other is in an active or forwarding state. If the access layer switch detects a failure on the active uplink (because of the failure of the distribution layer switch or a bad port), use of the UplinkFast feature on the uplink ports immediately unblocks the blocked port on the access layer switch and transitions it to the forwarding state, without going through the listening and learning states. Because of this, the switchover to the standby link happens quickly.

Deployment Models

Figure 4-4 shows possible deployment models at each layer. The access layer portion of the diagram shows the two models that are available in the access layer.

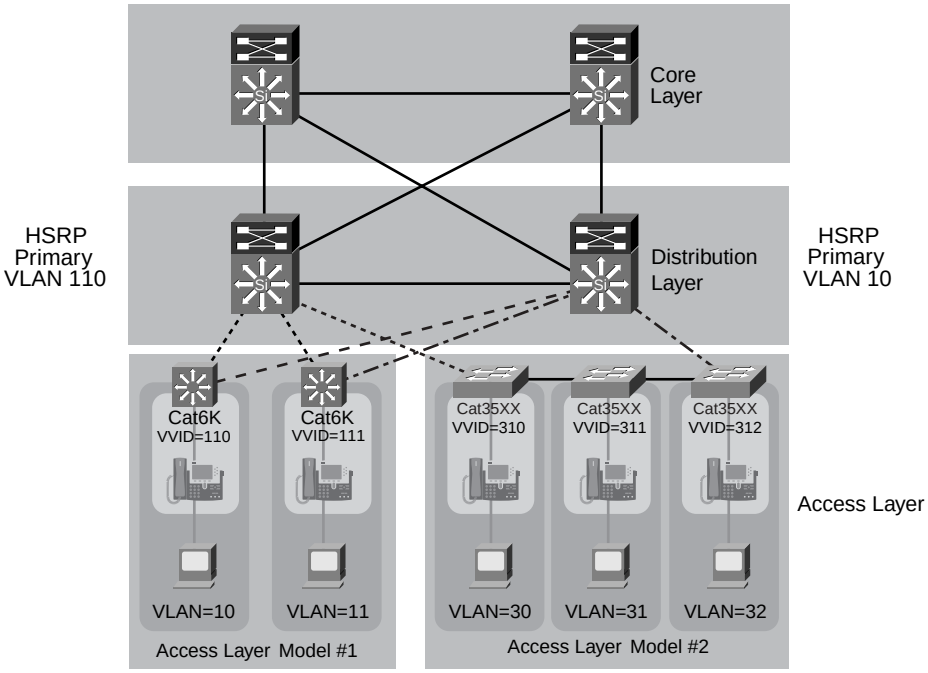
In the first access layer model, each access layer switch has dual uplinks to distribution layer switches. In this case, we recommend that you split the users among the access switches to address the failure situations.

In the second access layer model, the access switches are daisy chained and do not have dual uplinks to distribution layer switches. You have to be careful for the reasons explained in the next two paragraphs about how many of these low-end switches can be connected in a daisy-chained manner.

Some of the low-end switches include a scheme called “giga-stack,” which is a half-duplex environment. A half-duplex environment is bad for voice traffic because it is a collision domain. Because you are compressing voice, you could face voice-quality issues, depending on what kind of compression technique you are using. G.711 is more robust, but if you are using G.729a and lose two consecutive voice packets, the digital signal processor (DSP) will not be able to compensate for this packet loss, and users will likely complain about voice-quality issues.

In a half-duplex environment, you might run into these issues if you have daisy chained too many switches. If you are planning to daisy chain switches, start with a low number. If you have to increase the number of daisy-chained switches, monitor the packet drops and other statistics on the network. Also remember that if any one of the switches in the daisy chain of switches fails, it will cause the subnet to split, and you will run into connectivity issues.

Figure 4-4 *Deployment Models*



The access layer model 1 is well suited for deploying IPT.

Distribution Layer

At the distribution layer of the network, you have the following three options for redundancy. You can choose any one or a combination of options, depending on your capabilities and needs.

- Implement redundant distribution layer switches, each with two supervisory modules. In this case, you have two levels of redundancy: switch redundancy and supervisory module redundancy.
- Implement redundant distribution layer switches, each with one supervisory module. In this case, you have only switch redundancy.
- Implement one distribution layer switch with two supervisory modules. In this case, you have supervisory module redundancy.

We recommend that you design the network with redundant distribution layer switches, each with two supervisory modules, as shown in the distribution layer in Figure 4-4, for the highest level of redundancy and load balancing. The network infrastructure below the distribution layer is Layer 2, and it is unaware of Layer 3 information. At the distribution layer, you should implement the Hot Standby Routing Protocol (HSRP) for redundancy between the two

distribution layer switches: the primary and secondary switch. You also need to use passive interfaces on distribution layer switches that face the Layer 2 access switches, because they do not require Layer 3 information. Use of passive interfaces stops the propagation of Layer 3 information to Layer 2 switches. With HSRP, you can choose one of the following methods for redundancy:

- Make one switch the primary switch for the whole network and let the network fail over to the secondary switch in case of primary switch failure.
- Make both switches the primary switch for some of the network and the secondary switch for the rest of the network. By using this technique, you can load balance your traffic. One approach is to make one switch primary for the voice VLANs and the second switch primary for the data VLANs.

Because you are now analyzing Layer 3 infrastructure, you should make sure that you follow the Layer 3 guidelines listed here. These guidelines will help you to increase the overall convergence of the network.

- Use Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), or Intermediate System-to-Intermediate System (ISIS) Protocol for improved network convergence.
- Follow consistent configuration standards and naming conventions for all routers in the network for better convergence and ease of troubleshooting.
- Implement IP summarization toward the core to reduce routing protocol overhead and to ensure IP scalability.
- Implement stub or default routing in WAN hub-and-spoke environments to reduce routing protocol traffic overhead on WAN links.
- Review routing protocol impact and scalability based on device types, number of routes, and IP routing protocol neighbors.
- Review the timers of your IP routing protocols and tune them as needed for faster convergence only after you have performed thorough testing.

Core Layer

The core layer of the network should act as a transitory layer. Access switches should not be collapsed on the core layer. With parallel links in the core layer, you can provide redundancy and do load balancing and fast convergence. The core layer is based on Layer 3 protocols. All the guidelines mentioned in the previous “Distribution Layer” section apply to the core layer, too. The top layer in Figure 4-4 depicts the core layer infrastructure.

Cabling Infrastructure

Different categories of cabling are available when building Ethernet-based networks. Category 5 (Cat 5) cabling is the most commonly used in many networks because it offers higher

performance than other categories, such as Cat 4 and Cat 3. Cat 5 cabling supports data rates up to 100 Mbps (Fast Ethernet), whereas Cat 3 cabling supports data rates up to 10 Mbps (Ethernet). The Fast Ethernet specifications include mechanisms for auto-negotiation of speed and duplex.

By default, the switch port and the PC port on the Cisco IP phone are set to auto-negotiate the speed and duplex. Hence, if you are deploying IPT in a network that is built on Cat 3 cabling that supports a speed of only 10 Mbps, you have to manually set the connection between the IP phone and the switch port to 10 Mbps/full duplex to avoid the possibility of this connection negotiating as 100 Mbps/full duplex. This requires manually setting the speed/duplex on every IP phone switch port to 10 Mbps/full duplex, which could become a tedious task and cause administrative overhead in larger deployments.

Also, because the uplink connection from the IP phone to the switch port is 10 Mbps, you need to ensure that users who connect the PC to the back of the IP phone's PC port have their network interface card (NIC) settings set to 10 Mbps/full duplex, and you need to manually set the speed/duplex setting of the PC port on the switch to 10 Mbps/full duplex.

NOTE To understand how auto-negotiation works on Ethernet networks, refer to http://www.cisco.com/warp/customer/473/3.html.

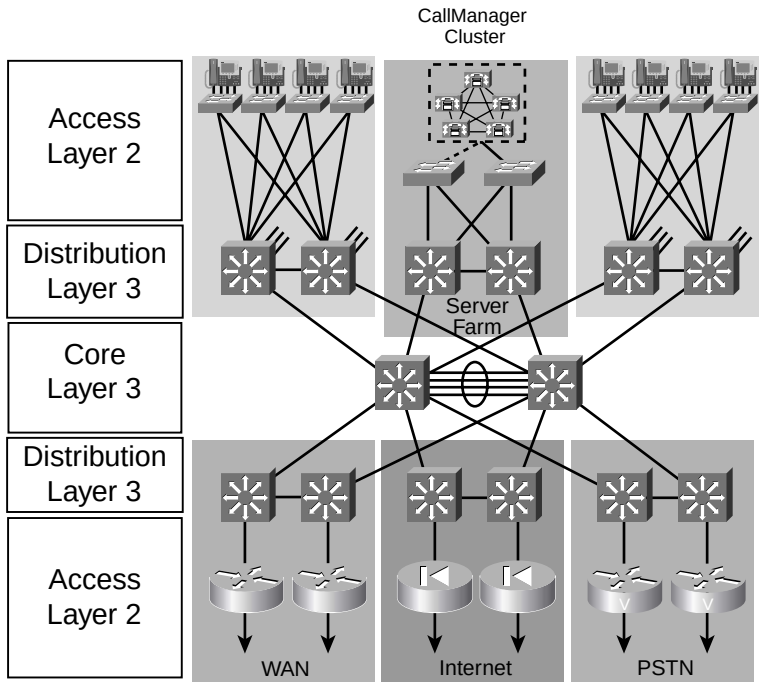
Common Guidelines

When you are reviewing the network infrastructure, make sure to provide redundancy at every layer and use standardized software versions throughout the network, to avoid situations in which hardware or software failure impacts the network.

Also, make sure to eliminate single points of failure in all the layers. At the access layer, you have a single point of failure if you do not have two outlets to the desk from two different catalyst switches. This situation applies in all data networks and even in legacy voice networks. If the connection between the IP phone or PC and the access layer switch fails, the device loses the connection. This is also true in legacy phone networks. If the phone line coming to your home fails, you lose the phone connection. The last hop is always a single point of failure, which is unavoidable. We have not seen common scenarios in which two NICs are placed in a PC or two PCs are placed in every office for redundancy, with redundant links from the access layer switch to these devices.

At the distribution layer, you need to make sure that you keep modularity in your network. To do so, plug in these different modules to the distribution layer and keep them separate, as shown in Figure 4-5, where you have WAN, Internet, PSTN, server farm, and internal PC/IP phone users connecting to their own access layer switches. The access layer switches have dual connections to redundant distribution layer switches. The distribution layer switches of each module have dual connections to redundant Layer 3 switches. This strategy provides a robust, highly available, and easy-to-troubleshoot network architecture.

Figure 4-5 *Modular Campus Architecture*



QoS in Campus Network Infrastructure

Implementing QoS is about giving preferential treatment to certain applications over others during periods of congestion. Which preferential treatments are enabled in a network varies depending on the technology (such as voice and video) and business needs.

QoS is not an effective solution when chronic network congestion occurs. If the network is frequently congested, you need more bandwidth. QoS should be implemented to ensure that critical data is forwarded during occasional brief periods of congestion, such as when there is a link failure and all traffic must traverse the remaining path.

You configure QoS in your network for the times of need. When you are implementing QoS in a network, you need to give voice traffic highest priority, followed by video applications and then data applications. You can divide data applications into multiple classes if necessary, because you might have some data applications that are more critical for your business (such as Systems Network Architecture [SNA] traffic, typically used by IBM mainframe computers) than simple FTP or web applications.

In our experience, voice and data traffic in a network that has not been configured for QoS experiences voice-quality issues because of the differences in the characteristics of traffic and voice traffic.

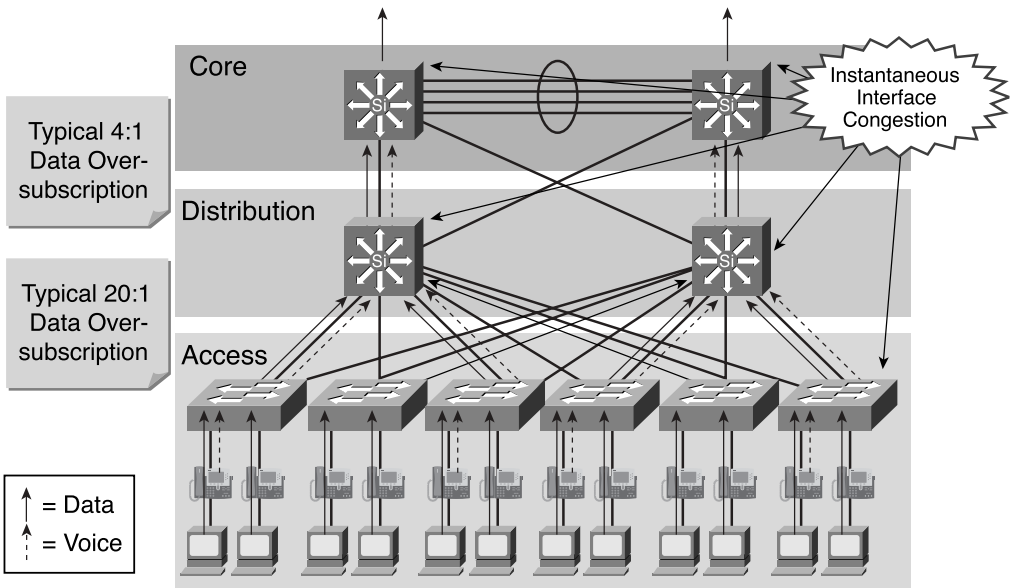
Data and Voice Traffic Characteristics

Most data traffic is bursty, delay and drop insensitive in nature (SNA is an exception, which is not drop insensitive), and can always be retransmitted. Voice data, in contrast, is consistent, smooth, and delay and drop sensitive. As mentioned earlier, in the section "Deployment Models," if you are using a G.729a codec and the network drops even two consecutive packets, those drops will result in poor voice quality. There are two types of delay: one-way delay and jitter. The jitter is variation in the delay, which also results in poor voice quality. Voice applications do not retransmit dropped packets, because the retransmission would cause the dropped packets to arrive to the destination even later, resulting in poor voice quality. When you put voice traffic on the same network that is carrying data traffic, you need to make sure that you remember these characteristics of voice and data.

Oversubscription in Campus Networks

Figure 4-6 shows the access, distribution, and core layers of the network architecture that XYZ built initially for data applications.

Figure 4-6 *Oversubscription in Campus Networks*



Usually, oversubscription is done at every layer while building the network for data applications. This oversubscription usually works well for data applications because of their nature, as described in the earlier "Data and Voice Traffic Characteristics" section. When adding voice applications to your existing data network, however, you might do either of two things to avoid congestion: redesign your network so that it is less oversubscribed, or add more bandwidth to the network. These two actions by themselves do not provide a voice application–friendly infrastructure. You will encounter interface congestion at the egress interfaces. When you add more bandwidth in the network, the data application characteristics do not change. The data applications have the same bursty nature and try to consume the added bandwidth.

The problem you want to solve is how to eliminate the instantaneous congestion points. When you look at the interface statistics, you might see only 20 percent usage and thus think that no congestion. But you are not seeing the statistics when the congestion occurs, due to some data application that is bursting traffic and consuming the bandwidth of that egress interface, causing the voice packets to drop. This instantaneous congestion in the network introduces bad voice quality. Users might call you at the end of the week and report that this week, they have experienced voice-quality issue twice. Troubleshooting this issue is going to be tough, because your users did not report the problem when they were experiencing the voice-quality issue.

The solution to this problem is to configure QoS in your network. If you have QoS configured in your network, at times of congestion, QoS ensures that voice traffic gets higher priority. QoS is an end-to-end mechanism, which should be configured throughout the network, starting from IP phones, access layer switches, distributions layer switches, and core layer routers.

If you are routing voice traffic over the WAN, you should configure QoS on the WAN routers for the WAN links, too. You should provision your WAN links to carry the additional voice traffic. You need to know how many calls you are sending over your network and how much bandwidth these calls require.

Before enabling end-to-end QoS in your network, you need to define the current and future important and critical applications for your business. Based on the business importance of these applications, you need to find out what the technical requirements are to provide preference to these applications. When planning and reviewing these applications, always keep future applications in mind and leave room in your QoS policy for them. For example, if you are currently planning for data and voice applications, leave room for future video applications in your QoS policy.

Network Trust Boundaries

The packets that enter your network or hardware can be marked into different classes; you can define the trust boundaries in your network. You can define some devices as trusted devices and some as untrusted devices. The packets that come from trusted devices are considered trusted

because the trusted devices classify the packets correctly. The packets that come from untrusted devices are considered untrusted because they might not classify the packets correctly. After you have marked the packets and defined the trust boundaries, you can force the scheduling of the packets into different queues. These queues invoke at the time of congestion.

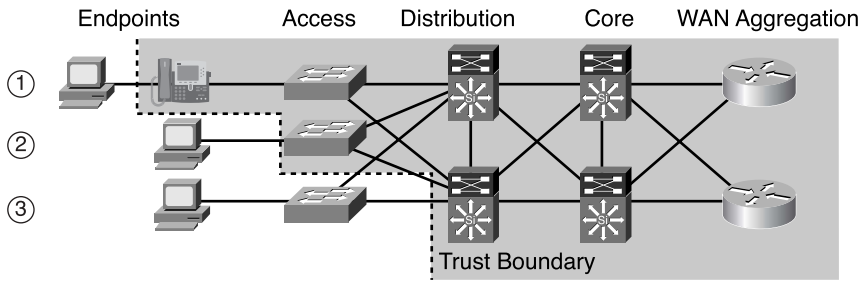
Defining trust boundaries is important in your network. As shown in Figure 4-7, in the first option, your trust boundary starts from an IP phone. Setting the trust boundary at the IP phone means that you can accept all the IP phone markings into the network without modifications.

In the second option, your trust boundary starts from an access layer switch, which means that the access layer switch is going to be marking the packets.

In the third option, your trust boundary starts from a distribution layer switch, which means that you cannot do anything with your high-priority packets until they reach the distribution layer switch, resulting in possible voice-quality issues.

You should always try to do classification close to the edge of the network, for scalability. This recommendation means that you should choose option one or two while planning for your IPT network. Choosing option one enables the IP phone to queue the packets that it is originating according to their Layer 2 CoS and Layer 3 ToS values.

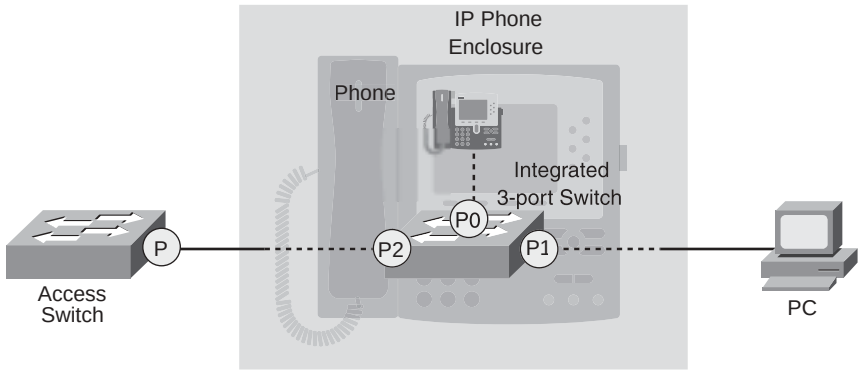
Figure 4-7 *Network Trust Boundaries*



IP Phone QoS

As mentioned earlier, QoS is an end-to-end mechanism; with IPT networks, QoS starts from the IP phone. As shown in Figure 4-8, a Cisco IP Phone has a built-in three-port 10/100 switch (not all Cisco IP Phones have the PC port on the back of the phone), where port 2 connects to the access layer switch and passes all the traffic to/from ports 0 and 1. Port 0 connects to the IP Phone's application-specific integrated circuit (ASIC) and carries traffic generated from the IP Phone. Port 1 (also called the access port) connects to a PC or any other device and carries traffic generated from there.

Figure 4-8 *Three-Port 10/100 Switch in IP Phone*



By default, an IP phone marks all the voice-bearer traffic that it generates with a Layer 3 IP precedence value of 5 (DSCP value of 46) and a Layer 2 CoS (802.1p) value of 5. The voice-control traffic is marked with a Layer 3 IP precedence value of 3 (DSCP value of 26) and a Layer 2 CoS (801.p) value of 3.

In Figure 4-8, the untagged data coming from the PC port (with no Layer 2 CoS value) passes through the IP phone unchanged, regardless of the trust boundary. The tagged data (802.1Q/p) from the PC or any other device that is attached to the access port (port P1 in Figure 4-8) of the IP phone can be trusted or untrusted. In trusted mode, the IP phone passes all the data unchanged. In untrusted mode, the IP phone re-marks the Layer 2 CoS value to the new value (if configured on the access layer switch) or changes it to 0, if nothing is configured. The default is untrusted mode, which is the recommend method.

Most of the Cisco switches have support for priority queuing on the egress interfaces. You should perform the configuration on the access, distribution, and core layer switches in such a way that the delay-sensitive packets, such as voice packets and voice-control packets, are placed in the priority queue. If no priority queue exists on the egress interface of a switch that you have in your network, place the delay-sensitive packets in the queue that has the lower drop threshold. Chapter 5, "Design Phase: Network Infrastructure Design," provides some configuration examples of this procedure. If the access layer switch is Layer 3 aware, it can pass the packets marked by the IP phones as unchanged toward the upper layers as long as the access layer switch ports are configured to trust the packets coming from the IP phones.

If the access layer switch is Layer 2 aware, the packets are sent to the next layers unchanged.

When voice packets reach the distribution layer switch (entering the Layer 3 boundary domain), they are mapped to corresponding Layer 3 ToS bits (IP Precedence and DCSP) and shipped to the core layer. The core layer forwards the packets based on the ToS bit values. When packets cross the Layer 3 boundary and enter the Layer 2 domain, you must remap Layer 3 ToS values to Layer 2 CoS values. Layer 2 CoS and Layer 3 ToS values are backward compatible, as shown

in Figure 4-9. Figure 4-9 also depicts the use of Layer 2 CoS and Layer 3 QoS values in different applications.

Figure 4-9 *Layer 2 CoS and Layer 3 QoS Chart*

L2	L3 Classification			Application
CoS	IP Prec.	PHB	DSCP	
7	7	-	56-63	Reserved
6	6	-	48-55	Reserved
5	5	EF	46	Voice Bearer
4	4	AF41	34	Video Conferencing
3	3	AF31	26	Call Signaling
2	2	AF2y	18,20,22	High-Priority Data
1	1	AF1y	10,14,16	Medium-Priority Data
0	0	BE	0	Best-Effort Data

NOTE The new IETF standard recommends that you mark signaling packets with a DSCP value of 24 (PHB value CS3) instead of the currently used value of DSCP 26 (PHB AF31). Only a few endpoints, such as Cisco IP Communicator and Cisco IP SoftPhone products, implemented this new change. Hence, until this new marking takes effect in all the products, reserve both values for signaling in the network.

Inline Power for IP Phones

The first-generation Cisco IP Phones received power through external power supplies. Later, Cisco invented the concept of supplying inline power to Cisco IP Phones by using the same Ethernet pair used to send data (Power over Ethernet [PoE]). The inline power has two ends. One end is the switch, which sends the 48V DC power on the same Ethernet pair used to send data. The other end is the Cisco IP phone, which can accept power on the same pair used for data or Cisco IP Phones can use the unused pair for accepting the inline power. The reason for supporting these two options on the Cisco IP phones is that some of the switches do not have the capability to provide inline power. In this scenario, you can use a power patch panel—the power comes from the switch to the patch panel, and the patch panel uses the unused Ethernet pair to send the inline power to the IP phone.

Cisco IP Phones are capable of accepting inline power and can inform the switch how much power they need. This allows the switch to allocate the correct amount of power to the Cisco IP Phone without over- or underallocating power. Initially, the switch does not know how much

power a Cisco IP Phone is going to need, so it assumes it needs the user-configured default allocation. After the IP phone is booted, it sends a CDP message to the switch with a type, length, value (TLV) object that contains information about how much power it needs. At this point, the switch adjusts its original allocation and returns any remaining power to the system for use on other ports.

NOTE IEEE has recently approved a new inline power standard, IEEE 802.3af. Cisco is complying with this new IEEE standard.

Since the ratification of the Power over Ethernet (PoE) standard IEEE 802.3af, Cisco has shipped the new Cisco IP Phone 7970G, which is compatible with this new standard. The new generation of Cisco IP Phones that will be released in the future will support both Cisco PoE and IEEE 802.3af PoE mechanisms. The Cisco IP Phones shipped prior to the ratification of the standard support only Cisco PoE. Hence, if you are deploying Cisco IP Phones in a network without Cisco switches, your options are as follows:

- Use the Cisco IP Phones that support IEEE 802.3af, provided your switch supports IEEE 802.3af.
- Use the external power patch panel to supply the power to Cisco IP Phones.

High-end catalyst switches such as Cisco 6000 series switches use inline-power daughter cards that sit on the 10/100 modules to provide the power to Cisco IP phones. If your network currently uses Cisco PoE, you can do a field upgrade to replace the Cisco PoE daughter cards with IEEE 802.3af inline-power daughter cards. The new IEEE 802.3af–compliant inline-power daughter cards support both Cisco PoE and IEEE 802.3af PoE. Thus, you can still have the old Cisco IP Phones that use Cisco PoE and also have new Cisco IP Phones that use IEEE 802.3af PoE.

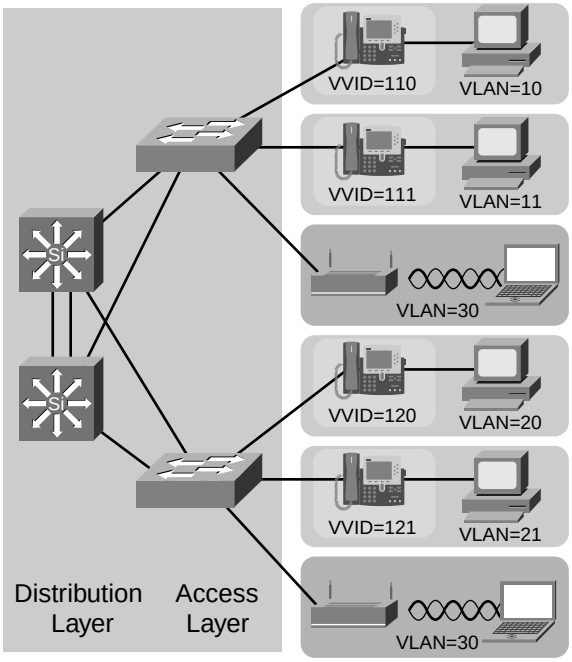
Refer to the "Power and Environmental Infrastructure" section later in this chapter for more information on how to plan for a scalable, highly available, redundant power infrastructure.

Wireless IP Phone Infrastructure

This section discusses briefly the integration of wireless IP phones in your infrastructure planning, as shown in Figure 4-10. As discussed earlier, in the "Access Layer" section, the purpose of keeping the VLAN in the closet is to limit the spanning tree in the closet. There are some exceptions to this rule; one of them applies when using wireless IP phones. If you want to use wireless IP phones and roaming, you have to do this on Layer 2. You will create a single wireless VLAN for wireless IP phones, which will span the closets. Because you can support spanning tree per VLAN, the wireless VLAN is going to be the only VLAN that is affected with

longer convergence times, if there is a problem. Make sure that you allow the wireless IP phones to use only this wireless VLAN (WLAN).

Figure 4-10 *WLAN Infrastructure*

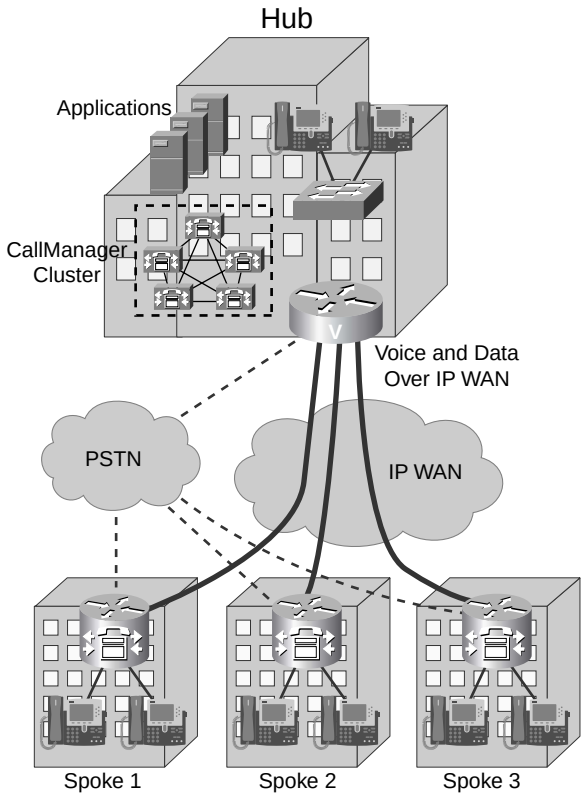


WAN Infrastructure

To support toll-quality voice traffic over your existing WAN, you have to re-engineer your WAN to support QoS and call admission control (CAC). Traditional telephony networks are connection oriented. If all 23 DS0s are in use, a PBX with a T1-PRI connection to the PSTN rejects the 24th call, because no physical channel is available to place the 24th call. In contrast, IP networks are connectionless in nature. Therefore, if you have a 128-kbps Frame Relay link supporting two good-quality 64-kbps (without considering protocol overhead) G.711 VoIP calls, and a request to place a third call is allowed, this would result in degradation of the voice quality of the existing two calls. To avoid oversubscribing the WAN links, you have to use CAC when transporting voice traffic on the WAN, as discussed in Chapter 1 in the "Next-Generation Multiservice Networks" section.

Based on presently available WAN technologies, you have to deploy a physical or virtual hub-and-spoke topology to make sure that you do not oversubscribe on the WAN links, as shown in Figure 4-11.

Figure 4-11 *Hub-and-Spoke WAN Topology*



The full or partially meshed topology cannot give the control you need to deploy CAC and QoS. The following are some of the available WAN technologies that can provide QoS:

- Leased lines
- Frame Relay (FR)
- ATM
- ATM/FR service interworking
- Multiprotocol Label Switching (MPLS) VPN
- Voice- and video-enabled IP Security (IPSec) VPN (V3PN)

By using QoS on any of the preceding WAN technologies, you can get guaranteed good-quality voice. Other WAN technologies, such as DSL and cable, can provide best-effort quality voice rather than guaranteed good-quality voice. The reason for this is that the cable/DSL service providers use the public Internet to transport the data and voice packets, which does not guarantee the delay and priority treatments that are required for voice traffic.

In the planning phase of the IPT deployment, you need to first obtain the information about the existing WAN architecture and WAN circuit characteristics. The "Wide Area Network" section in the Network Infrastructure Analysis Questionnaire in Appendix B assists you in gathering the information.

XYZ is currently using a combination of FR and ATM WAN technologies on its WAN. Table 4-1 summarizes the XYZ WAN circuit characteristics.

Table 4-1 *XYZ WAN Circuit Characteristics*

Link Name	WAN Router Model	Speed and WAN Type (ATM, FR, or Leased Line)	Current Utilization	CIR (if ATM or FR)
Seattle – San Jose	Seattle Router 3745	1 Mbps, FR	60%	1 Mbps
Dallas – San Jose	2651 XM	512 kbps, FR	50%	512 kbps
San Jose (Headend)	7200	1.5 Mbps, ATM	50%	1 Mbps
Melbourne – Sydney	Melbourne Router 3745	512 kbps, FR	40%	256 kbps
Brisbane – Sydney	2651 XM	256 kbps, FR	40%	256 kbps
Sydney (Headend)	7200	1.5 Mbps, ATM	50%	1.5 Mbps
San Jose-Sydney	7200	2 Mbps, leased line	50%	2 Mbps

CIR = committed information rate

QoS in WAN Infrastructure

Packet loss, one-way delay, and jitter (variation in delay) were discussed earlier in the context of the campus QoS infrastructure. These parameters become even more important in a WAN environment. Although you often hear that bandwidth is getting cheaper, most enterprise networks still have less WAN bandwidth than is actually needed. It is important to understand the various techniques that are available to reduce packet loss, delay, and jitter in the WAN circuits:

- Minimizing delay
- Using traffic shaping
- Provisioning WAN bandwidth

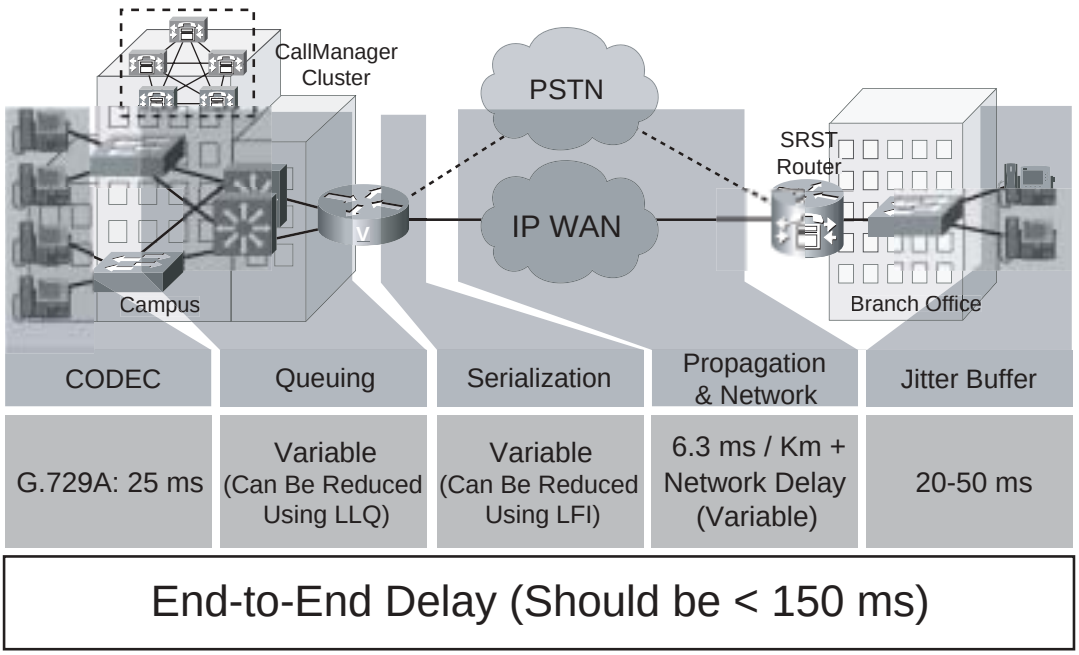
- Using voice compression

Understanding these techniques helps you to properly provision the WAN circuits in the real world.

Minimizing Delay

Figure 4-12 shows the components that introduce delay and the mechanisms that are available in routers that can minimize these delays to achieve good voice quality. The objective behind using the mechanisms is to achieve the ITU G.114 recommendation of 0- to 150-ms one-way delay for the voice packet.

Figure 4-12 *End-to-End Delay Components*



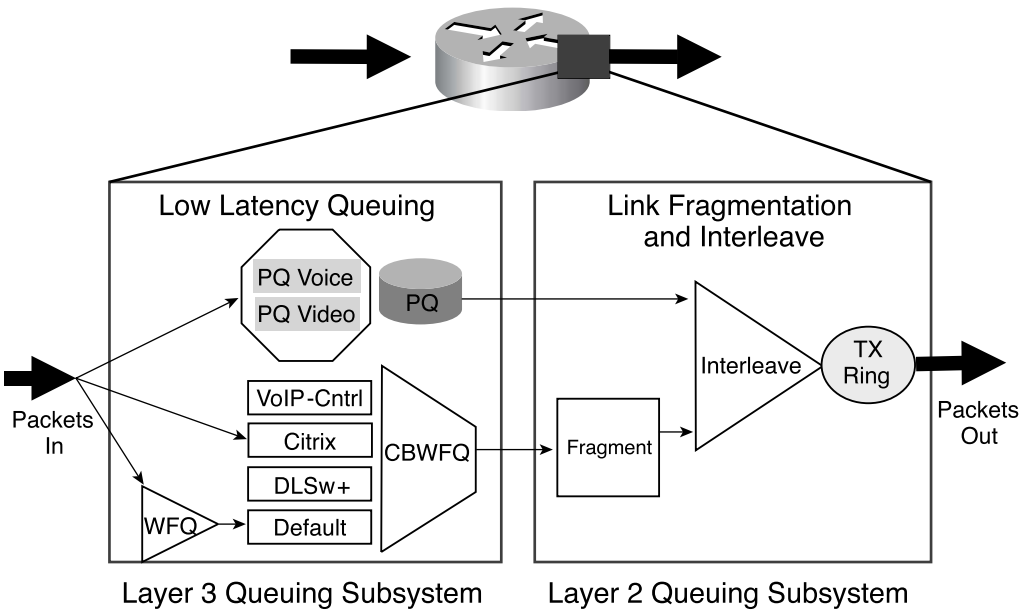
CODEC Delay

The first delay component is the delay that the voice codec introduces. The codec takes the voice sample, processes it, and creates a voice packet. The time taken for this process depends on the type of codec that is selected. The G.729a codec, shown in Figure 4-12, takes 25 ms to take two voice samples (10 ms for each voice sample plus a 5-ms look-ahead time) and put them into a packet before it can send this packet. Other codec types take about the same time except G.711, which takes less time.

Queuing Delay

As shown in Figure 4-12, the second component that introduces delay is queuing delay. Congestion in the network invokes the queuing in the routers. At times of congestion, packets start to build up in the queues within the routers. The packets in the queues eventually transmit, when congestion goes away, causing delay. The queuing mechanism you should use on the WAN links to reduce this delay is called Low Latency Queuing (LLQ), also known as Priority Queuing/Class-Based Weighted Fair Queuing (PQ/CBWFQ), as shown in Figure 4-13.

Figure 4-13 *PQ/CBWFQ and LFI Operation*



In Figure 4-13, the priority queue holds all the voice and delay-sensitive traffic, such as the following:

- **Voice traffic**—CoS value of 5, IP Precedence value of 5, DSCP value of 46, PHB value of EF
- **H.323 video-conferencing traffic**—CoS value of 4, IP Precedence value of 4, DSCP value of 34, PHB value of AF41

The CBWFQ holds voice-signaling traffic and data traffic:

- **Voice-signaling traffic**—CoS value of 3, IP Precedence value of 3, DSCP value of 26, PHB value of AF31
- **Data traffic**—Different priorities of data traffic

Serialization Delay

As shown in Figure 4-12, the third component that introduces delay is serialization delay. Table 4-2 shows the serialization delay matrix.

Table 4-2 *Serialization Delay Matrix*

Link Speed	Frame Size					
	64 Bytes	**128 Bytes**	**256 Bytes**	**512 Bytes**	**1024 Bytes**	**1500 Bytes**
56 kbps	9 ms	18 ms	36 ms	72 ms	144 ms	214 ms
64 kbps	8 ms	16 ms	32 ms	64 ms	128 ms	187 ms
128 kbps	4 ms	8 ms	16 ms	32 ms	64 ms	93 ms
256 kbps	2 ms	4 ms	8 ms	16 ms	32 ms	46 ms
512 kbps	1 ms	2 ms	4 ms	8 ms	16 ms	23 ms
768 kbps	640 µs	1.2 ms	2.6 ms	5 ms	10 ms	15 ms

You derive the delay values in the table by calculating the time it would take to send 1 byte on the circuit for the appropriate speed. The following example illustrates the calculation of serialization delay for a 56-kbps circuit.

> 56 kbps/8 bits = 56000/8 bits = 7000 bytes per second
> 1 second/7000 bytes per second = 143 microseconds to transmit 1 byte

You can then extrapolate the serialization delay for various byte sizes by multiplying the time required for 1 byte at a given circuit speed times the frame size to be sent. The following example illustrates the serialization delay for a 1500-byte packet on a 56-kbps circuit:

> 143 microseconds for 1 byte at 56 kbps × 1500 bytes = 214 ms for a 1500-byte frame at 56 kbps

From the previous calculation, you can see that a 1500-byte packet takes 214 ms to reach from one end to the other end on a 56-kbps link. Therefore, if a 1500-byte packet is in the transmit queue on a router in front of a small voice packet that has a requirement of 0- to 150-ms one-way delay, the voice packet has to wait at least 214 ms before it can be placed on the wire. As the link speed increases, the time required to transmit the 1500-byte packet from one end to the other end decreases. For example, in Figure 4-14, the same 1500-byte packet takes only 15 ms to make it to the other end on a 768-kbps circuit.

When using a 768-kbps or lower-speed link, you always encounter this problem in which you have different large-size packets causing delay to small, constant-size voice packets. The varying sizes of the large packets cause voice packets to arrive at the destination at irregular intervals. This variation in delay is called jitter. You can reduce the delay introduced by the large packets and the jitter condition by using Link Fragmentation and Interleaving (LFI) mechanisms such as Multilink PPP (MLPPP) on point-to-point links, ATM, Frame Relay and ATM Service Inter-Working (SIW) environments, and FRF.12 in Frame Relay environments. When using a

768-kbps or lower-speed link, use LFI mechanisms to fragment the large data packets and interleave small voice packets between the fragmented data packets (refer to Figure 4-13).

Propagation Delay

As shown in Figure 4-12, the fourth component that is a source of delay is propagation delay. Propagation delay is the amount of time it takes to transmit the bits of packets on the physical wire. The factors that influence propagation delay are the physical circuit distance between the source router and the destination router and the type of circuit media that is used, such as fiber-optic link or satellite link. Propagation delay is generally fixed but grows as the length of travel from source to destination. Consider the propagation delay especially if the connecting media is a satellite link that introduces large amounts of delay. A voice packet traveling across this media might not meet the ITU-T recommendation of less than 150 ms one-way delay if all the other delay factors are combined.

Jitter Buffer

As shown in Figure 4-12, the fifth source of delay is the jitter buffer. Depending on the type of codec in use, the jitter buffer size could change. The jitter buffer holds about two and one-half voice packets (each voice packet has a couple of 10-ms voice samples) and is dynamic in nature. The rate at which the voice packets arrive at the jitter buffer is uneven. The jitter buffer looks at the time stamps of the arriving voice packets to create a large enough jitter buffer. Then it stores and plays the voice packets to the user in a constant and even manner, so that the user is not interrupted. If you have excessive jitter in your network and the jitter buffer cannot hold that many packets, these packets are dropped. It is important to control the jitter in your network by using a combination of LLQ/PQ-CBWFQ, LFI, and traffic shaping.

Using Traffic Shaping

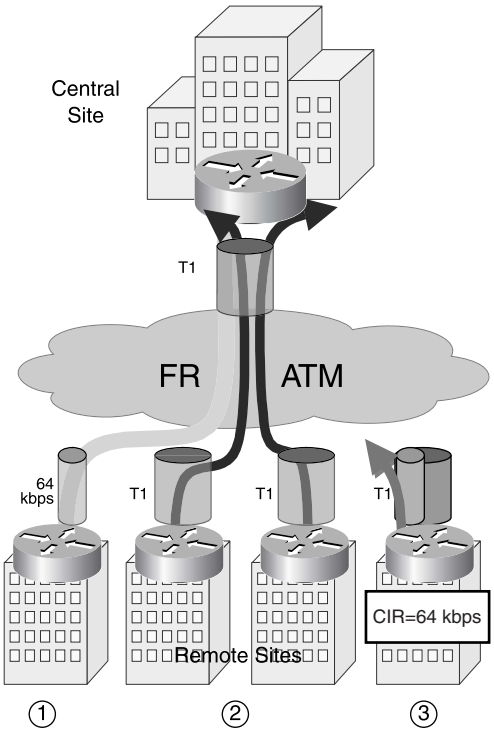
The job of a router is to transmit packets as fast as possible and put them on the wire. If you have a 64-kbps link and a Committed Information Rate (CIR) of 32 kbps on your FR or ATM link, the router does not consider the 32-kbps CIR and tries to send the packets at the rate of 64 kbps. More or less, every router tries to transmit more than its respective CIR assigned by the provider on the FR and ATM networks. This causes congestion within the network and eventually results in packet drops. When you want to transmit voice packets over the FR and ATM networks, you have to change the traffic pattern, because you cannot afford the voice packet loss. You have to make sure that the router considers the CIR value.

The traffic-shaping functionality on the router delays the excess traffic in a buffer and shapes the flow to ensure that packets are not transmitted above the CIR values.

You should also make sure that you take care of line-speed mismatch between the central and remote sites. As shown in Figure 4-14, if you have a central site with a T1 link speed and a

remote site with a 64-kbps link speed, you should not try to send data at T1 speeds to the remote site, because the remote site is not capable of receiving data at T1 speeds.

Figure 4-14 *Mismatch of Speeds Between Central and Remote Sites*



Even if you try to send data at T1 speeds, it will sit in the egress queue of the central site router, causing extra delay for your voice packets. When supporting voice, you cannot use oversubscription between your remote and central sites. Traffic shaping helps you to engineer your network in a way that you do not run into issues related to the following:

- Line-speed mismatch
- Remote site to central site oversubscription
- Bursting above CIR

Provisioning WAN Bandwidth

After you have deployed QoS in your campus and WAN infrastructure, one of the most important steps is to provision the WAN links in your network. You should make sure that the sum of voice, video, voice-control, video-control, and data traffic does not exceed 75 percent of your

link bandwidth. You want to leave 25 percent of the link capacities for the critical traffic such as routing protocol traffic, which keeps your network up and running.

Table 4-3 shows the voice bandwidth consumption based on the choice of codec and the sampling rate. Note that the bandwidth values shown in the rightmost column include only Layer 3 overhead.

Table 4-3 *Voice Bandwidth Consumption (Without Layer 2 Overhead)*

Codec	Sampling Rate	Voice Payload in Bytes	Packets per Second (pps)	Bandwidth per Conversation
G.711	20 ms	160	50.0	80.0 kbps
G.711	30 ms	240	33.3	74.7 kbps
G.729a	20 ms	20	50.0	24.0 kbps
G.729a	30 ms	30	33.3	18.7 kbps

You also need to consider Layer 2 overhead when provisioning the WAN bandwidth. Table 4-4 provides the voice bandwidth consumption with Layer 2 overhead taken into consideration.

Table 4-4 *Voice Bandwidth Consumption (with Layer 2 Overhead)*

Codec Sampling Rate	Ethernet 14 Bytes of Header	PPP 6 Bytes of Header	MLPPP 10 Bytes of Header	Frame Relay 4 Bytes of Header	ATM 53-Byte Cells with a 48-Byte Payload
G.711 at 50.0 pps Sampling rate 20 ms	85.6 kbps	82.4 kbps	84 kbps	81.6 kbps	106 kbps
G.711 at 33.3 pps Sampling rate 30 ms	78.4 kbps	76.3 kbps	77.3 kbps	75.7 kbps	84.8 kbps
G.729a at 50.0 pps Sampling rate 20 ms	29.6 kbps	26.4 kbps	28.0 kbps	25.6 kbps	42.4 kbps
G.729a at 33.3 pps Sampling rate 30 ms	22.4 kbps	20.3 kbps	21.3 kbps	19.7 kbps	28.3 kbps

As you can see in Table 4-3, increasing the sampling rate reduces the bandwidth required per conversation, because more voice samples are sent in a single IP packet, thus reducing the protocol overhead. This is especially attractive in ATM networks. Table 4-4 shows that increasing the sampling rate to 30 ms for the G.729a codec reduces the bandwidth utilization by 37 percent compared to using the sampling rate of 20 ms when using ATM. You can change the sampling rate for the codecs in CallManager by modifying the following service parameters:

- PreferredG711MillisecondPacketSize (default 20 ms)
- PreferredG723MillisecondPacketSize (default 30 ms)
- PreferredG729MillisecondPacketSize (default 20 ms)

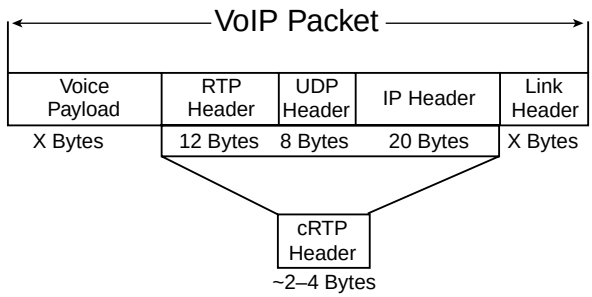
These parameters are cluster-wide parameters and affect all the IPT devices that are attached to the cluster.

However, before you decide to change the sampling rate, you need to be aware of two factors: This change adds more latency due to packetization and serialization delay, and if you lose one packet, it can affect voice quality because you are losing more information than that contained in a smaller sample. So, when you are doing bandwidth provisioning, you have to keep in mind the voice- and video-control traffic. The voice- and video-control packets are small, but you need to reserve the bandwidth for these call-control packets. Refer to the CallManager Solution Reference Network Design Guide (SRND), *IP Telephony Solution Reference Network Design for Cisco CallManager 4.0,* available on Cisco.com at http://www.cisco.com/go/srnd, to determine the amount of bandwidth that you need to reserve.

Using Voice Compression

Voice packets are carried using RTP, UDP, and IP as a protocol stack. The IPv4 header is 20 bytes, the UDP header is 8 bytes, and the RTP header is 12 bytes, totaling 40 bytes of header information, as shown in Figure 4-15.

Figure 4-15 *RTP Header Compression*



After this 40 bytes of header information, two 10-byte frames (the Cisco G.729a codec implementation) of real voice payload are carried, totaling another 20 bytes of voice payload. Simple math shows that the header is twice the size of the real payload. To address this particular issue, an RTP header compression technique called compressed RTP (cRTP) is used on low-speed point-to-point links. When enabled on a router, cRTP compresses the 40-byte header to 2 or 4 bytes. This dramatically reduces the bandwidth required per call, as shown in Table 4-5. Referring to Table 4-4, a G.729a call at 50 pps on a PPP link requires 26.4 kbps of bandwidth. Referring to Table 4-5, the same call with cRTP requires only 12 kbps, a 45 percent savings in the bandwidth required. This means that you can send more calls within the same WAN link without increasing the bandwidth on the link. However, keep in mind that enabling cRTP on a router requires extra processing power on both ends of the link. One link compresses and the other decompresses, resulting in extra work on both routers.

Hence, you should restrict the use of cRTP on low-speed point-to-point links. On high-speed links, it is better not to use cRTP, because you have enough bandwidth and you can avoid putting extra pressure on both routers of the point-to-point link. However, if your voice traffic on the high-speed links amounts to more than 30 percent of the link capacity, you can enable cRTP to save costs.

Table 4-5 *Bandwidth Consumption with cRTP (Including Layer 2 Headers)*

Codec	PPP 6 Bytes of Header	Frame Relay 4 Bytes of Header	ATM 53-Byte Cells with a 48-Byte Payload
G.711 at 50.0 pps	68.0 kbps	67.0 kbps	85 kbps
G.711 at 33.3 pps	66.0 kbps	65.5 kbps	84.0 kbps
G.729a at 50.0 pps	12.0 kbps	11.2 kbps	21.2 kbps
G.729a at 33.3 pps	10.1 kbps	9.6 kbps	14.1 kbps

NOTE An online voice codec bandwidth calculator tool is available on Cisco.com, at http://tools.cisco.com/Support/VBC/do/CodecCalc2.do. This tool calculates the bandwidth requirements per voice call.

To accurately provision the WAN bandwidth, you need to obtain the following information:

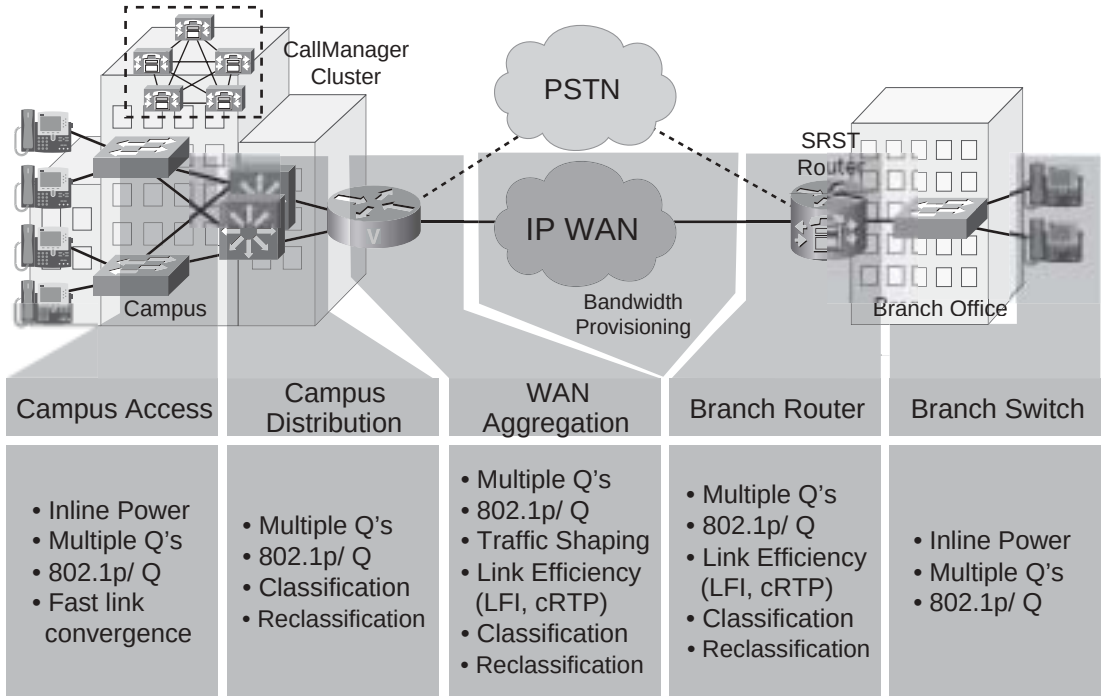
- What are the various traffic flows across the WAN link?
- Are there requirements to give priority treatment for a specific traffic flow?
- What is the WAN technology deployed?
- What is the current utilization of the WAN link?
- What is the choice of the codec and the sampling rate?

- How many voice calls are required across the WAN?
- Is RTP compression required to save the bandwidth?

After you have the previous information, with the help of Tables 4-4 and 4-5, you can determine the amount of bandwidth required for the voice traffic.

Figure 4-16 summarizes all the techniques and features discussed and recommended at different layers in the network infrastructure to provide end-to-end guaranteed delivery of your voice traffic.

Figure 4-16 *IPT Network with End-to-End Guaranteed Delivery*



As stated earlier, XYZ is planning to deploy voice applications on its existing data network. To do so, it has to deploy the right set of QoS parameters on its campus and WAN networks. This chapter has provided you the best practices for implementing QoS in the LAN/WAN environments to deploy IPT. Chapter 5 uses these best practices and some of the information collected in this chapter regarding the XYZ network to design its network to support voice applications.

Network Services

Network services are critical to the overall functionality of IPT environments. The major network services are DHCP, DNS, Network Time Protocol (NTP), and directories and messaging.

DHCP

All IPT implementations should implement DHCP for IP phone provisioning; otherwise, manual phone configuration is required, which is not a recommended practice. The DHCP service should support adding custom option 150, or you can use option 66 to support Cisco IPT deployment. DHCP uses options to pass IP configuration parameters to DHCP clients. The following are some commonly used options:

- **Option 003**—IP address of the default gateway/router
- **Option 006**—DNS server IP addresses
- **Option 066**—TFTP boot server host name

The custom option types are configurable parameters in the DHCP server, which passes the values specified in these custom options to DHCP clients when leasing the IP configuration information. Most options are defined in DHCP RFC 2132. You can define the custom options based on need. IP phones and other IPT endpoints in a Cisco IPT network can receive the information about the TFTP server via custom option 150 or option 66. The endpoints then contact the TFTP server to download the configuration files. The advantage of using custom option 150 over option 66 is that you can configure an array of IP addresses corresponding to more than one TFTP server in custom option 150, whereas option 66 allows you to configure only one host name. IP phones and other IPT endpoints understand the array of IP addresses listed in custom option 150 and use this multiple TFTP server information to achieve redundancy and load balancing of the TFTP server in the IPT network.

If your network already uses a DHCP server to lease out the IP addresses for the PCs/workstations, you can use the same server to lease out the IP addresses for the IPT endpoints as long as they support custom option 150 or option 66. In small-scale IPT deployments, involving 500 or fewer IP phones, you can enable the DHCP server service on the CallManager Publisher to lease the IP addresses to the endpoints. For larger deployments, you should consider separating the DHCP server function-ality from the CallManager Publisher server to avoid the extra CPU utilization of the DHCP service.

When you are deploying Cisco IPT solutions, use of custom option 150 is recommended because of its ability to send the TFTP server information as an IP address (or as multiple addresses to achieve load balancing and redundancy) instead of as a single host name, as in the case of option 66.

DNS

DNS translates domain names to IP addresses and vice versa. This process is also referred to as name resolution. You can use the local name resolution methods by using the LMHOSTS/HOSTS file on each server. The following list gives you some of the processes that depend on name resolution when deploying the Cisco IPT solution:

- The SQL replication process keeps the SQL database information synchronized among all the CallManager servers in the cluster. SQL replication processes on each server use the local LMHOSTS/HOSTS file to learn about the other servers in the cluster. Hence, the recommendation is to use the LMHOSTS/HOSTS file resolution method. (See the note following this list.)
- If you are using DHCP option 66, which allows you to configure only the host name, IP phones and other IPT endpoints need to contact the DNS server to resolve the TFTP server name to an IP address. Therefore, you should provision the DNS server to resolve the TFTP server name to an IP address.
- If you are using DHCP custom option 150, use the array of IP addresses for this option rather than the host names, to avoid the dependency on the DNS server. If you choose to use the host name, ensure that the DNS server is provisioned to resolve the TFTP server name(s) to an IP address.
- If you are planning to use MGCP gateways in the IPT network, you have to enter the router/switch host name in CallManager while configuring the MGCP gateway. If the router/switch is configured with the domain name (by using the **ip domain-name** *word* command), you must configure the fully qualified domain name (FQDN) in CallManager instead of just the host name. For example, if your router/switch host name is 3745-GW and you configured the domain name as xyz.com (using the **ip domain-name xyz.com** command on the router/switch), then, in CallManager, when you are configuring the gateway, you should use 3745-GW.xyz.com as the MGCP domain name. In this case, CallManager needs to contact the DNS server to resolve the 3745-GW.xyz.com name to an IP address. You can get away without using the DNS name by configuring the static name resolution entry in the HOSTS file. However, in a network with a large number of gateways, this becomes a tedious task.
- If you are considering CallManager directory integration with an external directory (refer to the “Directories and Messaging” section later in this chapter), you should use the DNS name of the domain controller when configuring and installing the directory plug-in instead of specifying an IP address. You can configure DNS to return more than one IP address for a single host name. That way, CallManager can contact the alternate domain controller if the first domain controller is not reachable.

NOTE To use local name resolution using the LMHOSTS/HOSTS file, you need to configure the mapping of host names and IP addresses in each file. These files are located in the C:\WINNT\system32\drivers\etc directory on CallManager servers and other Cisco IPT application servers. The disadvantage of using this method is that you need to visit each server and update the files whenever you make changes such as adding, deleting, or modifying the name-to-address mappings for the servers. The benefit of using this name resolution method is that you avoid the dependency on the DNS services.

NTP

NTP service ensures that all the network devices synchronize their clocks to a network time server. If you already have an existing NTP server in the network, you should configure all the IPT devices (such as CallManager servers, voice gateways, and other IPT application servers) to use the same NTP server. Refer to the following Cisco.com web page to find out how to configure CallManager and other IPT application servers to synchronize their time with the NTP server:

http://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/products_configuration_example09186a008009470f.shtml

Directories and Messaging

As discussed in Chapter 1, in the "CallManager Directory Services" section, embedded in CallManager is an LDAP-compatible directory called DC Directory (DCD), which can be integrated with corporate directories such as Microsoft Active Directory and Netscape Directory. Directories store employee-related information such as e-mail ID, phone numbers, location, and so forth. Cisco IPT applications use DCD to store user information such as password, PIN number, phone number, speed dials, and so forth.

If your enterprise already has Active Directory or Netscape Directory deployed, you can integrate Cisco IPT applications with such external directories without using the embedded directory. This directory integration reduces the administrative overhead by providing a single repository for all the applications (IPT and enterprise applications). If you are considering directory integration, you need to understand the directory architecture before you proceed with the integration. XYZ uses Microsoft Active Directory and requires corporate directory access from the IP phones. XYZ does not want to use directory integration.

If you are considering deploying unified messaging, you also need to understand the architecture of the existing messaging network. Chapter 7, "Voice-Mail System Design," discusses this in more detail. XYZ uses a Microsoft Exchange–based e-mail messaging application and wants to deploy a unified messaging system.

So far, this chapter has discussed how to analyze the existing LAN/WAN infrastructure and the availability of various network services. The following section looks at the power and environmental infrastructure. This infrastructure plays a major role in IPT deployments, because when you deploy IPT, you need to plan and provision your power infrastructure to handle the power requirements not only for CallManager and other application servers, but also for the numerous endpoints such as the Cisco IP Phones.

Power and Environmental Infrastructure

Lack of power and environmental reliability can dramatically affect overall IPT network availability. Even short-term outages require rebooting of affected equipment, increasing the length of time that equipment is unavailable.

Deployment of an IPT solution to take advantage of inline power–capable switches and IP phones decreases the cost of maintenance and enables faster deployment. In this method of deployment, IP phones receive power from the attached LAN switches. Hence, deployment of redundant power supplies in the wiring closet switches ensures high availability. In addition, battery power backup systems and generator backup systems make the network highly available.

Power and environmental planning is not unique to IPT deployments. Legacy phones also generally receive power from the legacy switch with UPS and generator power provided for the PBX.

The following factors affect power- and environmental-related availability:

- Availability and capacity of the power backup systems, such as the uninterruptible power supply (UPS) and generators
- Whether or not network management systems are used to monitor UPS and environmental conditions
- Whether recommended environmental conditions such as heating, ventilation, and air conditioning (HVAC) for network equipment are maintained
- Availability and quality of the surge-protection equipment used in the infrastructure
- Natural threats inherent in the geographic location of equipment, such as lightening strikes, floods, earthquakes, severe weather, tornados, or snow/ice/hail storms
- Whether the power cabling infrastructure installed is conformant to National Electrical Safety (NEC) and IEEE wiring standards for safety and ground control
- Whether during power provisioning process factors such as circuit wattage availability and circuit redundancy for redundant equipment and power supplies are taken into consideration
- Reliability of the IPT equipment sourcing the power to the IP Phones

When deploying IPT, calculate the amount of power required ahead of time by taking into consideration the number of in line powered IP phones and the additional number of servers such as CallManager and other application servers. While designing the IPT solution, ensure that, where possible, multiple power drops and redundant power supplies are provisioned in the network to further boost the availability of each device.

Table 4-6, from American Power Conversion (APC), provides power availability estimates with various power-protection strategies.

Table 4-6 *Power Availability and Protection Strategies*

	Raw AC	5-Minute UPS System	1-Hour UPS System	UPS System w/ Generator	Power Array w/ Generator
Event Outages	15 events	1 event	.15 event	.01 event	.001 event
Annual Downtime	189 minutes	109 minutes	10 minutes	1 minute	6 seconds
Power Availability	99.96%	99.979%	99.998%	99.9998%	99.99999%

Source: American Power Conversion, Tech Note #24

From Table 4-6, it is clear that to achieve five 9's of power availability, you need a UPS system with a generator.

When you are deploying an IPT solution with inline power capable switches in the wiring closets, it is essential to calculate the capacity of the power supplies required in each wiring closet. To make this calculation, you need to make a list of the following items:

- The switches and routers in the network that need to provide the inline power to IP phones
- The switch/router hardware platform
- The quantity of IP phones, along with model numbers, that connect to each closet switch (power consumption varies between IP phone models)
- Other modules that are installed in the switch

To determine the power supply requirements of the Cisco switches and routers, to provide inline power to IP phones, use the web-based Cisco Power Calculator, available at http://tools.cisco.com/cpc/launch.jsp.

NOTE At the time of planning, you would not have decided which switches to use to connect the IP phones, or the quantity and type of IP phone models required in the network. Hence, it is impossible at this stage to determine the total power consumption and switch power supply capacity requirements. Typically, you finalize which IP phone models and quantity to use during the design phase. Because power is an infrastructure component, all the information that is required to properly size the power is covered in this chapter, and Appendix B includes the tables to document the switch/router inventory.

Telecom Infrastructure Analysis

This section examines the XYZ telecom infrastructure. The Telecom Infrastructure Analysis Questionnaire, included in Appendix C, assists you in conducting this analysis. You need to conduct this analysis to understand how the current telecom infrastructure is built and how it operates. Based on this information, you can design the IPT network so that it operates in a similar way, and at the same time introduce new features and services. The information presented in this section uses answers that XYZ provided to the questions in the questionnaire.

PBX Infrastructure and Migration

XYZ requires replacement of the PBX systems at all the remote branch locations and at the Sydney HQ location, except at the San Jose location, as mentioned in Chapter 3.

The PBX at the San Jose site requires integration with the new IPT system. Table 4-7 provides the details of the PBX systems at the San Jose and Sydney locations. This information helps you to determine what types of gateways are required to achieve the integration, what features in CallManager need to be enabled, etc.

Table 4-7 *Details of XYZ PBX Systems*

Site	PBX Vendor Model Software Version	PSTN Interface Signaling	Interface Type to IPT System	Number of T1 Trunks to PSTN
San Jose	Lucent/Avaya Definity G3Si Version 10	T1-PRI NI 2	T1-QSIG	6
Sydney	Lucent/Avaya Definity G3Si Version 10	E1-PRI NET5	E1-QSIG	4

The large user presence at the San Jose site prevents a complete forklift of the PBX system. Hence, a slow migration is required at this site. A discussion with the PBX staff at San Jose proposed the solution described next for smooth migration of users to the IPT system.

As shown in Table 4-7, the San Jose site has six T1 trunks. At the beginning of the IPT deployment in the San Jose site, only four of the T1 trunks that are currently terminating on the PBX will be moved to voice gateways in the IPT system. In Sydney, you need to plan a complete migration to IPT. All users will retain their old PBX extensions after the migration to the new IPT system. When a user moves to the IPT system, the legacy PBX is configured to forward the calls to their IP phone.

At the end of the complete migration of users to the IPT system, all the remaining T1/E1 trunks will be moved to voice gateways. At this point, the legacy PBX systems might be removed.

Telephony Numbering Plan

XYZ uses a four-digit dial plan at every central and remote branch location. After the migration to IPT, each user will retain their old extension number on the new IP phones. At all sites, the carrier sends all the digits to the PBX. PBX retains only the last four digits to extend the call to the end station.

Table 4-8 provides information on the PSTN trunk types, Direct Inward Dial (DID) numbering ranges, and numbering plan for each site of XYZ.

Table 4-8 *Current Numbering Plan at XYZ*

Site Name	DID Range	Station Directory Range	Type of PSTN Signaling
San Jose	+1 408 555 3000 to +1 408 555 4999	IP Phone DNs 3000–4999	6 T1 PRI NI2
	+1 408 555 2500 to +1 408 555 2999	PBX station DNs 2500–2999	
Seattle	+1 206 555 2100 to +1 206 555 2199	2100–2199	1 T1-PRI
Dallas	+1 972 555 5600 (grouped line) +1 972 555 5611 (fax)	5601–5619 (Non-DID numbers, private numbering plan)	1 T1-PRI
Sydney	+61 2 5555 6000 to +61 2 5555 6999	6000–6999	4 E1 PRI ISDN Net 5
Melbourne	+61 3 5555 4300 to +61 3 5555 4399	4300–4399	1 E1 PRI ISDN Net 5
Brisbane	+61 7 5555 8680 (grouped line)	8681–8699 (Non-DID numbers, private numbering plan)	1 E1 PRI ISDN Net 5

Voice-Mail Infrastructure and Migration

From the initial requirements given in Chapter 3, XYZ has two voice-mail systems: one at San Jose and the other at Sydney. The Simplified Message Desk Interface (SMDI) integration method integrates the Octel voice-mail system with the PBX systems. The deployment of IPT enables migration of user mailboxes from Octel systems to the Cisco Unity system in a phased manner. As per the XYZ requirements, discussed in Chapter 3, in the "Integration and Replacement of Legacy Voice-mail Systems" section, Cisco Unity will be deployed in Sydney with the unified messaging mode in redundant fashion and the Octel voice mail systems in San Jose will continue to exist.

During the migration, XYZ requires all the users to be able to send and receive between the Octel voice-mail system in San Jose and the Cisco Unity system in Sydney. This requires networking of Cisco Unity and Octel voice-mail systems. The Cisco Unity Bridge application provides intermessaging between Cisco Unity and Octel voice-mail systems.

Emergency Services

Today, XYZ uses basic 911 service, in which calls are forwarded to a public safety answering point (PSAP). There is no guarantee that the call reaches the correct PSAP, and the PSAP does not get information about the location of the caller.

The Enhanced 911 (E911) solution, an advanced version of basic 911 services in North America, addresses the user mobility issue and provides the following benefits:

- Automatically provides the location of the caller to the PSAP
- Calls reach the right PSAP based on the user location

Cisco Emergency Responder (CER) tracks user movements and sends the user's current location information to the PSAP. CallManager provides the basic functionality required to route the emergency calls.

The XYZ branch offices are located in Seattle, Washington, and Dallas, Texas. As discussed in Chapter 1, in the "Cisco Emergency Responder" section, these two states do not require businesses to comply with E911 (as of the time of writing the design proposal). Hence, you do not need to design the IPT network with CER.

Telephony Features and Applications

The current PBX systems at the San Jose and Sydney central sites support basic functions, such as call forwarding, call transfer, call conferencing, and the following applications:

- Auto-Attendant
- An internal help desk support group with 10 agents supporting internal IT issues of XYZ
- An external help desk support group with 40 agents supporting XYZ product issues

XYZ requires the future IPT network to migrate all the legacy applications to the IPT system. In addition, XYZ would like to implement the following functionality in the newly built IPT system:

- IP phone services
  - Corporate directory lookup from IP phones
  - Calendar and other useful services
- Extension Mobility feature for mobile users
- Cisco IP SoftPhone support for a few users

Business Continuity and Disaster Recovery

Before you deploy any new product or system in the network, it is important to understand not only the potential underlying risks and impact of disasters, but also how to quickly recover from such situations and document these procedures by developing a business-continuity or disaster recovery plan.

In legacy voice networks, the central component of call processing are the PBX/key systems. A PBX system comes with dual process cards so that a failure of one card does not affect business operations. In a similar way, the Cisco IPT system offers grouping of CallManager servers to form a CallManager cluster. A cluster offers high availability. A failure of a single server in the cluster does not impact the call processing.

An organization that is looking for a high level of business continuity in case of any disaster should consider splitting a single CallManager between multiple data centers. Refer to the "Clustering over the IP WAN" section in Chapter 1 to understand this design and recommended best practices.

The second factor that affects business continuity is the availability of the backup power, as discussed earlier in this chapter in the "Power and Environmental Infrastructure" section.

You need to include the IPT systems as part of your backup operations and protect the systems from viruses and other security attacks by installing antivirus tools.

Securing IPT Infrastructure

The Internet has made it easy for anyone to access different denial of service (DoS) tools, viruses, and applications that are used for financial fraud, theft of information, and sabotaging data or networks. Usually, someone writes an application and puts it on the Internet, available for everyone to grab.

Many tools are easily available on the Internet to attack networks. These include, among many others, tools to carry out DoS attacks, VLAN attacks, Address Resolution Protocol (ARP) attacks, MAC attacks, and spanning tree attacks. If you are deploying real-time applications

into your data networks, you need to make sure that security breaches are prevented. These security breaches can slow down or bring down the network, causing the network to be unable to support voice calls. You need to make sure that your internal and external network is not misused in any way. For example, if someone tries to introduce large amounts of traffic across your WAN link, it results in dropped voice calls. This is a potential case of DoS attack and, in this situation, having the right set of QoS policies and CAC in place prevents the excessive traffic and avoids the call drops.

Deciding which security measures to implement requires that you balance how much risk you are willing to accept and how much money you are ready to spend to protect your network against security breaches.

Regardless of your decision, you have to make sure that your network is built following a layered approach and you have taken the necessary measures to secure it at every layer. This means that compromised security at any one layer does not compromise security at every layer. For example, if someone is able to break the password and get into one of the VLANs, IP phones, CallManager, or any other network component, they should not be able to get into the whole network. PC endpoints usually require user authentication, but typically IP phones do not. You have to realize that if you want to build a secure IPT network, you have to build it on a secure data network. If your data network is not built securely, you will not be able to build a secure IPT network.

Remember that now your voice is traveling over your existing data network. Some of the simple steps to provide security include having separate voice and data VLANs, using access control lists (ACLs), and using firewalls.

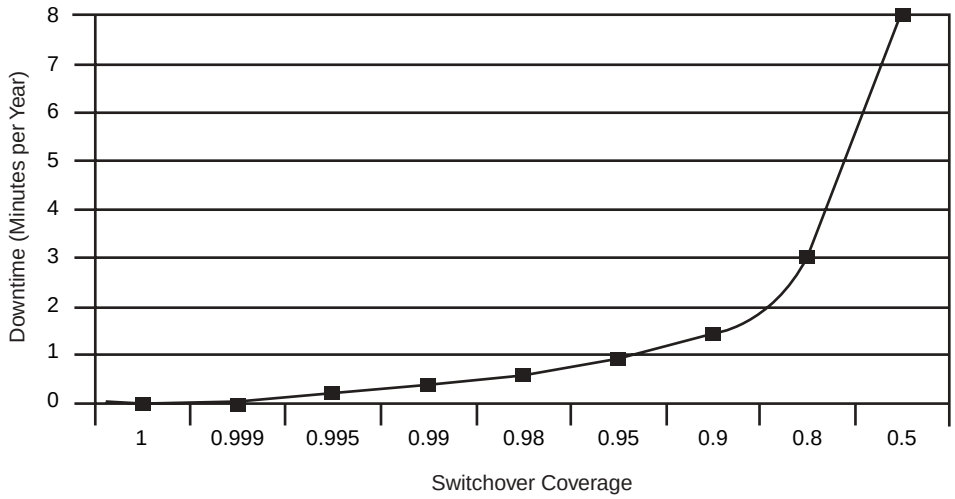
Chapter 6 provides security recommendations to protect the XYZ IPT infrastructure.

Redundancy and High Availability

The key component of network design is redundancy. Redundancy not only prevents equipment failures from causing service outages, but it also provides a means for performing maintenance activities such as upgrades without impacting the service.

The predominant factor that determines the effectiveness of a redundancy scheme is the switchover coverage, defined as the probability of a successful switchover to the standby side whenever needed. Switchover coverage of 0.9 indicates that, on average, when a switchover is required, nine out of ten incidents will be successful. The chart in Figure 4-17 illustrates the impact of switchover coverage on the downtime of a system.

Figure 4-17 *Impact of Switchover Coverage*



Switchover coverage of 0 is equivalent to a simplex (nonredundant) system, thus rendering the redundancy setup completely ineffective. Switchover coverage of 1 represents an ideal redundancy setup; it reduces the downtime of a simplex system by about four orders of magnitude. Although it is difficult to achieve perfect coverage, a good redundancy design can achieve coverage of 0.99, which offers a downtime improvement over a simplex system by about two orders of magnitude.

Availability refers to the percentage of total time that a network or system is available for use. A network or system that has high availability includes specific design elements that are intended to keep the availability above a high threshold (for example, 99.999 percent).

XYZ requires the highest level of availability at every layer and component of the network. The following is a list of a few design principles to achieve high availability:

- **Maximize the redundancy**—Maximizing the redundancy allows you to provide uninterruptible service to the end users. An example is a CallManager cluster, which contains more than one server and provides call-processing redundancy. Another example is the XYZ LAN infrastructure, which has two distribution layer switches and two core layer switches to provide redundancy.
- **Minimize complexity**—Reducing complexity minimizes the time to rectify problems, thereby increasing the overall availability of the system or device.
- **Minimize points of single failure**—Minimizing single points of failure increases the redundancy in the network. An example is a connection to the PSTN. If you have only a single T1/E1 circuit that, for some reason, goes down, no one from that location can make outbound calls. Hence, you should plan for redundant circuits to minimize these types of single points of failure.

As you have seen in the infrastructure analysis, XYZ has a high level of availability and redundancy in its current infrastructure. Chapter 6 provides recommendations to achieve the same level of high availability and redundancy for the IPT infrastructure of XYZ.

IPT Network Management System

Each IPT deployment is different, but generally, a Cisco AVVID IPT environment includes a CallManager cluster, IP phones, a PSTN gateway(s), a voice-mail system (Cisco Unity and/or a legacy voice-mail system), L2/L3 switches, routers, and applications such as Automated Attendant, Personal Attendant, Emergency Responder, CCC, CRS, and others.

While you are planning for management and monitoring of an IPT network, the main goal should be to define a list of parameters that can be proactively monitored in an IPT environment. The output of these predefined parameters is intended to establish a set of alarms for spontaneous problems and a proactive early-warning system that is based on comparing baseline data to current conditions.

The following two steps help you to define a solid management and monitoring policy for your IPT network:

- Define a set of parameters that needs to be monitored on every component of your IPT network.
- Select IPT network management and monitoring products and tools that are capable of monitoring the defined set of parameters.

Several products and tools are available to manage and monitor your IPT network. The CiscoWorks IP Telephony Environment Monitor (ITEM) product gives real-time, detailed fault analysis specifically designed for Cisco IPT networks and other products from third-party vendors. It is a proactive tool to evaluate the health of IPT implementations. Cisco ITEM provides alerting and notification of problems and areas that you should address to help minimize IPT service interruption. Cisco ITEM also identifies the underutilized or imbalanced gateway resources, whereas its historical trending and forecasting of future capacity requirements helps you to plan for growth.

Given the type of IPT infrastructure, CallManager server health, CallManager services health, CallManager functionality, IP phones functionality, IP gateway health, QoS monitoring, L2/L3 switches, and applications are some components that we recommended for monitoring your IPT network.

XYZ requires proper network management tools to monitor its IPT infrastructure. Chapter 9, “Operations and Optimization,” discusses in detail the parameters, tools, and techniques for managing and monitoring IPT networks.

Summary

This chapter provided the tasks and best practices involved in the planning phase of the IPT deployment. It used XYZ's answers to the questionnaires provided in Appendixes B and C to plan the IPT network. You have also seen the steps that are required to ensure that the infrastructure is ready to carry the converged traffic. Based on all the information collected and the current state of the XYZ network, Chapter 5 covers the design of network infrastructure, such as enabling QoS in the LAN/WAN, to support the IPT rollout for XYZ.