White Paper

Critical Steps for Successful VoIP Deployment

VoIP-WP101-R

This white paper will help you identify the top 10 most critical steps for successfully deploying IP-based telephony systems within your enterprise.

April 12, 2005

Introduction

Digital communications using Pulse Code Modulation (PCM) and Time Division Multiplexing (TDM) circuit switching first made their mark during the mid-1970s and quickly became the dominant technologies in enterprise communications systems.

Over the past few years, a different type of digital communications platform, one based on Internet Protocol (IP) standards and using a Local Area Network (LAN) or Wide Area Network (WAN) infrastructure for switching and transmission of voice and data signals, has been evolving. This Voice over Internet Protocol, or VoIP, is poised to become the next dominant technology for enterprise communications.

VoIP is a way to carry voice calls over an IP network by digitizing and packetizing voice transmission streams between two endpoints. The most basic VoIP implementation is a simple voice call between two PC clients that have the necessary hardware and software. A newer implementation, IP telephony, uses VoIP standards to create a telephony system that can have higher level features such as advanced call routing, networking, voice mail, contact centers, etc. It is this ability to integrate voice, data, and video applications using a single network infrastructure that makes deploying an IP telephony platform an essential step toward creating a next-generation network.

Ethernet switch and router networks originally deployed in the 1990s were designed for data communications only and therefore were not ideal for handling real-time voice communications, where small changes in network characteristics can affect call quality. As a result, early adopters of VoIP faced new challenges when moving from traditional voice networks to IP networks. Issues such as transmission delay (including delays for encoding, decoding, and packetizing voice samples), network jitter, packet loss, and echo were found to seriously affect the Quality of Service (QoS) demands of real-time voice communications. In addition, there are a number of security issues that have been identified that must be taken into consideration when implementing an IP telephony system.

IP telephones currently account for more than one-third of total Private Branch Exchange, or PBX, station shipments in North America, and the consensus among forecasters is that IP stations will eclipse traditional-instrument shipments within the next year.

VoIP and IP Telephony

As described above, VoIP is the process of digitizing voice signals using any one of a variety of encoding techniques, including those specified by the International Telecommunications Union (ITU) or solutions such as the Broadcom Corporation® BroadVoice™ vocoder, and then converting them to IP format. The IP is a networklayer (Layer 3) protocol with appropriate addressing and header control information that enables packets to be routed. Early implementations of VoIP technology have quickly evolved from simple station-to-station voice calls into today's full-function IP-PBX systems, today's most commonly implemented IP telephony system. IPPBX systems use a LAN/WAN to support control signaling and voice transmission between individual endpoints such as IP telephone instruments, PC client softphones, and 802.11 wireless handsets, etc., and also among distributed common equipment hardware used to support traditional circuit switched telephones and trunk connections.

An enterprise with an installed circuit-switched PBX telecommunications system has several options for migrating to an IP telephony system. Many businesses have installed systems that can easily be upgraded to an IP-enabled system design by adding media gateway circuit boards to link IP endpoints (station equipment and trunk circuit interfaces) with the PBX's internal circuit-switched network. Media gateways are also used to support converged system designs that distribute traditional circuit-switched port cabinets across a LAN/WAN for campus or multiple premises communications. Circuit-switched PBXs that are upgraded and/or enhanced to support VoIP capabilities are usually referred to as converged IP-PBX systems.

An IP-PBX system without an integrated circuit-switched network is referred to as a client/server design. This pure packet-switched IP telephony system consists primarily of a call telephony server and distributed IP endpoints, using the LAN/WAN for all control signaling and voice transmission processes and media gateway equipment to support traditional analog station equipment and Public Switched Telephone Network (PSTN) trunk interfaces.

Deployment of an IP telephony system based on a mixed circuit/packet or pure packet-switched design is likely to require upgrades and enhancements to your existing LAN/WAN to achieve the voice communication quality level that users have grown accustomed to. Key network design guideline requirements and issues are addressed below under the heading "Considerations."

Benefits of an IP Telephony System

The primary benefits of deploying an IP telephony system are:

- cost savings and cost reduction;
- system design and performance enhancements; and
- ability to provide enhanced telecommunication features, functions, and applications.

Businesses can achieve financial benefits from an IP telephony system through any of the following: reduced upfront capital expenditures for installed system hardware/software; ongoing cost savings through simplified maintenance/operation activities; reduced transmission services; or increased productivity of workforce.

For example, systems based on a call telephony server design have reduced common equipment hardware requirements because fewer port circuit cards housed in port carriers are required. At the same time, systems based on a call telephony server are likely to be less expensive than those requiring traditional proprietary common-control cabinets.

Another cost-saving design benefit is that media gateway boards can be programmed to support a greater number of physical IP stations than traditional port-circuit interfaces. Using existing cabling and switch infrastructure originally deployed for data only may also reduce upfront installation and implementation costs.

A major benefit of current-generation IP telephones that have integrated multiple Ethernet switch ports is that they allow existing desktop PCs to be connected to the voice instrument for access to the LAN, without the need for additional closet switch capacity. This saves costs in that separate wiring for voice and data transmissions is not required.

Ongoing expenses in operations, administration, and maintenance personnel can be reduced if management of both voice and data communications are combined within the same organization. System upgrades are usually easier and less costly with newer system designs because of the plug-and-play nature of IP station equipment. Off-premises telecommunications carrier services can be shared for both voice and data communications, minimizing dedicated voice-only private lines between enterprise locations.

Finally, fewer transmission resources are required if voice codecs using compression are deployed for off-premises calls. Deploying an IP telephony system can significantly improve your system design structure and configuration, particularly for the vital design issues of redundancy and survivability. Multiple active call telephony servers and control/transmission signaling paths can be used in an IP-PBX system configuration. Pooling of media gateway resources minimizes single points of failure while optimizing available media-channel connections.

IP endpoints, unlike TDM endpoints, are not physically linked to a single dedicated interface, but can use any accessible call telephony server or media gateway for call processing, transmission, and switching requirements. Organizations with multiple locations also benefit from an IP telephony design because a centralized call telephony server can use existing WAN or Virtual Private Network (VPN) services to support remote stand-alone IP station equipment and/or traditional common equipment hardware.

There are a variety of new features and applications that are enabled or enhanced by an IP telephony system design, including integrated voice/text messaging; unified communications (presence, collaboration, and instant messaging); and 802.11 mobile communication (wireless VoIP). An IP telephony system can also support increased user productivity through advanced desktop telephones with large-pixel display fields and integrated thin client browser-like functionality that supports access to information and data residing in databases internal and external to the core voice communication system.

Considerations

There are a number of LAN/WAN design and engineering guidelines that must be followed to successfully support voice communication on a packet-switched network originally designed for data communication. The demands of real-time voice traffic and applications require a variety of QoS techniques to manage transmission bandwidth according to different application demands and network management settings, to optimize audio and tone service levels.

LAN/WAN QoS levels fluctuate over time due to unanticipated changes in usage patterns and traffic flow. This is normally not an issue in a data-only network; however, if QoS is degraded for short time periods it may significantly affect IP telephony services noticeable by all system users, even if data communication services appear satisfactory. Several basic control methods can be employed to manage QoS levels to ensure the higher grade of service level required by real-time voice communication. These methods include:

- Reserving fixed bandwidth for mission-critical voice communication applications;
- Restrictions on network access and usage for defined users or user groups;
- Traffic priority assignments;
- Utilization of VLANs (Virtual LANs) to virtually separate voice and data; and designation of which kinds of traffic can be dropped when congestion occurs.

The most common-sense approach to minimize potential QoS problems owing to traffic congestion and its resulting issues such as packet delay and jitter is to increase available transmission bandwidth and switching capacity between IP endpoints. The first IP telephony systems were implemented over LANs that included hubs and shared port connections on 10 Mbps Ethernet switches. This resulted in significant QoS problems.

To avoid these problems, and to future-proof your network, each IP telephone should be installed using a dedicated 10/100 BaseT connection on the local wiring closet switch. Embedded QoS capabilities in the IP telephone, such as 802.1p/Q and jitter buffers, allow station users with integrated voice/data desktops, such as PC clients connected to the LAN through the voice instrument's integrated Ethernet switch ports, to use a single switch port in the local wiring closet switch without fear of degrading their voice communication service.

Deploying 1 Gbps Ethernet switch backbone networks is also recommended to reduce traffic congestion problems. Next-generation networks will commonly deploy 10/100/1000 BaseT connections at the desktop/wiring closet layer, and 10 Gbps networks on the backbone. You should expect to see IP telephones with 1Gbps Ethernet switch port connectors available in the near future to take advantage of the higher-transmission-rate networks, further minimizing QoS concerns to the desktop. The declining cost and increased performance levels of integrated circuit (IC) technology make it possible to deploy affordable higher-speed Ethernet switches and network interfaces. In the future, advances in the core switching technology at the telephone chip set and board level will someday make bandwidth congestion a non-issue.

For organizations that do not have unlimited transmission bandwidth and switching resources, there are several QoS mechanisms commonly used to support today's IP telephony systems. The two common QoS solutions are Class of Service (CoS) IEEE 802.1p/Q tagging (Layer 2) and Type of Service (ToS) prioritization (Layer 3).

An enhanced version of ToS is known as Differentiated Services (DiffServ). CoS and ToS functionality must be embedded in Ethernet LAN switches (stand-alone and embedded in IP telephones) and media gateways (stand-alone devices, port circuit boards, and embedded chip sets in IP telephones) to give priority to switching and transmission of voice communication packets to minimize transport delay across the network between endpoints.

Another common approach to IP telephony is the use of Virtual LANs (VLANs). VLANs can be used to provide more efficient use of LAN bandwidth, are used to distribute traffic loads, and are scalable to support high performance requirements at a microsegment level. Traffic types such as real-time voice and delay-insensitive data can be segmented. IEEE 802.1Q is used as a VLAN packet tagging standard.

Two major problem areas that affect IP telephony QoS are packet loss and delay. These two impairment factors are sometimes interrelated. Packet loss causes voice clipping and skips, often resulting in choppy and sometimes unintelligible speech.

Voice packets can be dropped if the network quality is poor, if the network is congested or if there is too much variable delay in the network. Even the best engineered networks may not stop congestion-induced packet loss and delay, making it necessary to integrate jitter buffers in IP telephones and media gateways.

Dynamic receiver buffers that can be programmed to increase or decrease in size can be used to handle late-arriving packets during periods of traffic congestion. Signal processing elements in most current IP telephone voice processors can correct for up to 30 milliseconds (ms) of lost voice.

Several techniques are available for replacing a lost packet or a packet that is delayed beyond the jitter buffer threshold. One method is to estimate the information that would have been in the packet. This concealment method generates synthetic speech to cover missing data. Another technique is to regenerate or duplicate the last packet in the transmission sequence and substitute it for the missing packet.

Echo – reflected signals of the speaker's voice that are heard in the speaker's ear – is another problem that can affect voice communication quality. In a circuit – switched telephone network it is caused by signal reflections generated by the hybrid circuit that converts signals between a 4-wire circuit (a separate transmit and receive pair) and a 2-wire circuit (a single transmit and receive pair). It is usually acceptable in the PSTN, because the round-trip delays through the network are smaller than 50 milliseconds, and the echo is masked by the normal side tone every telephone generates (though it is more commonly experienced in this environment in conference calls). In an IP telephony network echo becomes a problem because the round-trip delay across a LAN/WAN is highly likely to be greater than 50 milliseconds. To solve this problem, echo cancellers must be embedded in the IP telephone design.

In IP telephones, there are two types of echo cancellation that must be considered: line echo cancellation in the handset and acoustical echo cancellation on the speakerphone. Echo on the handset is something that is not noticeable with traditional TDM phones due to their low delay characteristics. Due to the slight delay introduced by IP networks, even a small echo on the handset is noticeable.

Thus an IP phone system must also include a short-tail handset/headset echo suppressor.

Hands-free speakerphone is affected by an acoustic echo that can be a function of the IP telephone design itself. Quality and placement of the speaker, the microphone within the phone enclosure, and the enclosure design itself affect the voice quality, the full-duplexness of the speakerphone, and echo in the system. An acoustic echo canceller (as opposed to a line echo canceller) capable of canceling 60 ms to 90 ms of echo is required.

Security Issues

IP telephony systems and networks are vulnerable to the following security breaches:

- access control;
- data control;
- disruption; and
- eavesdropping

All servers, media gateways, gatekeepers, and IP voice terminals are susceptible to attack. There are a variety of IP telephony system security issues to be aware of. Security threats and resolutions include:

- packet sniffing/call interception, resolved by using a switched LAN infrastructure to limit sniffing problems;
- virus and Trojan-horse applications, resolved by using host-based virus scanning software;
- unauthorized access, resolved by using host-based intrusion detection systems and application access control;
- application layer attacks, resolved by updating computer system software with the latest security fixes;
- caller identity spoofing, resolved by using software utilities that notify system administrators of unknown devices attached to network;
- toll fraud, resolved by using a system gatekeeper that denies network access to unknown phones attempting to log in;
- denial of service, resolved by segregating voice and data transport segments to reduce the likelihood of an attack;

- repudiation, resolved by authenticating users before they access a telephony device, thus reducing the likelihood of a later denial that a call ever occurred; and
- trust exploitation, resolved by using a restrictive trust model and private VLANs to limit trust-based attacks.

In addition to the techniques outlined above, it is strongly recommended that you have media encryption integrated into the IP telephones and media gateways to prevent sniffing/eavesdropping of voice and signaling packets. Several encryption algorithms that are commonly used in these devices include:

- DES (Data Encryption Standard);
- 3DES (3xData Encryption Standard);
- AES (Advanced Encryption Standard);
- RC4; and
- RC5 (“Streaming” encryption)

Wherever possible, endpoints with hardware acceleration for these functions are recommended over software implementations.

Another important aspect of security is the management of clients on the network. Broadcom Corporation, one of the industry leaders of stand-alone security encryption and authentication silicon for enterprise networks, has developed and patented a security-based client management system called BroadSAFE™. This breakthrough technology enables IT managers to manage client devices within their enterprise more securely and cost-effectively and also protects against network attacks.

BroadSAFE technology consists of three elements: (1) a key management server that resides at the head-end; (2) key management software that directs and manages many clients; and (3) a low-cost silicon-based security module that is resident in the client devices themselves to protect key material from being exposed. BroadSAFE is an extremely cost-effective certificate and key management solution that can be extended to other client devices within the network such as IP telephones, network interface cards (NICs), cable modems, and wireless devices. See Figure 1 below.

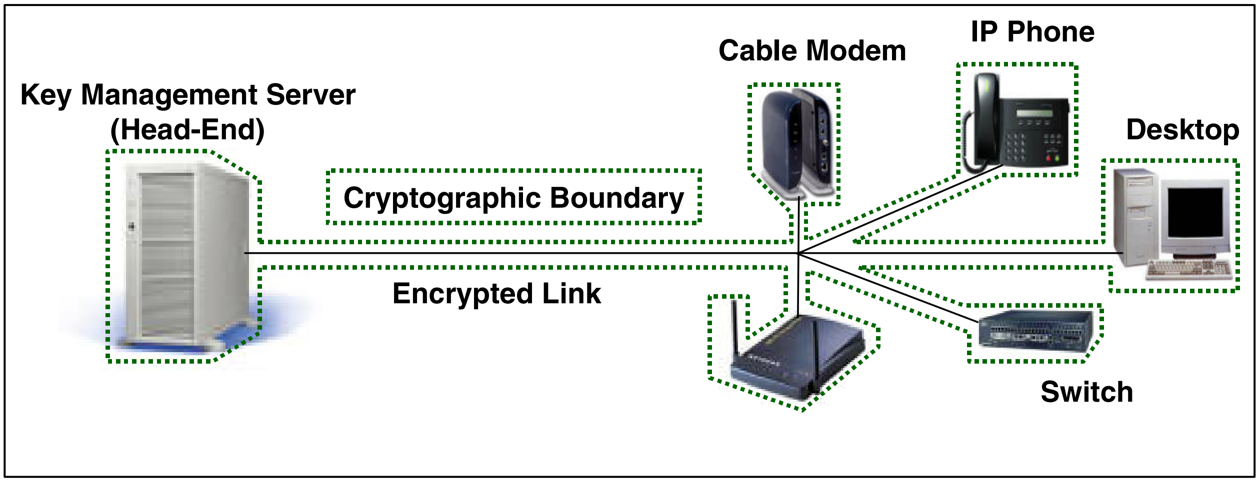

Figure 1

The BroadSAFE system manages clients such as cable modem, IP telephone, desktop computers, network switches, and wireless access points.

With BroadSAFE-enabled client silicon, you can get a factory-installed identity that is stored securely within your device. Once a product has an identity, a security system can be built around it through a management server with a hardware security module (HSM) installed in it. Since the device has an identity stored in hardware, the device itself can now be managed remotely.

IP Voice Terminals

There are several IP voice terminal options, including desktop instruments, PC client softphones, and mobile 802.11 handsets or PDAs. Most IP telephone desktop instruments closely copy the look and operation of traditional digital models; however, the internal design elements and functional capabilities are very different.

Technical design and functional attributes common to IP telephones are:

- Voice codecs
- Integrated Ethernet switches
- QoS
- Jitter buffers
- Voice Activation Detection (VAD)
- Echo cancellers
- Infrared/Bluetooth connectivity
- Thin client browser
- Security

IP telephones have integrated voice codecs that convert analog voice signals into digital-packet format. A variety of vocoder algorithms can be programmed into the instrument design, including ITU-T standards such as G.711, G.723.1, G.729A, and G.722, and solutions such as the Broadcom BroadVoice codec. The BroadVoice codec supports wideband high-fidelity voice that provides a 16 KHz or 32 KHz sampled output instead of the traditional 8 Khz sampled output associated with traditional Pulse Code Modulation (PCM), also known as G.711. BroadVoice provides some additional benefits, including reduced transmission bandwidth requirements (about one quarter that of the ITU G.722 wideband codec specification), reduced transmission delay (due to a faster compression process), and no Intellectual Property Right (IPR) costs.

Wideband vocoding is likely to become the preferred choice for station users in the near future because of superior sound quality for basic voice conversations, but particularly for audio streaming applications that include wideband frequency signals, such as music.

Except for entry-level models, IP telephones are commonly equipped with integrated multi-port Ethernet switches. One RJ-45 connector port is used for interfacing to the LAN; a second port can be used to support a station user's personal computer to avoid using an individual RJ-45 wall jack connector for the network connection and switch port in the local wiring closet Ethernet switch. QoS software, such as 802.1p/Q, must be supported by the embedded switching element to prioritize traffic at the integrated voice/data desktop work area to avoid additional transport delays and congestion. Jitter buffers are also included in the technical design to minimize quality problems due to delayed or lost voice packets.

To optimize available network bandwidth and reduce traffic congestion, IP telephone designers use embedded voice activation detection (VAD) software. VAD software, often referred to as silence suppression, is used to detect the absence of audio and conserve bandwidth by preventing the transmission of "silent packets" over the network (believe it or not, about half of all talk time is characterized by silence). VAD software monitors signals for voice activity so that when silence is detected for a specified amount of time, the application informs the voice communication protocol software and prevents the voice codec output from being transported across the network.

As discussed earlier, echo cancellation techniques can be used to improve voice quality. IP telephones are equipped with both handset/headset echo suppression software and acoustic echo cancellation software to converge and suppress echoes caused by signal reflections, which impair the quality of a voice conversation.

All of the above IP telephone design elements and functions can be embedded in a single advanced IC chip, such as those found in the Broadcom BCM1101 family of VoIP processors. The BCM1101 is a highly integrated, single-chip IP phone solution that integrates:

- 150 MHz RISC processor and 108 MHz Digital Signal Processor (DSP): Supports VoIP protocol stacks, operating system, enhanced IP phone application software, as well as core telephony algorithms including jitter buffer management, packet loss concealment, acoustic echo cancellation for full-duplex speakerphone, a wide range of vocoders, and a variety of telephony algorithms (e.g., DTMF and Call Progress Tones).
- Analog codecs: Three analog codecs capable of supporting both narrowband 8 KHz and wideband 16 KHz sampling, which, in conjunction with wideband voice coders such as the Broadcom BroadVoice32 vocoder, will enable IP phone networks to deliver high-fidelity voice transmission.
- Three-port 10/100 Ethernet switch: Integrates three full-duplex-capable Media Access Controllers (MACs), a serial management port, an address resolution engine, a non-blocking switch controller, 64 KB of internal switch memory, 802.1p prioritization for voice packets, 802.1Q VLAN tagging support for segmenting physical networks into multiple logical networks, and a set of management information base (MIB) statistic registers.
- Two 10/100 BaseT Ethernet Transceivers: The transceivers integrate support for in-line powering over Ethernet and support auto-MDI/MDIX detection to allow for the use of any cable type in either port.

Wireless connectivity to other devices can be supported using infrared (IR) or Bluetooth technology. At the desktop, wireless links can be used for a headset, PDA (directory synchronization, speed dialing), printer, or keyboard/mouse (directory access, data input, menu selection). Potential vertical-market wireless link applications may include medical monitoring equipment and retail barcode scanners.

One of the major advances in recent IP telephone design is the integration of thin client browser-like functionality that can be deployed for a variety of station user applications, including external server database access and display downloads such as directories, schedules, inventory lists, and customized Web pages; menu screen downloads and data input; visual message listings (voice, text, fax,); audio streaming; and visual alerts. Several IP telephone models use touch screen technology for menu selection and data input. IP telephone browser functions are typically supported using either XML or HTML. Today's most advanced models may also include an embedded Windows .CE O/S and Java Virtual Machine (JVM) code for more sophisticated integrated applications capabilities.

Current and planned IP telephones will include hardware security functions, including AES media encryption to prevent voice and signal sniffing and eavesdropping, and Denial of Service (DOS) software, which will be necessary to maintain acceptable QoS levels if telephones become targets of attacks from outside the network. In addition, one-time-programmable identification cells, such as those provided by the Broadcom BroadSAFE security system, will make device identification and configuration more advanced and easier to manage.

Another category of IP voice terminals is mobile IP telephony devices running on 802.11 wireless LANs. These devices include Wi-Fi telephone handsets and wireless PDAs with a softphone download. Wi-Fi telephone handsets designed specifically for IP telephony systems are equipped with programmable line/feature buttons and display fields that access and support all the IP-PBX features and functions available to wired desktop instruments. PDAs can potentially offer the same level of communication functionality as a desktop PC client softphone.

Top 10 Critical Steps

There are numerous financial, system design and application benefits that can be derived from an IP telephony system, but only if an IT professional properly plans, implements, and operates the new voice communication solution. With all the benefits of a VoIP system in a converged network, there are key considerations and actions that need to be taken for the most successful implementation. These are summarized below as the top 10 most critical steps for ensuring VoIP deployment success.

1. Identify the potential benefits to be derived from an IP telephony system, as compared to the existing voice system solution, to determine if a system migration is warranted.
2. Determine the optimal IP-PBX system design (IP-enabled, converged, or client/server) for the system configuration requirements, including the mix of IP and non-IP ports, recognizing that each type of design and port configuration mix will have unique LAN/WAN traffic engineering requirements.
3. Prior to the new system selection process, perform a cursory audit of the current LAN/WAN infrastructure to assess design weaknesses that would likely degrade real-time voice communication services. Include in the audit an evaluation of all network node elements, available software options, and redundancy level of switches, routers, power sources, and network transmission links.

4. Determine current and forecasted traffic requirements.
5. Adequately test and monitor the following performance characteristics of the current LAN/WAN, which would affect voice-grade QoS levels:
    a. packet transmission latency;
    b. jitter;
    c. packet loss; and
    d. echo
6. Adequately test and monitor the LAN/WAN for any of the following potential security breaches:
    a. access control;
    b. data control;
    c. disruption; and
    d. eavesdropping
7. Deploy the necessary steps to upgrade the LAN/WAN to correct any QoS and security problems that would degrade voice communication service.
8. Perform traffic simulation studies over the upgraded LAN/WAN to determine if the desired voice-grade service levels have been satisfied.
9. Ensure that the selected vendor is properly authorized and certified to configure, program, and install the new IP telephony system across the upgraded LAN/WAN.
10. Continually test and monitor the IP telephony system and LAN/WAN after initial deployment to ensure that satisfactory QoS and security benchmarks are maintained.

As these critical steps illustrate, ensuring that the “old data network” has been properly analyzed and upgraded for real-time voice communication requirements is one of the most important tasks for successfully deploying an IP telephony system. Even if you are not yet ready for your first IP-PBX system, you can begin preparing now for the eventual installation by “future-proofing” your LAN/WAN with the necessary bandwidth, QoS and security design parameters at the earliest opportunity. Knowing that the next voice communication system solution will be based on IP telephony, it’s never too early to begin planning and implementing your VoIP network.

Phone: 949-450-8700
Fax: 949-450-8710
E-mail: info@broadcom.com
Web: www.broadcom.com
VOIP-WP101-R

BROADCOM CORPORATION
16215 Alton Parkway, P.O. Box 57013
Irvine, California 92619-7013

04/12/2005