

## Moving from Legacy to Convergence

As should be expected, migrating a network from a legacy architecture to a next-generation technology is not a small undertaking. It involves so much more than simply launching a few platforms, connecting up the circuits, and calling it a network.

There are countless systems and applications that are all connected in some fashion to the network as well as the various network elements. These systems must somehow interoperate with all the other systems and applications, to ensure a seamless transition. Throughout the entire process of transitioning the network, the operator must somehow ensure that subscribers never experience a degradation in service, and that all investments are protected and future-proof.

When the telephone companies of the world implemented Signaling System #7 (SS7) and the Intelligent Network (IN), their intentions were certainly noble. Yet SS7 and the IN concept failed on a number of fronts in my mind. There was so much emphasis on the “killer application” that would somehow justify the expense of implementing such an infrastructure, that the entire industry simply set itself up for disappointment.

The concept itself was a great idea and is certainly still worth pursuing in today’s modern networks. You will see constant themes of the IN throughout this book as we discuss the various functions and features of the IMS, but the implementation needs to change.

For example, the IN called for services and applications to be located in the core of the network instead of on the network switches themselves. The idea was to reduce the cost of supporting services and applications by eliminating the need to replicate the service at every single network node.

However, for this to work, special software was required at every switch responsible for delivering the service. The switch software was responsible for accessing the service control point (SCP) responsible for providing the service. The software “triggers” became extremely expensive, and therefore it became prohibitive to launch some services on a grand scale in the smallest of networks.

When the public began pushing for more mobility, the technologists of the industry once again demonstrated how this could be accomplished using the existing architecture of the world’s networks, utilizing SS7 and the IN. But the cost to implement such

a service was just too prohibitive and therefore prevented the world from realizing this feature.

VoIP enabled mobility, demonstrating that such a service was possible using the Internet technology and was a viable service offering for even the smallest of service providers. However, the issues of security were troublesome for traditional operators, making VoIP a troublesome alternative.

The industry also learned that depending on a vendor's end-to-end platform solution was costly. SCPs, for example, would only run the software provided by the vendor selling the hardware. An SCP could cost millions for a simple service like Calling Name.

The industry is attacking these problems aggressively, as it works at redefining the world's communication networks, as well as the business model that funds them. Application platforms, for example, are being standardized on generic platforms available from any vendor at a fraction of the cost of a traditional SCP. By standardizing these platforms, operators will be able to purchase an application server from any vendor they choose, and place any vendors' software on that platform.

This means operators are no longer married to a single vendor for their service platforms. They can pick and choose from hardware vendors and software solutions to meet their business needs. This opens up a whole new market for software vendors who could not previously compete against the platform giants.

While it has been proven that voice services can be offered over the Internet, there is still work to be done to make this as robust as the traditional networks we use today. Of course in the end it may not really matter to the key buyers of communications services. The younger generation does not accord service reliability as high a priority as their parents, as demonstrated by their choice not to own a landline at home. They are perfectly content using their cell phone for all their needs, even if the service quality is not the same as what they could get from landline service.

The transition to an all-IP network means making some changes to the very technology that makes the Internet possible. These changes will make the technology all that much more robust and "carrier grade." But more important, the implementation of this technology is being well defined, providing operators with a clear and reliable means of implementing IP throughout the network, delivering Internet-like applications to all subscribers, while still maintaining the very business model that funds the network to begin with.

This chapter addresses the migration from a legacy network to an all-IP network, using planned phases rather than "flash-cutting" the entire network. The discussions throughout this chapter are based on what the author has witnessed from the world's leading carriers.

## Migrating the Backbone to an IP-Based Network

There are stark differences between wireline and wireless in terms of migration plans to an all-IP-based network. The wireline operators of the world began in the 1960s with plans to convert the backbone of their networks to packet-based rather than circuit-switched, to address the growing issue of maintaining many different levels of network for different traffic types.

Their migration has been more chaotic than wireless, often choosing new technologies as they came along, rather than crafting a long-term migration and implementation plan with a common goal in the end. Many times it appears as if the wireline operators are simply choosing the technology of the day to meet their packet requirements.

The wireless operators, on the other hand, have an orchestrated, laid-out plan and strategy for moving the world's wireless networks to packet. Consider the work of the 3GPP and the evolution of the GSM specifications. In reality, both are probably about the same when it comes to choosing the latest technology, but the 3GPP has certainly chosen an orderly migration path.

The migration from TDM-based networks to packet-based networks began some time ago. Bell Laboratories began development of Asynchronous Transport Mode (ATM) as a new backbone technology, enabling the Bell System Companies in the U.S. to move all of their bearer traffic to a packet-based network rather than a circuit-switched one.

ATM eventually moved out of the labs and began the long road of implementation in the world's networks. While largely successful, many may argue that it is still cost-prohibitive when compared to the cost of IP. Still, IP cannot offer the same reliable service of an ATM transport network, a fact that has slowed the implementation of IP in many traditional telephone networks.

The primary issue is the lack of support in TCP/IP for real-time traffic such as voice and video. TCP/IP was developed simply for the transport of data and is far more tolerant of delays and packet loss. Voice and video, on the other hand, are not so tolerant, which is why ATM was adopted so quickly.

The ATM protocol answered the primary need for all operators: Quality of Service (QoS). By laying ATM on top of a SONET fiber backbone, operators can realize a very robust packet-based backbone capable of moving all of their aggregate traffic.

However, ATM is not the best protocol for voice and video for many reasons. Developers realized that if they developed a protocol specifically for voice and data, it would consist of smaller packets delivered much quicker to the end points. This theory does not work, however, for data networks.

When data is sent using smaller packets, it takes many more packets for the successful transfer of large data files. This is not only inefficient; it can create a lot of overhead within the network. ATM was a compromise between the two; providing smaller packets for voice and video, eliminating the delays in packet transmission, while offering large enough packets to support the transfer of larger data files.

TCP/IP development has continued as well. The Internet Engineering Task Force (IETF) realized that the TCP protocol is not a good transport for real-time applications. They set off to create a new peer protocol referred to as Stream Control Transport Protocol (SCTP). This protocol was first used in support of SIGTRAN (SS7 transport over IP) and has since expanded to other uses within the VoIP domains.

Many of the shortcomings of IP have been addressed, and service providers have quickly learned the economies brought about by an IP infrastructure. Yet providing highly reliable and secure telecommunications services over an IP network requires some changes to the technology as well as the implementation of IP networks.

One of the key issues with VoIP is really an implementation problem. There is lacking a set of implementation/interoperability standards for the deployment of a VoIP network.

## 30 Chapter 2

For example, an operator may choose to deploy a media gateway controller (MGC) for call and session control, but it has many choices for the session control protocol.

Even if an operator selects SIP, there is little defined in the way of implementation for SIP today to support security. Certainly if we investigate the breaches that have been committed today in VoIP networks, we will find that these breaches were a direct result of implementation weaknesses.

Quality of Service (QoS) and bandwidth management are a couple of key areas that have required work in the past as well. Operators have adopted numerous methodologies for dealing with these issues and have begun transitioning their core network to IP.

Before an operator can take advantage of IP services, it must first convert the backbone network to packet-based. Look at how the GSM network has evolved. Wireless provides a good model for this discussion because of the planned and methodical approach taken by GSM operators to evolve the networks to support packet-based services.

GSM operators first added an overlay network to their existing infrastructure for data traffic. The base station controllers (BSCs) moved packet data traffic away from the mobile switching centers (MSCs) to this packet data network (the General Packet Radio Service, or GPRS).

The GPRS network then provided IP facilities into the Internet and other IP-based networks. This allowed the operators to make investments in their packet networks without having to expand the capabilities of the voice switches in the network.

Wireline operators have followed this path as well, deploying IP in their backbone transport networks, and moving bearer traffic over these transport networks. This is the first step toward an all-IP network.

This is where the VoIP elements come into play. In order to support the IP backbone, there needs to be conversion of traditional voice to packetized voice. This is the job performed by media gateways, under the control of media gateway controllers.

VoIP networks were developed to convert voice transmission from its traditional analog format into a digital packet format that could be transported over the new IP backbone. However, there is more to this than simply converting the voice to packet formats. Voice transmission is not tolerant of delays. If there is a delay in the delivery of the voice packets, conversation becomes intolerable.

This is the challenge faced by many VoIP providers. While many have solved the latency and QoS problems for peer-to-peer calls, there is still work to be done for calls that begin in one network and are transported to IP networks.

VoIP introduced many other challenges as well, but this is outside the scope of this book, so I won't go into those details. I will mention here though that these challenges are partly what drove the 3GPP to begin development on IMS.

But more than just voice services rely on the backbone network. Signaling is also transported through the backbone along with the voice traffic. Since signaling (SS7 specifically) is already packet data, there is no need to convert the signaling data to packet. However, the SS7 protocol relies on transport protocols that were developed for use on TDM facilities. The transport layers of SS7 (the Message Transfer Part) will not support IP facilities and therefore must be replaced with a new transport protocol before SS7 can be transported via IP.

This was the work of the IETF, which developed the SIGnaling TRANsport (SIGTRAN) protocol. SIGTRAN replaces the MTP layers of the SS7 protocol with transport protocols developed specifically for IP networks.

These protocols emulate the MTP services, over IP networks. This is necessary for a number of reasons, QoS within the signaling networks being one of the primary drivers. There are many procedures provided by level 2 and level 3 of the SS7 protocols to ensure the availability of signaling links, as well as the integrity of the signaling data itself. One of the simplest of these procedures is the transmission of a fill-in signal unit (FISU).

The FISU is really just a protocol flag carrying no real information. However, its absence signifies trouble with the transport (the physical link). The main purpose of providing this as a function is to provide a proactive, rather than reactive, detection mechanism for link failures.

In other words, instead of finding out that a link is out of service when there is data to send, the protocol and all of the network entities use the FISU as a link integrity measurement. As long as the entity is able to receive and process the FISU, the link is operating correctly. If the entity is no longer receiving FISUs, there is something wrong with the link.

The links themselves are always transmitting something. If there is no signaling data to be delivered, then FISUs are transmitted over the idle links. The entities are always checking the health of the link even when there is no data being sent.

This proactive approach to maintaining transport reliability is seen at level 3 of the SS7 protocol as well. When a link fails, there are automatic procedures to ensure the orderly routing of signaling data around the failed routes or links. This improves the availability of signaling routes by ensuring packets are rerouted through good routes when other routes and links fail.

All of this is automatic, of course, and many times when a link fails, it is brought back into service before anyone even has time to react. These processes have to be emulated in an IP environment, to continue to ensure the availability and reliability of the signaling network.

There are several protocols provided in the SIGTRAN protocol suite:

- M2UA
- M2PA
- M3UA
- SUA

SIGTRAN is used to support the transport of SS7 level 4 signaling data (ISUP and TCAP) over an IP facility. The payload of these SIGTRAN protocols is still ISUP and TCAP, so the entities themselves must still support SS7. There are also specific entities that interface with the IMS that support SIGTRAN and provide the conversion between the two signaling types, as we will discuss in later chapters.

One of these functions is the signaling gateway (SG). The signaling gateway is responsible for interfacing into the SS7 network, and converting the MTP layers to SIGTRAN

## 32 Chapter 2

back into the packet network. The ISUP and SCCP/TCAP layers remain intact and unaffected by the changes.

The signaling gateway is another means of evolving the network from a TDM-based core to an IP-based core. For example, an operator may decide to maintain its existing TDM facilities in the core network, while at the same time implementing an IP network as an overlay. As new entities are added to the network, they are added on the IP side of the network, using a “cap and grow” approach rather than a replacement strategy.

Using the signaling gateway at the edge of the TDM networks provides a bridge into the IP network. The operator can then depend on media gateway controllers (MGCs) to accept the SS7 signaling, and eventually make the conversion to SIP.

The conversion to SIGTRAN is an important stepping stone to full network transition, since signaling performs the important function of call control. Converting the signaling facilities to IP provides many economies to the operator and allows it to quickly realize additional capacity and throughput not present in its legacy signaling networks. The business case to IP backbone, therefore, becomes much easier to justify when built around cost savings, and network growth with added density.

The signaling gateway only converts the transport layers to SIGTRAN/IP. Since ISUP and SCCP/TCAP are not supported in IMS, these layers must also be converted to the Session Initiation Protocol (SIP). This conversion is provided by the media gateway controller, which accepts the SIGTRAN/SS7 signaling from the legacy network and converts this signaling to SIP-based signaling toward the IMS. This is one of the reasons operators should contemplate VoIP deployments as the next phase toward IP-based IMS.

A VoIP deployment will consist of all IP entities supporting packetized voice and data across an all-IP backbone. However, the SS7 legacy must still be supported even in the VoIP domain. Calls originating in the TDM domain will cross boundaries, as will the SS7 signaling associated with these calls, requiring support of SS7 even in the IP domain for some time to come.

### Deploying VoIP as a Growth Strategy

Besides the obvious that Voice over IP (VoIP) provides an economical means of growing the network, the VoIP functions (media gateway and media gateway controller, specifically) provide the next phase of implementation needed to support a full IMS network.

Consider this: the TDM network relies on switches, which provide all of the functions needed to originate and terminate a telephone call. These switches are expensive today and are difficult to cost-justify in small rural markets.

However, if an operator could deploy a small, inexpensive box consisting of nothing more than a switching fabric (the matrix connecting one circuit to another), the operator should be able to reduce the cost of their service offering in those markets.

Removing the “intelligence” from the switch means placing the call control in the core of the network. This was the original concept behind VoIP networks. Place the switching fabric out at the network edge, but keep all of the intelligence and call control in the core where it can be secured and maintained.

The MGC is the entity bringing call control to the core of the network. This is the entity that interconnects all of the media gateways together, and using a call control



protocol (such as SIP) communicates to each of the media gateways what resources (such as codecs) are needed to support a call or session.

The voice traffic still needs to be packetized, and network growth needs to be supported without significant investments in legacy network equipment. The purchase of additional legacy switching nodes does not make sense if there is a long-term plan to convert to IP, and VoIP can support the voice network as the operator begins its migration to IMS.

The transition at this first step is usually at the tandem level (back in the core of the network). Then as subscribers are added, or legacy equipment needs replacement, those replacements are achieved using VoIP deployments (MG/MGC). This now takes care of packetizing the voice portion of the network and supports slower markets even after IMS is fully deployed. The operator can then slowly begin retiring those legacy switches and replace them with media gateways, while extending the reach of its IP facilities to all of their markets.

Of course, we would be foolish to think that voice is the only reason to migrate to an IP infrastructure. Data is a natural fit for the IP backbone (since this is what IP was developed for), but video can be delivered over the IP network as well.

At this point, the operator has implemented IP in the core backbone, migrated its signaling to SIGTRAN/SS7, and begun deploying VoIP at the core, and then the edge of the networks to support packetized voice. Now all that is left are the service platforms and the operator is ready to declare itself a convergent network, right?

Wrong. The missing link here is still call (or session) control. While it is possible to implement an all-IP network and support any service an operator wants today, managing these networks is an absolute nightmare.

Look at companies such as Skype and Vonage. They began using proprietary architectures and session control, and quickly found out that these approaches did not scale very well. They are now in trouble as they struggle to rebuild their networks in response to tremendous growth they did not anticipate.

Add to the picture billing and partner management, and you can quickly have an absolute nightmare on your hands. Let's look at what is happening with wireless today. I have spoken with numerous wireless carriers who are providing music downloads to their subscribers. The service delivery is the least of their problems.

They found that their existing billing systems did not support this type of service, and so they had to build a completely new billing mechanism to support music downloads. This new billing system had to somehow be integrated with their existing billing systems (many operators have shared with me that they have as many as 15 different billing systems, all supporting different disparate services).

So while it is true that an operator can deliver any service it needs using an IP network, it faces many challenges when it comes to managing that network, and maintaining a secure, reliable network. This is where the IMS comes in.

## Deploying IMS

The business case for deploying IMS is not about the services it provides (there are none), nor is it the killer applications (there are none). The business case for implementing IMS is a little more difficult than that, but all the more rewarding long-term.

## 34 Chapter 2

Implementing IMS is about supporting a single architecture for all services, rather than multiple systems for multiple services.

For example, let's say you are an operator with a traditional IN-based network (using SS7 call control/signaling). You now want to offer your subscribers a new service for music downloads. Since SS7 does not support this type of service, you will have to find an alternative (most likely an IP-based service delivery platform with this capability).

Your billing system is the next hurdle. Your present billing system supports CIBER/TAP3 records from your switches, but it does not support IP-based services, so you will have to add a new billing system as an overlay to your existing system. This will somehow have to be integrated into your present billing presentment system so that the proper charges can be applied to the subscriber bill.

To make matters worse, your present billing mechanism (and all audit functions of that billing system) are based on a minutes-of-use model. Music downloads are not billed this way. Subscribers pay for the music download one time, for a flat fee. In some cases, you may want to issue a license where the subscriber pays for a period of time. At the end of that period of time, the subscriber has to pay another cycle.

Your legacy systems do not support this model, and hence the need to add new systems that do not integrate very well with the legacy systems. You end up managing these separately.

You now have the billing taken care of, but you have no means of auditing the transactions between the subscriber and your content delivery platform. Worse, the content is owned by another content provider, so you must interface to its server to purchase the content, and then deliver the content to your subscriber. The content provider must be paid at the time of your transaction, but the subscriber is not going to pay before receiving a bill from you at the end of the month.

When the subscriber finally receives their bill, that subscriber refuses to pay, because he or she never received the content. You do not have the tools to see the transaction when it took place because your existing monitoring system does not support IP networks and does not provide visibility to the IP transactions with the content provider. You have to purchase yet another system to monitor the IP portion of your network.

And of course, we haven't talked about the network requirements to provide the transport of music to your subscriber. Delivering music downloads over IP is simple, yet it can be complicated if you are trying to ensure that the music is indeed received by the subscriber. If you are relying on the Internet model for this service delivery, be prepared to lose revenues from piracy (already prolific over the Internet). Now you have to add a digital rights management system (DRM). Which of course cannot be integrated with any other systems in your legacy network.

This is not so far-fetched. There are many operators today delivering multimedia services using their traditional networks with IP overlays. However, when one tries to support all of the back office requirements and other support systems needed, it quickly becomes a nightmare to support.

This is why the IMS is a better alternative than traditional approaches, or even pure IP-based networks. The Internet model works great as long as you don't care about things like security, business intelligence, customer care, fraud, and billing. When it



comes to these things, the Internet model becomes much more difficult and costly to implement.

The IMS, on the other hand, is designed to support all media, and all services, using one common architecture and one common signaling method. This simplifies all of the other functions needed by an operator to support its network and its services.

It also reduces the overall cost of supporting multimedia. A service delivery platform can be reused for many different services, all running through the same facilities. All of your platforms are interconnected through the same infrastructure, making it possible to offer unique, value-adding services such as presence.

The ability to begin integrating various services is an important factor to consider when making a decision toward implementing IMS. Tying many different platforms together to support a single service is no small feat if all of these platforms rely on proprietary protocols. IMS supports this capability by normalizing all session control through SIP. This is perhaps the killer app for IMS.

Changing to IMS does not happen overnight. There are many legacy systems that will have to interoperate with the IMS network as it is implemented. Some operators have chosen to treat their IMS deployments as green-field networks, running them completely separate from their legacy networks. This can work, but it leaves a lot of legacy equipment stranded with no opportunity of recuperating the capital investments.

Others have chosen a more transitional approach, using the legacy network and the IMS together, with gateways and other elements in between the two networks supporting the interworking between the services layer and the transport layers. This approach ensures subscribers continue enjoying the services they have now, while providing them the opportunity to enjoy new multimedia services, without abandoning any part of the network.

This certainly makes the best business sense. Simply “turning away” from the legacy network and dumping all your investment into an IP infrastructure is not smart business; it quickly strands your core subscribers on the legacy side with non-competitive services. Operators need the ability to continue offering their legacy customers new, innovative, and competitive services through strategic investments in their legacy networks.

At the same time, new services should be offered on IMS-ready platforms to prevent the stranding of those investments. This ensures the platforms the operator invests in will make long-lasting investments supporting an all-IMS environment when the time comes.

Most will agree that if a legacy network exists, the best approach is to transition from an IN-based network to IMS. This is much easier to accomplish in the long run when using solutions available today to bridge between the old and the new. The sections that follow provide more detailed information about how these networks interoperate with one another.

### **Interworking Between the Legacy Network and IMS**

Within the core network there are two parts of the network that must be supported. The transport of bearer traffic is the easiest. Once bearer traffic is packetized, moving it through an IP infrastructure is much simpler (yes, I know I am oversimplifying things here) than maintaining a TDM circuit-switched network.

## 36 Chapter 2

The voice is in a form that must be converted to packet before it can be sent through the IP infrastructure. The IMS itself is not really a part of this, since the IMS is really the call control portion of the network. The IMS itself is the architecture that allows the various packet elements within the network to communicate all aspects of the sessions and share this information between multiple entities.

The second challenge comes in the form of signaling, which is really session control. Session control ensures that subscribers are able to access the same services they enjoy in their home networks anywhere they connect. It is what ensures a subscriber is legitimate and is authenticated prior to connecting to your network. Session control is about maintaining complete control over every service you deliver in your networks, enabling security, billing, and much more. Signaling and session control are how network entities exchange information about a session in an effort to be able to support the session.

This means converting the signaling plane from SS7 to SIP after implementing IP as the transport for the signaling network. SIP is the call control signaling protocol for the IMS. It replaces SS7 in the control plane, supporting all forms of media in addition to voice. This model is very similar to the Intelligent Network (IN), where SS7 is used to communicate between network entities for the support of voice.

The IMS provides the same functions theoretically as the IN used today, except the IMS supports more than just the voice services. It supports all media types and all services within the network, using the same signaling and the same call control.

Again, it is not foreseen that the service providers of the world are simply going to abandon their SS7 networks and start replacing them with SIP. This has never been the case historically as new technologies came along. Certainly SS7 and the IN were not implemented overnight. Operators took many years to implement their SS7 networks, implementing small portions of the network at a time, until eventually the entire switching network was interconnected with SS7 signaling.

So far we have only discussed the transition of the voice transport and signaling parts of the network. There is much more to a network than signaling and switching. The support systems that are used to manage these networks is perhaps the most important aspect of the business, because it is these support systems that allow an operator to maintain profitability, secure the network from attack and unauthorized access, and accurately bill for its services.

### Migrating the OSS/BSS

The jury is still out when it comes to OSS/BSS systems for the IMS. Much is yet to be done to provide a complete end-to-end solution for the various functions within the back office and support systems. Provisioning of the various entities, managing the facilities through inventory systems, and service order provisioning where new services are activated for subscribers are some of the functions required to support any telephone network.

There are some solutions available on the market today, supporting SIP and DIAMETER protocols and providing various functions such as monitoring and provisioning. Many more are being developed.

The charging systems used to support billing are evolving, as are the standards themselves. The 3GPP is continuing development of the charging standards to be used in IMS. Charging must be changed, because the IMS supports all forms of media in addition to voice. Charging systems today are built for voice services, or for event-type charging (such as messaging delivery), but do not integrate very well. The 3GPP has addressed this through a completely new architecture to support the charging for multimedia services throughout the network.

Performance management systems are continuing to evolve as well, but most have not yet been developed to capture end-to-end network transactions. This is a critical factor in maintaining an IMS network; not just for performance management but also for revenue assurance and security.

For example, if you are providing music downloads, provided through a third-party partner, your monitoring system should be able to capture the entire transaction. This includes the signaling from the handset requesting the download (the HTTP session accessing the Web portal and selecting the link to download the music file). The File Transfer Protocol (FTP) session used to download the music file from the content provider's server through your network to the handset should be captured to ensure successful delivery. The entire transaction should be captured on the same system so that you don't have to deploy multiple systems to trace each part of the transaction.

It is simply not enough to see one portion of the network. As an operator, you must be able to monitor everything that occurs in the network; from the handset to the service delivery platforms, back to the handset. This is especially important as the revenue chain shifts from minutes-of-use to content purchases.

There are many different functions in OSS/BSS. I will cover the basic functions, but there are most likely many more within your own networks that need to be updated to support SIP. The basic functions are as follows:

- Network monitoring
- Billing and revenue assurance (collection and mediation)
- Service management

Network monitoring has traditionally entailed connecting probes to signaling links within the SS7 network and collecting the SS7 signaling messages for analysis. These systems typically operate in a real-time mode, providing limited storage (anywhere from three minutes to three days). This is typically fine for most troubleshooting, but some applications require much more storage capacity.

The purpose of the network monitoring system is to report on the health of the signaling network and all of its facilities. This involves alarming when signaling links fail or reach congestion, and reporting on the status of the signaling entities themselves. Over the last several years, these same systems have begun providing *call detail records (CDRs)* based on the SS7 signaling.

These CDRs are then fed to other systems such as fraud management applications and billing systems used for inter-carrier billing. These systems were not designed for

## 38 Chapter 2

the tasks many operators need today, simply because there were no requirements to monitor anything more than the voice setup.

In the IMS, monitoring is much different. The IMS supports all sorts of transactions, and it supports many different types of protocols on the data side (such as HTTP and FTP). SIP is used to provide session control, but there are many Internet protocols that are used to access various files and services that must be monitored along with the SIP.

Also consider that the IMS is all-IP, so tapping into the IMS requires tapping into the routers used to interconnect the various IP facilities. All entities within the IMS are interconnected using routers and IP interfaces, so at the transport layer IP must be the first source for capturing session data.

Obviously, since the facilities operate somewhat differently than traditional TDM-based facilities, the metrics used to measure the quality of the facility will change, but the most significant change is the capacity required. The amount of signaling that takes place in an IMS environment is many times higher than found in traditional SS7 networks. In fact in many trials the network vendor Tekelec has participated in, there has been a ten-fold increase in the signaling volume (just voice sessions alone).

There are many reasons for this such as registration and security procedures. When you add in video, messaging, audio, and any other media session supported in IMS, the volume grows exponentially. This is because the IMS requires much more interaction between the user device and the network. These transactions must be captured by the monitoring system in order for the monitoring system to be able to provide the status of the device, QoS of the network transactions, and the overall health of the entities within the IMS.

One benefit of monitoring IMS networks is that everything is managed in one network architecture with the same signaling protocol. SS7 is strictly voice, but SIP controls everything within the IMS. This can be a significant benefit to companies looking for more visibility into their networks and subscribers' activities.

This provides much more opportunity for monitoring systems. Instead of focusing on the health of the signaling network, these systems need to evolve to support many different functions. The newest trend is to use signaling data combined with subscriber data to create business intelligence. Monitoring systems can and should play a very central role in providing the necessary data and software applications for business intelligence within IMS networks.

This is especially true in IMS because literally everything a subscriber does to communicate is controlled through SIP and the IMS core. This provides an excellent opportunity for the systems collecting SIP signaling to provide this information for business intelligence as well.

Another area in which monitoring systems can play a vital role is in the collection of billing (or charging) transactions. There are two areas where billing information can be found. The first is within the SIP signaling itself. SIP signaling carries several headers used to communicate billing information to various entities within the network.

The billing (or charging) information carried within the SIP headers is then used by the various entities within the network to generate an actual charging detail record.

The charging data does not necessarily provide the information necessary to derive charging and rating, but it identifies the services being charged for and the charging entities within the IMS charging architecture that are responsible for the collection and correlation of the charging data. This information is already being captured by monitoring systems.

The charging entities themselves use the DIAMETER protocol to communicate actual charging data based on what the charging entity derived from the SIP signaling. This means that if the monitoring system is already collecting the SIP information and can support DIAMETER as well, then all that is needed is a charging verification application to compare the two sources for discrepancies.

Auditing of transactions to ensure they were successful (service assurance) and verifying charges are accurate are two very important functions when deploying IMS. They are missing from many traditional networks today, and operators are finding out very quickly as they begin looking into these areas that they are losing much more revenue than they first believed, simply because they have no visibility to the operations within the network.

Operators simply cannot afford to lose revenues because of things they cannot see. Likewise, they cannot afford to lose revenues because of service delivery failures. This is yet another area monitoring systems must be able to support. Since they are capturing the SIP data, all that is needed is an application that provides reporting of service-specific transactions. For example, was a text message delivered successfully or did it fail.

These areas require monitoring of much more than just the IMS domain. The access domain must also be monitored to be able to ascertain where trouble began, and what caused failures. This means supporting GPRS, UMTS, GSM, CDMA, SS7, VoIP (H.323, H.224, H.248, etc.), and any other technology used in the access network. If your monitoring system can support all of these areas, you are well prepared for IMS implementation and should be able to manage your IMS network very closely.

## Interfacing to the IMS

In an ideal world, connecting to the IMS would be as simple as turning on our communicator and selecting the media and service we wanted. Or better, simply communicating in whatever form tickles our fancy at any moment in time and letting the device control the rest. But alas, we are not in an ideal world.

Instead we are in a world filled with old and new, legacy and cutting-edge technology with new-fangled devices providing a myriad of applications. Yet despite all this new-fangled technology, we still have rural areas with multiparty lines and outside plant that most likely outdates most of those who maintain it. This means that implementing IMS architecture is not as simple as installing a few pieces of equipment and plugging them in. There is a lot of interworking that will be required as with any new technology.

Despite what many of the non-technical “marketers” may be trumpeting, the IMS will not replace existing infrastructure overnight. We will not wake up one day and

## 40 Chapter 2

suddenly be able to use our mobile phones as powerful multimedia devices connecting us to anyone anywhere in the world at the touch of a button.

Instead, we will find ourselves relying on the same devices we use right now, with some new features and capabilities gradually (year by year) entering our daily lives. Operators will transition their networks to IMS rather than simply replace everything from scratch. There are numerous factors for this.

First of all, there is simply too much investment in all that equipment out there. This equipment has not even paid for itself yet (at least not in accounting terms). Most operators are not willing to write their investments off for at least 10 to 15 years. Second, there is no business case to simply start over with IMS. IMS does not provide any new services or killer applications.

Rather, IMS enables new services and applications by providing the infrastructure that provides more robust control and management than the Internet does today. In the meantime, existing networks will have to interface to the IMS as part of a transitional strategy.

This is not uncommon in this industry. Many new technologies have been implemented through transitional strategies (the IN and SS7 is a good example of this). In fact we can draw many similarities and lessons learned from the early implementations of the IN.

The concept of an Intelligent Network (IN) using SS7 for call control started in 1964, continued to evolve as a standard throughout the 1970s, and was finally implemented in the U.S. in the 1980s. Europe adopted SS7 for connecting switches to one another for simple call control, but using a mesh network configuration without signal transfer points (STPs). The U.S. did the opposite, implementing SS7 with STPs for the support of 8xx service.

This was a long road from the inception of the technology to the actual implementation. But this is not the only example. ATM development began in 1969 but did not really begin taking off until the 1990s. This represents about a 20-year cycle, from beginning, to maturing the standards, to actual implementation.

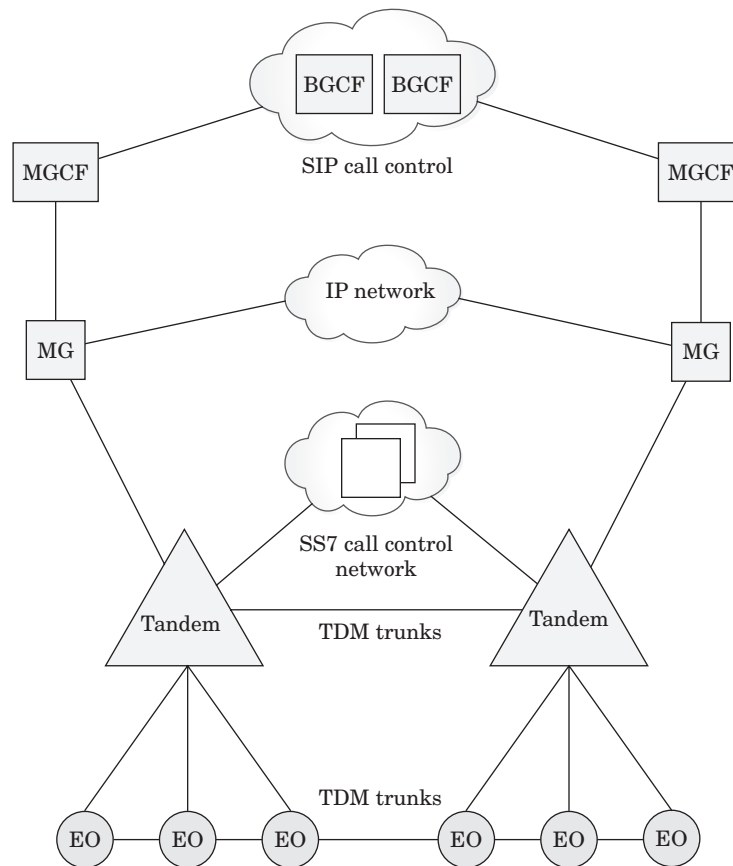
Even newer technologies and architectures such as Voice over IP (VoIP) will require interworking with IMS, as these two architectures are not 100 percent interoperable with one another. Gateway functions are required to ensure this interoperability, which is the focus of the next section.

### **Circuit-Switched Domains (CS)**

The circuit-switched domain, as shown in Figure 2.1, consists of analog and digital switching nodes, and while the voice may be digitized, it is not packetized. This requires additional nodes before the voice traffic (or bearer traffic) can be routed over an IP network. Packetizing the voice is only one requirement though.

Since the facilities within the circuit-switched domain have a different set of attributes than the domain itself, the method of signaling in the circuit-switched domain is not compatible with the packet network. In the circuit-switched world, Signaling System





**Figure 2.1** Circuit-switched domain

#7 (SS7) is used to communicate from one switch to another, the facility requirements for each call. The SS7 protocol specifically identifies the circuits to be used, the attributes of that circuit (such as codecs to be used), and even if echo cancellation is required (to name just a few identifiers).

More importantly, it is SS7 that allows switches to communicate with databases such as number portability to determine how to route calls through the network. SS7 and the IN architecture have enabled services such as wireless roaming, and many services we take for granted today (such as Calling Name and Freephone services).

SS7 can be divided into two functions. The first function is for the setup and tear-down of voice circuits between switches in the network. This is the responsibility of the ISDN User Part (ISUP) protocol. The second function is for the connection and communication with various databases within the network. This is the job of the Transaction Control Application Part (TCAP).

## 42 Chapter 2

This signaling method works very well within today's circuit-switched networks but is not compatible with packet networks, because the facilities have different attributes, and the media being sent through these facilities have different requirements. For example, in a packet network the amount of bandwidth is variable, and therefore the amount of bandwidth required for a session must be identified. The method used to packetize the voice (or whatever bearer traffic is being sent) must be identified so that the packet can be disassembled at the destination.

There is much more information exchanged, of course, in both domains, as we will see in the next few chapters as we break down the processes and procedures for the IMS signaling. Remember throughout these discussions that we are talking primarily about the signaling within each of these domains and not the bearer traffic.

When a subscriber initiates a call within the fixed circuit domain, that subscriber's location is identified through the facility he or she uses to gain access. This concept, by the way, is carried forward within the IMS as well, but with a major difference. In the circuit-switched domain, the subscriber identity is fixed to the facility (the telephone line) used to access the network. Since this location is fixed, mobility is not possible within the circuit-switched domain (at least not using today's traditional methods).

To access the network, the subscriber only needs to pick up the telephone and begin dialing. There is no consideration for registration or authentication; these are all manual processes that take place when the telephone line is ordered. The connection is then made based on the dialed digits. This is a far departure from the IMS model, where the subscriber can access the network from any location and facility, and the subscription tied to the facility itself is not usually the same as the subscriber accessing the network.

This is different for wireless, however. In a wireless network, the subscriber can be anywhere within the home network, or in another network. We will talk about the wireless model later, as there are many obvious differences between wireline and wireless challenges.

To route a circuit-switched call to the IMS, there needs to be interaction between the circuit-switched domain and the packet domain, and then the IMS domain. There may be cases where the circuit-switched domain connects directly into the IMS domain through gateways, but it is more likely that initially these connections will be made through VoIP connections.

The purpose of the VoIP gateways is to convert not only the bearer path to packet, but also the signaling required for routing the bearer traffic through the IP domain. VoIP uses a variety of signaling methods that are not always fully compatible with SS7, so breakout media gateway controller functions (BGCF) may be needed to convert this signaling. The purpose of the BGCF is to accept the SS7 signaling and use that signaling to determine how the bearer traffic is to be routed through the IP domain.

The BGCF does not necessarily "convert" in purest terms; it would be more accurate to say that the BGCF reads the SS7 signaling and uses the parameters within the SS7 signaling to determine where the bearer traffic needs to be sent. It is not converted, because most of the parameters are relevant to the circuit-switched facilities and do not apply to the IP domain. There are no echo cancellers, for example, within the

IP domain, so the parameters identifying these requirements are not needed within the IP signaling.

The BGCF will create new signaling for the bearer traffic within the IP domain, based on the destination of the bearer traffic and the attributes of the media themselves, but without regard to how it was received from the circuit-switched domain. This signaling then gets sent to the IMS access point, dependent on the architecture of the IP domain transiting the traffic. In other words, if the operator is using someone else's VoIP infrastructure for routing into the IMS domain, then the VoIP network will access the IMS through the P-CSCF within the IMS network.

If the operator is using its own BGCF, then the signaling may be sent to a P-CSCF within the same operator's network, or be sent to another operator's network acting as an IMS domain. There are also some cases where operators may implement two completely independent networks: one the legacy circuit-switched network and one the IMS network. They will need the BGCF then for generating the Session Initiation Protocol (SIP) signaling needed to communicate with the IMS, while still maintaining a connection back in the circuit-switched domain.

Consider the BGCF as the call controller between both the circuit-switched network and the IMS. The BGCF maintains the circuit-switched connection as well as the IP connections, for as long as the session requires. When the session is complete, the BGCF will then release the circuit-switched facilities by using the SS7 release procedures. It does the same on the IP side using the SIP procedures. This means that the BGCF must also be stateful, maintaining the status of every session under its control.

Once the BGCF creates the signaling using SIP, connection into the IMS is possible, but there are two variations of SIP. SIMPLE SIP is the first form developed for use in VoIP networks by the IETF, but it lacks many of the more robust attributes added by the 3GPP for use within the IMS. These extensions to the SIP protocol are required before a call can terminate within the IMS domain, because most of the extensions were added for authorization and authentication.

One other important note about routing calls from the circuit-switched domain into the IMS: the SS7 protocol is routed using Time Division Multiplexed (TDM) facilities, while the IMS is all IP-based. Many operators have already begun converting their backbone networks to all-IP. This includes the facilities traditionally used for routing of SS7 messages through the network.

Signaling gateways are used to convert the lower layers of the SS7 protocol to IP. The Message Transfer Part (MTP) is compatible only with TDM facilities and therefore must be replaced with a set of protocols compatible with IP facilities. SIGTRAN replaces the SS7 MTP while preserving the upper layers of the SS7 protocol (ISUP and TCAP). This allows operators to maintain their existing signaling infrastructure and transition the transport backbone to IP in preparation for an all-IP network.

The upper layers of the SS7 protocol (ISUP and TCAP) are still needed for managing the resources within the circuit-switched network, but they are not needed within the IP domain, as we have already discussed. The signaling gateway does not concern itself with these upper-layer protocols, leaving that responsibility to the BGCF/MGCF instead. So the operator can connect its existing SS7 network into the signaling gateway

using IP as the transport behind it and begin routing all their SS7 signaling over the IP network.

So now that we have identified all of the pieces needed to connect from the circuit-switched domain, we can talk about the flow of traffic between the networks. The call is established within the circuit switch and routed through trunking facilities to a media gateway connecting into the circuit-switched domain. The MG is controlled by a MGCF, which means the signaling comes from the MGCF.

The MGCF then interfaces to the circuit switch for signaling via SS7. The MGCF may support circuit-switched facilities for interfacing into SS7, or there may be a signaling gateway function to convert the facility to IP (using SIGTRAN) prior to connecting into the MGCF.

The SS7 message is then used to determine what the bearer traffic is, what is required at the destination to access the bearer traffic, and the final destination for the session. The MGCF then creates a SIP message for routing into the IMS. The bearer traffic continues through media gateways to the final destination.

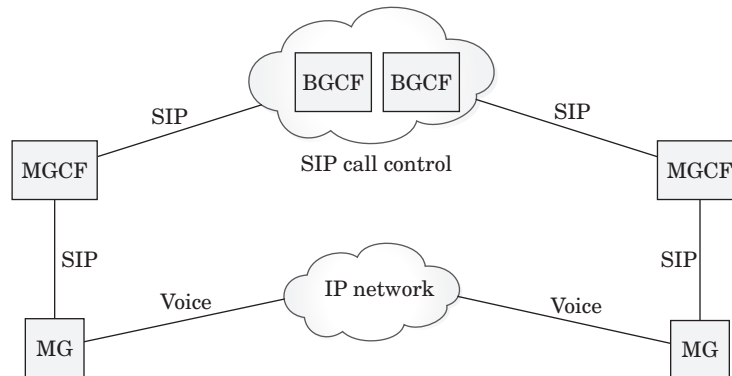
The MGCF interfaces into the IMS via a BGCF (the same function, but the BGCF acts as a signaling gateway into another network). The MGCF provides the SIP signaling needed by the IMS network to be able to set up a session within the IMS domain and control that session. The BGCF in turn connects into the P-CSCF for the serving IMS network, at which point the call is now under the control of the IMS network (at least the portion of the call within the IMS domain).

**The Media Gateway (MG)** We have so far talked about the signaling traffic, but the bearer traffic must be routed as well. It is important to understand that the IMS itself is really about call control, and not bearer traffic. In other words, to control the transmission of voice, data, messaging, video, and any other media we can think of through an IP network, while maintaining security and preventing unauthorized access, there needs to be a set of functions where this can be accomplished. It has already been proven through decades of network experience that the best means for maintaining session control in any network is through a central core function, which is what the IMS was designed around.

The bearer traffic in this scenario is coming from a circuit switch which only connects via non-IP facilities. This bearer traffic must then be converted to an IP facility. This is accomplished by sending the bearer traffic to a media gateway (MG). The MG then connects to the legacy facility on one side, and IP on the other. As shown in Figure 2.2, the MG is under the control of the MGCF, which is the same as the BGCF, with the BGCF providing a gateway function into each individual network.

There will usually be multiple media gateways connecting to one single MGCF, providing a very economical means for supporting voice services in an IP-based domain. The media gateway also supports customer premises equipment by providing an IP facility to the customer network, and connecting via IP PBX or some other VoIP entity at the customer premises.

The media gateway is really the switching fabric in VoIP networks. The switching fabric is what interconnects one circuit (or port) to another for phone calls and other



**Figure 2.2** The media gateway (MG) and the media gateway controller (MGC)

session types. The media gateway performs the task of connecting the various circuits to one another for an IP network, under the control of the MGCF.

Once the signaling reaches the IMS domain, session control is managed by the IMS, providing the necessary call control signaling back into the circuit-switched domain. For example, a voice call may be originated within the circuit domain, passed to the MG and associated MGCF, and routed into the IMS. The bearer path remains within the IP network, under the control of the domain it is residing in.

If the session is terminated within the IMS domain, the SIP will terminate the call using the BYE method. This is then forwarded back into the circuit-switched network via the BGCF, which creates an SS7 REL message back to the switch.

The easiest way to relate to this is to remember that signaling is used to communicate from one network element to another regarding the facilities that are needed to form a connection end-to-end. If the facility is IP, then MGCF is needed outside of the IMS, and CSCF is used within the IMS. We will discuss more about the CSCF functions in later chapters when we discuss the inner workings of the IMS network itself. For now, know that the CSCF provides session control within the IMS domain.

The MG therefore becomes an important element when converting voice (or other non-IP media) into packetized media for routing through a packet network. But what if you are using a SIP phone within an IP network? The SIP phone acts as the SIP user agent, and while the MGCF is still used for call control within the VoIP domain, this can later be eliminated and replaced with the CSCF within the IMS.

The long-term goal is to have all SIP-enabled devices, eliminating the need for media gateways and other devices to packetize various non-IP media. Once a phone or other device is capable of packetizing the media and creating SIP signaling, the CSCF is all that is needed for session control.

**The Media Resource Function (MRF)** In the circuit-switched domain, service tones and recordings are all provided via the switch and other external elements (such as voice response units). These are not compatible with packet networks, however. Since there

are no switches in the packet domain, there must not only be another function to generate the various service tones we are all accustomed to hearing, there must also be a controller for managing the various tones and recordings.

This function lies within the Media Resource Function (MRF). The MRF consists of two distinct functions: the media resource processor (MRP) and the media resource controller (MRC). The MRC can interface to multiple MRPs to generate all of the tones and announcements needed within the IMS domain.

The MRP then is responsible for creating the tone or announcement based on instructions from the MRC. The MRC uses SIP for communicating the requirements (such as what tones or announcements are to be provided). This replaces the methods used within the circuit-switched domain of routing calls over dedicated facilities to recording or announcement devices. In this case the facilities are IP connections.

**The Media Gateway Control Function (MGCF)** The MGCF is widely used within VoIP networks already, and its role within the IMS is the same. The purpose of the MGCF is to provide connectivity at the control layer into the IMS, controlling all of the media gateways that are managing the bearer traffic.

The MGCF is also where some features and applications reside. In the circuit-switched domain, the switches provided many features and applications such as conference calling and call park. These are now under the MGCF, which is the “brains” of the operation.

The signaling function at the MGCF provides call control for all packetized voice as it enters into the network. The MGCF only communicates with media gateways within the same domain, however, and is not intended for interfacing with other MGCFs in other networks. The MGCF must then interface with a gateway function for interconnection with other domains.

The Breakout Gateway Control Function (BGCF) provides this functionality and interfaces with other BGCFs in other network domains. The MGCF then provides the call control within its own network; it may be implemented regionally or within the core network. Actual implementation of the MGCF function depends largely on the network topology and size.

For very large networks, it is more efficient to distribute the MGCF within regions, providing better control from a geographic perspective over growth and traffic grooming. This could be thought of as analogous with the tandem function within the circuit-switched domain, but it is just as analogous as the bridging function within LAN/WAN networks, although the traffic mixes will be significantly different.

Packet data networks often engineer bridges using the 80/20 rule. They are configured in such a manner that the bridge routes 20 percent of the traffic off-net, and 80 percent on-net. Tandems, on the other hand, are specifically designed for interconnection of different networks and network service areas.

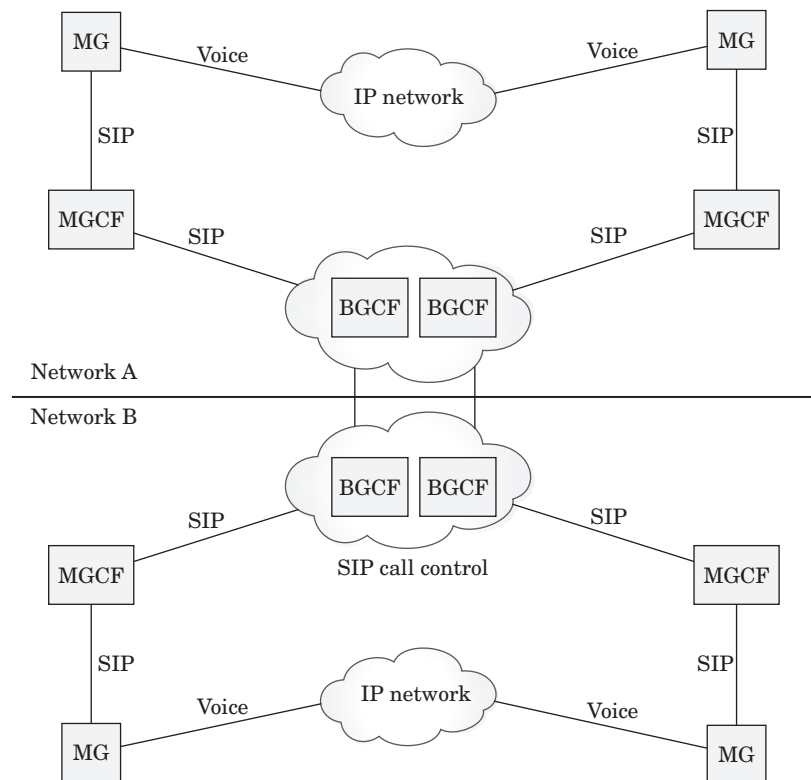
The MGCF can be engineered in such a way as to route traffic between media gateways within its own control, and a smaller percentage of traffic routing to other media gateways outside of its control. They can also be implemented as more of a central function providing a sort of tandem function within a network.



Either way, their function within the IMS is to manage the packetized voice that is routed into the IMS domain, and to pass the control of these calls through the MGCF up to the Call Session Control Function (CSCF). They are needed only when interconnecting with the Public Switched Telephone Network (PSTN).

**The Breakout Gateway Control Function (BGCF)** We have talked about the BGCF some already. The BGCF sits at the border of the network and controls interconnections between two networks. This means that the BGCF must provide some security capabilities to prevent unauthorized access into the network.

As shown in Figure 2.3, the BGCF interfaces with the various MGCF entities within its own domain and then provides the connection to another network connecting into the BGCF of that network. This allows operators to screen some aspects of the session information from competitors. For example, the operator may wish to “hide” the addresses of other nodes within its network. This would prevent the other networks from identifying the network topology.



**Figure 2.3** The Breakout Gateway Control Function (BGCF)

## 48 Chapter 2

The BGCF can also provide encryption for all outbound traffic. This is typically achieved through the use of IPsec, where the message is encrypted and then placed inside another packet for routing. The message is then sent from one network to the destination network, encrypted and embedded within a normal signaling message. Also referred to as tunneling, this prevents intermediary networks from discovering many aspects of the network as well as the sessions themselves.

There is one caveat to tunneling: if you are monitoring traffic end-to-end within the network, unless there is some means of capturing the cipher keys, you will be unable to decrypt the message and monitor the traffic effectively.

In the IMS domain, it should be noted that the S-CSCF connects directly with the BGCF for outbound signaling. If the S-CSCF has determined that a SIP message is to be routed to another network, then the S-CSCF routes the SIP message directly to the BGCF.

If the message is to be routed internally (within the same domain as the S-CSCF), then the S-CSCF routes the message to the MGCF. This may be done directly or through another CSCF, depending on the operators' deployment and implementation.

### Packet-Switched Domains (PS)

One would think that within the packet domain, there is no need for gateways or other entities to route into the IMS. However, the packet domain is not necessarily IMS compatible. In today's networks, operators have been evolving the network from circuit-switched to packet-switched, which means you have hybrid networks.

A good example of this is the GSM network. GSM started as an IN/SS7 architecture model, using the SS7 protocol to communicate to internal databases that manage subscriber location and registration within the network. The switches themselves use circuit switching when routing calls between networks, but in many cases X.25 packet switching was implemented for calls within a base station subsystem, and back to the switch itself.

As GSM matured, it began evolving certain aspects to packet-switched using IP. This is indeed how IMS came about in the first place, as part of this evolution. But there are still legacy components that must be supported, until such a time when handsets are equipped as SIP User Agents (UAs) and can communicate directly with the IMS infrastructure without interfacing with any other entities.

The packet-switched domain can be wireline focused or wireless focused, so this section is broken into two parts to discuss both Voice over IP (VoIP) and wireless implementations.

### VoIP Domain

We have talked quite a bit about the VoIP domain already in the sense that calls from the circuit-switched domain must then be routed through the VoIP domain to packetize the voice, and to convert the signaling from SS7 to SIP. This being the case, we have already identified several of the functions within this domain, but we will cover them again here from a different perspective.

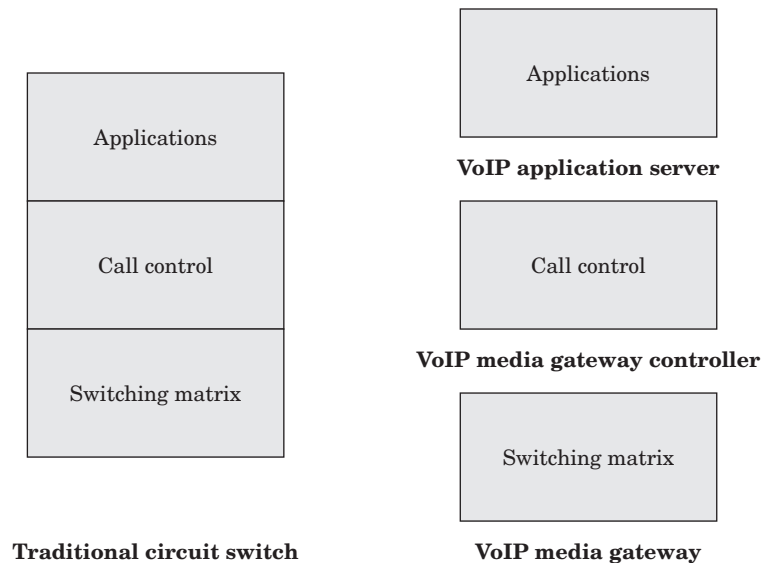
The VoIP domain consists of entities that provide the functions commonly found in a telephone switch, with one major difference: the functions are distributed. When the concept of VoIP first began, the idea was to separate the function within a switch and provide these functions in a more economical fashion. As shown in Figure 2.4, the switch can be broken into three major functions:

- Switching fabric (or matrix in legacy terms)
- Signaling
- Applications

The switching fabric is the cheapest part of the switch. This is where circuits are connected to other circuits within the switch, for connecting of a call. Think of the telephone operators of days far gone and how they used their answering positions to connect calls with other parties. The switching fabric does this same function under the control of a processor (in other words, we automated the operator function).

Detach this function from the processor, and you have a relatively inexpensive device that can be placed throughout the network. For example, an operator providing service to a remote rural area cannot afford to deploy a full-blown circuit switch into this market, but it can deploy an inexpensive media gateway in the market and place the controller someplace more central, supporting media gateways in many different rural areas.

So now you have the switching matrix being provided by the media gateway. The media gateway does not have any processing power, and therefore it must rely on a



**Figure 2.4** Splitting the switch functions

controller to tell it how connections are to be made, and to control those connections. The media gateways do not have any signaling between themselves per se; they communicate with their controller. A number of protocols are used between the media gateway and the controllers. This is another issue with many VoIP implementations, because it is difficult to interwork many different brands of devices if they do not support the right protocols.

The controller is a more central function. The media gateway controller can sit within the core network, or it can be placed within a specific geographical location and provide call control for many different media gateways. The media gateway controller function (MGCF) is the brains of the VoIP network. The MGCF is also where the signaling portion of the switch is placed. It is the MGCF that communicates with other MGCFs within its own network, providing call control between these various entities.

Since the processing for a call is not distributed in key areas, this function can be used to support multiple communities of interest, rather than deploying one per town that can only be used to support that one town. This is the direction of VoIP deployments and the major attraction from an operator's perspective. It does not come without issues, however.

The multitude of signaling protocols is one of the largest issues and has caused implementation nightmares for many operators. This was especially true for wireless operators trying to support applications. Since wireless is heavily dependent on databases (the Visited Location Register and the Home Location Register, for example), it becomes paramount that every entity within the network be able to communicate with the Mobile Switching Center (MSC) to access these resources.

The applications and features in the VoIP model are also separated from the switching function and deployed on application servers. This presents many cost savings and allows operators to implement just about any type of service they want to offer, as long as their MGCFs can communicate and support it.

A voice application server, for example, may provide mobility services, conferencing services, or even messaging. Operators such as Skype and Vonage are heavily dependent on these application servers because this is where mobility is supported. Mobility, by the way, is the concept of receiving calls no matter where you are located. The network always knows your IP address and always knows how to route calls to your device (as well as what device to route calls to).

In essence, the VoIP model is almost IMS ready, except that many different protocols are used to support all of the communications between all of the network entities, and very few security and authentication controls are provided by the network. Almost all of the security and authentication controls are functions of the MGCF and require implementation by the operator.

However, the concept of inserting a module within the subscriber device for the exchange of authentication credentials is largely a wireless concept. VoIP implementations may have some security, but there is no means of authenticating the subscriber device today.

Certainly an operator can provide packetized services today, with all of the features and capabilities that can be provided within the IMS, and indeed many are doing

this now. However, they are lacking in the control and security area, which is why IMS has become so important to so many large operators.

The VoIP domain, then, still must have a connection into the IMS, which is through the BGCF/MGCF. If the operator owns both a VoIP network and an IMS network, then it can pass calls/sessions between the two domains using the MGCF. However, if the VoIP provider is not the same as the IMS provider, then the BGCF is used as an interconnect part. As you will learn in later chapters, there are specific functions provided by the BGCF that differentiate it from the MGCF.

Once the signaling reaches the BGCF, it must be routed to the P-CSCF within the area (or whatever means the operator chooses for P-CSCF assignment). Remember that all sessions must be routed through the P-CSCF first, which then routes to the I-CSCF, which is then responsible for routing to the S-CSCF.

VoIP only supports voice and data, and therefore there must be other interfaces to support other media types, for example, the delivery of messaging in a wireless network and the support for video over IP (IPTV). These require other network elements and a separate means for delivery. This is because, even though the network itself cannot support the media types, the network elements are designed for voice only.

Support of these media types involves overlay networks, such as GPRS in the GSM network. GPRS is explained in the next section, but it provides an overlay network supporting various data services such as Internet access, video and audio support, and other packetized services.

### General Packet Radio Service (GPRS)

The GPRS network works as an overlay to the existing GSM network. All packet data received from a GSM handset is routed from the base station controller (BSC) to the Serving GPRS Support Node (SGSN). The SGSN is a packet data node supporting multiple media types in a packet network.

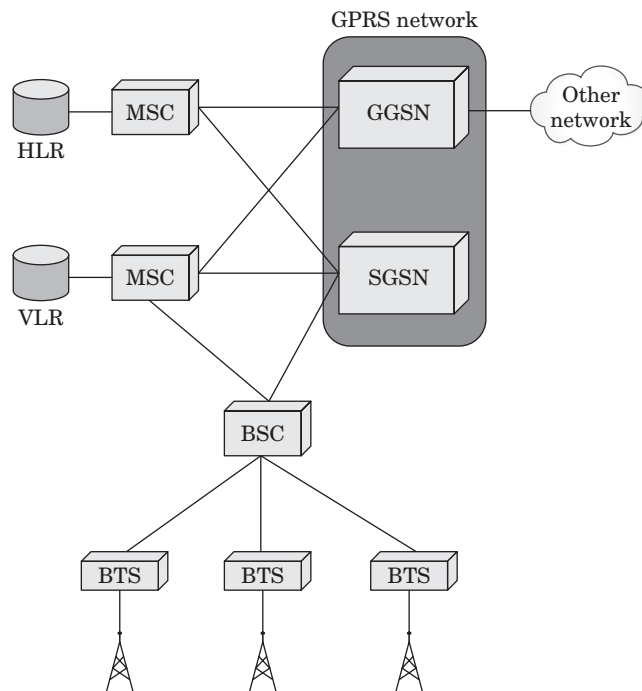
As shown in Figure 2.5, the SGSN provides connectivity to other SGSNs within the same network, acting as the packet data network for the wireless operator. None of this traffic is routed through the Mobile Switching Center (MSC), since this switch is designed to support voice.

To interface to external packet networks, the Gateway GPRS Support Node (GGSN) is used. The GGSN provides connectivity to other packet networks, including other wireless carriers' GPRS networks. This overlay network then provides complete packet data support within a wireless environment within the core network, but this does not extend to the air interface. Other technologies exist to provide support of packetized broadband services at the air interface.

The GPRS network provides and manages connections to packet networks. This means that GPRS must provide some fashion of session control for each of the connections within its domain. When connecting to the SGSN, a Packet Data Protocol (PDP) *context* is created. Think of the PDP context as the connection into the packet network, each connection being identified by its own unique PDP context.

When connecting from a wireless device to an application server in the IMS domain, the SGSN/GGSN creates a PDP context for the session and then manages this connection

## 52 Chapter 2



**Figure 2.5** GPRS network architecture

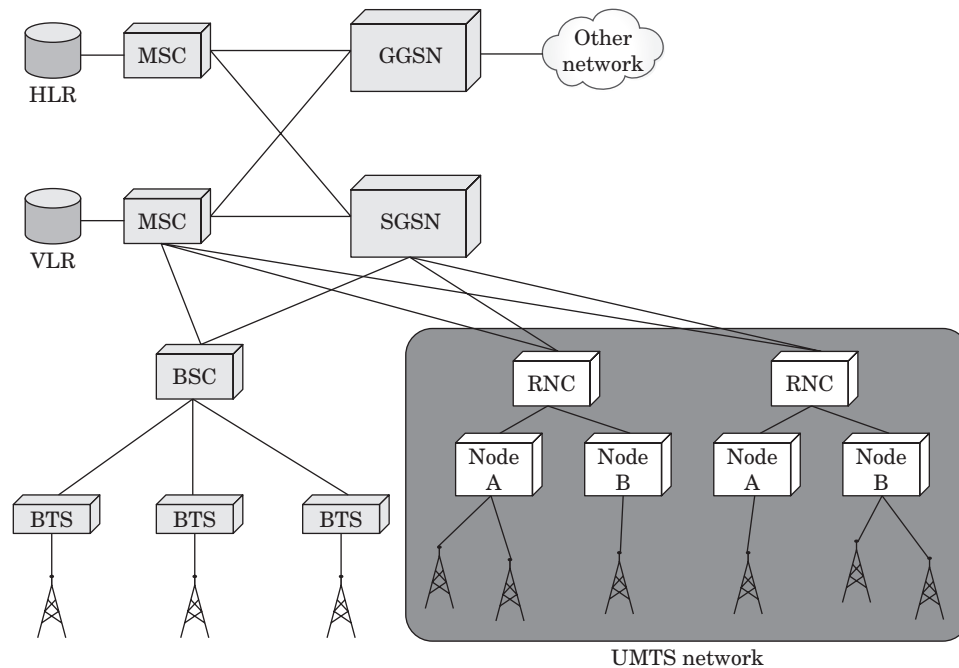
on the GPRS side. The GGSN then interfaces with the P-CSCF, which provides the session control within the IMS domain. When connecting to servers and applications, the GPRS network uses the Access Point Name (APN) for the device to identify which services it is accessing (based on the server name being connected to).

### UMTS and CDMA Domains

The Universal Mobile Telecommunications Service (UMTS) provides broadband packet services enabling wireless subscribers to use Internet services and other multimedia-type services such as video and multimedia messaging. With a bandwidth of 2 MBps, UMTS provides the bandwidth required to support some of these services that require more bandwidth, such as video (IPTV). Voice is also supported through this interface but is routed from the UMTS nodes to the MSC (the circuit-switched portion of the network).

As you can see in Figure 2.6, accessing the IMS through a UMTS interface (or any other access technology for that matter) within a GSM network still involves routing the packet data through the GPRS SGSN/GGSN nodes. The Radio Network Controller (RNC) in the UMTS portion of the network interfaces with the SGSN within the same network, which in turn interfaces with the GGSN.





**Figure 2.6** UMTS network

It is the GGSN that then provides the connectivity back into the IMS P-CSCF. The P-CSCF is always the first point of access in the IMS, regardless of the access method. Voice traffic does not necessarily go through this same route, because (as you'll recall) the voice must go through media gateway, under the control of the MGCF. SIP signaling is the only data that is routed through the CSCF functions of the IMS.

This is the same then as in wireline VoIP, where the voice is sent to a media gateway (MG) for converting to packet, and the signaling is sent to the MGCF for conversion to SIP. Once the signaling has been converted to SIP, the MGCF is then able to communicate directly with the IMS P-CSCF.

CDMA is a little different in that the architecture does not include the SGSN/GGSN (see Figure 2.7). However, there is an equivalent function: the Packet Control Function (PCF) interfacing with the Base Station Controller (BSC), which is responsible for the routing of packet data to the packet network within CDMA.

The Packet Data Service Node (PDSN) then provides connectivity to packet services such as the Internet, or other packet networks. The PDSN therefore serves the same role as the GGSN, acting as the gateway into other networks. The PDSN interfaces with the media gateway within the IMS domain if there is voice; otherwise, for packet data the interface is to packet entities within the packet domain. The session is controlled by SIP, so the SIP signaling is routed to the P-CSCF within the IMS.

## 54 Chapter 2

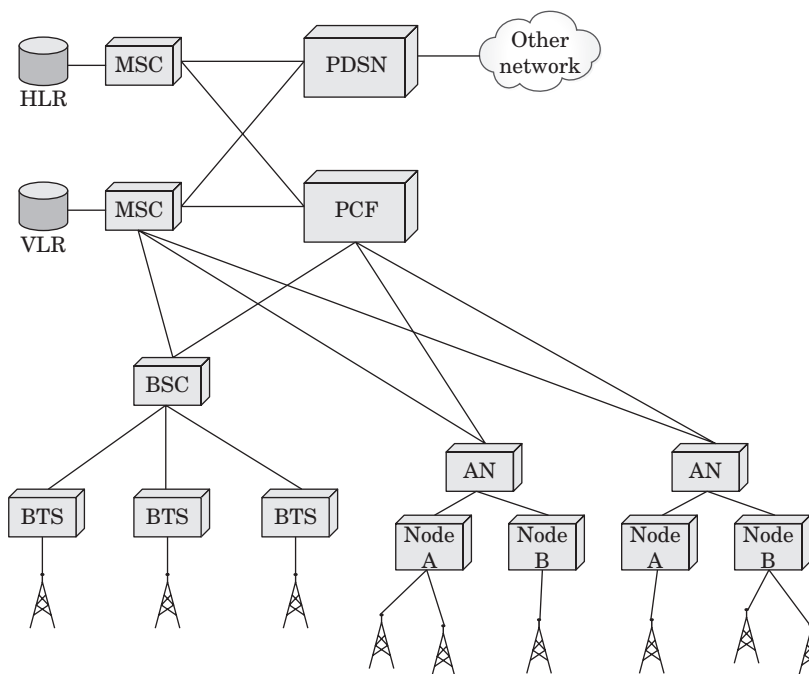


Figure 2.7 The CDMA network and packet domain

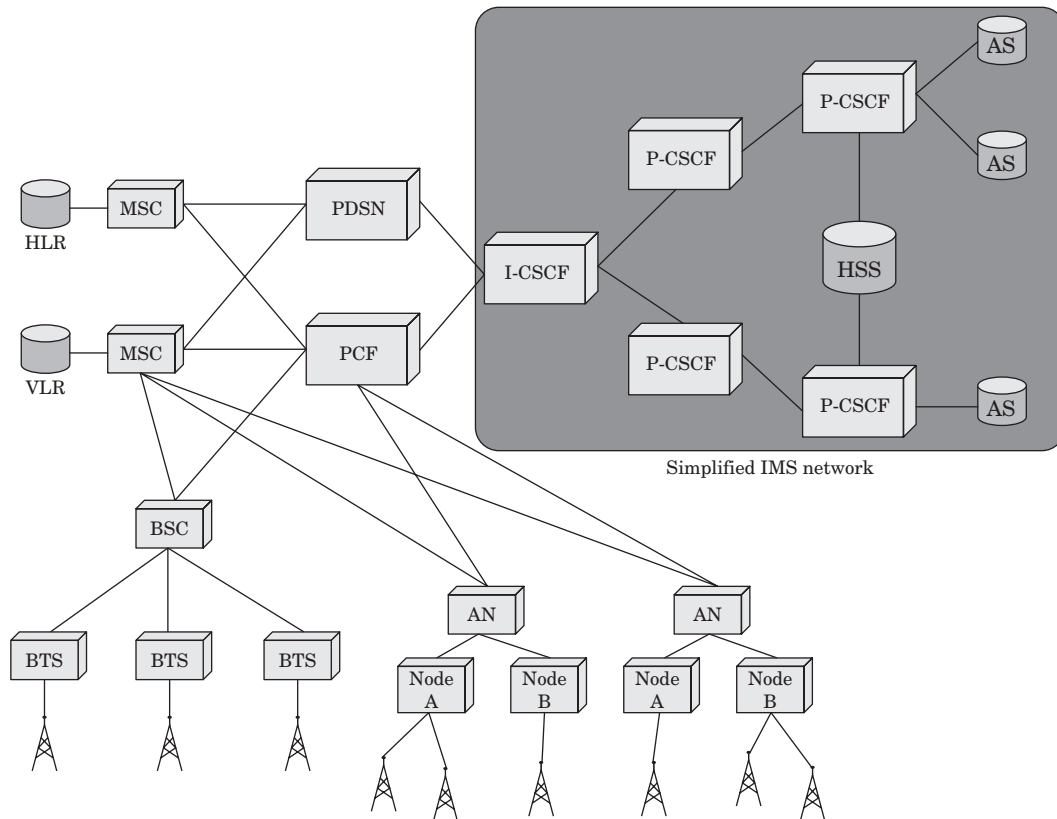
### From IMS to IMS

In a perfect IMS universe, there is no need for access networks to support anything other than IP and SIP. Of course, we are not in a perfect IMS world (at least not yet), and there is a significant amount of network still in service that is not packet. For this reason, we will not realize the full benefits of a total SIP network for a long time.

When I say total SIP network, I am referring to a network where all of the devices are equipped with SIP user agents and are capable of supporting IMS SIP. This would allow the devices to interface with the CSCF within the IMS domain directly without any conversions or signaling gateways (see Figure 2.8). MGCFs would not be required since the devices are already SIP capable.

These same devices would be able to transmit everything in packet mode, eliminating the need for media gateways and other support devices in the network. Regardless of the media type, all transmissions would be packet data, and signaling would be SIP. This is the future direction of IMS.

This is not as far off as some might think. It is possible we may see implementations of SIP-enabled handsets in the very near future, which will only serve as a major incentive for operators to move rapidly to an all-IMS environment. With support for packet data and SIP network-wide, many elements and systems can be completely eliminated from the network.



**Figure 2.8** The pure IMS network

Of course, this is still talking about an ideal world. There are many back office support systems that will have to transition, because it is simply not possible to cut the cord overnight and toss these systems out of the window. The entire business of the operator is based on many of these support systems, so throwing them away is out of the question.

Likewise development is still lacking for many of these systems that support IMS. For example, the entire area of billing is still being defined and refined. Operational support systems (OSSs) are moving in this direction quickly, yet they have a different view today than what operators may need going forward as their business models change. This is yet another reason why we may not see full SIP-to-SIP, IMS-to-IMS interoperability without gateways and other devices to interface to legacy platforms and systems we have already discussed.

This is truly an evolutionary approach to IMS implementation, and for any operator who already has a legacy network in place, it is the only approach that makes any business sense. The long-term goal is to support SIP-enabled devices in a pure IMS environment, but the road to get there will be long and require transitional approaches.

