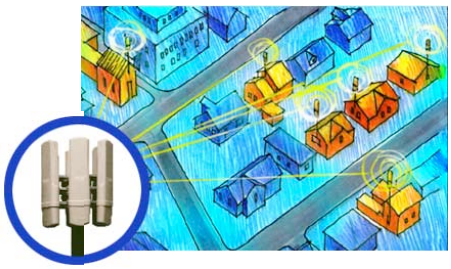
MOTOROLA



Canopy® - VoIP Architecture

Application Note

Canopy-VoIP-Architecture-AN-en
Issue 1
June 2006

CANOPY™
Motorola Wireless Broadband Platform

Notices

The vendor data in this Application Note derive from the Canopy User Guide and various HotZone provided MetroMesh User Guides. Motorola provides this vendor data for Canopy users information only and does not provide any recommendations.

Please refer to the Canopy System User Guide, posted at www.motorola.com/canopy for:

- Personal safety guidelines in Preventing Overexposure to RF Energy
- Important regulatory and legal notices

Trademarks, Product Names, and Service Names

http://www.motorola.com/canopy

Table of Contents

Table of Figures

New in This Issue

This document is Issue 1 of the Canopy – VoIP Architecture Application Note.
This section is a placeholder where changes will be listed in future issues.

Using This Canopy – VoIP Architecture Application Note

This document should be used with following Motorola Canopy® documentation:

- Canopy System User Guide

- Important: Visit the Canopy Support Web Site to download the latest Canopy software and Canopy User Guides. http://motorola.canopywireless.com/support

Searching This User Guide

To search this document, look in the Table of Contents for the topic. To find information based on any expression used in this document, open the document in an Adobe Reader® session and

- Use the page numbers at the bottom of the screen and in the thumbnails. These match the page numbers in the Table of Contents.
- Use the **Edit→Search** command (or **Ctrl+F**) to find a word or phrase.[1]

Getting Additional Help

To get information or assistance as soon as possible for problems that you encounter, use the following sequence of action:

1. Search this document, the user manuals that support the modules, and the software release notes of supported releases
    a. in the Table of Contents for the topic.
    b. in the Adobe Reader® search capability for keywords that apply.[1]
2. Visit the Canopy systems website at http://www.motorola.com/canopy.
3. Ask your Canopy products supplier to help.
4. Gather information such as
    - the IP addresses and MAC addresses of any affected Canopy modules.
    - the software releases that operate on these modules.
    - data from the Event Log page of the modules.
    - the configuration of software features on these modules.
    - run the Gather Customer Support Tool within CNUT
5. Escalate the problem to Canopy systems Technical Support (or another Tier 3 technical support that has been designated for you) as follows. You may either
    - send e-mail to technical-support@canopywireless.com.
    - call 1 888 605 2552 (or +1 217 824 9742).

For warranty assistance, contact your reseller or distributor for the process.

Go to page 39 for Additional Resources

[1] Reader is a registered trademark of Adobe Systems, Incorporated.

Canopy – VoIP Architecture Application Note:

1.0 Abstract:

Motorola Canopy is a Broadband Wireless Access (BWA) technology intended for the fixed and nomadic ("portable") market and employing unlicensed electromagnetic spectrum over metropolitan distances. The customer edge of Canopy is an Ethernet cable to a local Internet typically consisting of one or more computer and/or IP routers. Historically, the customer's network is intended for data.

Recently, technology has extended data to include voice; generically termed Voice over IP (VoIP). Unlike data, VoIP is sensitive to end-to-end delay, packet discard in the intermediate network due to congestion, and is a symmetrical flow.

This new capability has Canopy operators wondering if and how Canopy-based BWA plays are role in formal or informal VoIP service.

As a service to Canopy operators and sales teams, this Application Note describes the characteristics of using Canopy BWA in a VoIP architecture and the possible business opportunities.

All non-Motorola vendor examples and their characteristics are derived from publicly available material and are included only to represent possibilities.

2.0 Business Case for VoIP

In this section, a short review of the Canopy BWA architecture is provided to set the stage for a VoIP architecture discussion. Figure 1 shows the Canopy operator's network with Canopy Base Stations and customer Subscriber Modules. Note the carrier's network consists of links between packet switches, usually IP routers. In addition, the carrier's network is interconnected to one (or more) other Internet Service Providers to attain global Internet connectivity for the carrier's BWA customers.

The Subscriber Module (SM) is produced in several variations, namely the Classic SM, the Advantage SM, and the SM Lite. As the latter is comparatively new it is described here.

Canopy Lite SMs work with the Canopy Advantage access points and deliver speeds of 512 Kbps throughput with 768 Kbps burst and a maximum of 100 Kbps full duplex Committed Information Rate (CIR). The Canopy Lite SMs offer substantially lower costs with the same high performance, reliability and interference tolerance as all Canopy SMs. The Canopy Lite SM can be software upgraded via floating license keys from the Canopy Prizm element management system to add incremental throughput (to 1, 2, 4 or 7 Mbps) quickly and economically. See Figure 20 for SM Lite's performance restrictions.

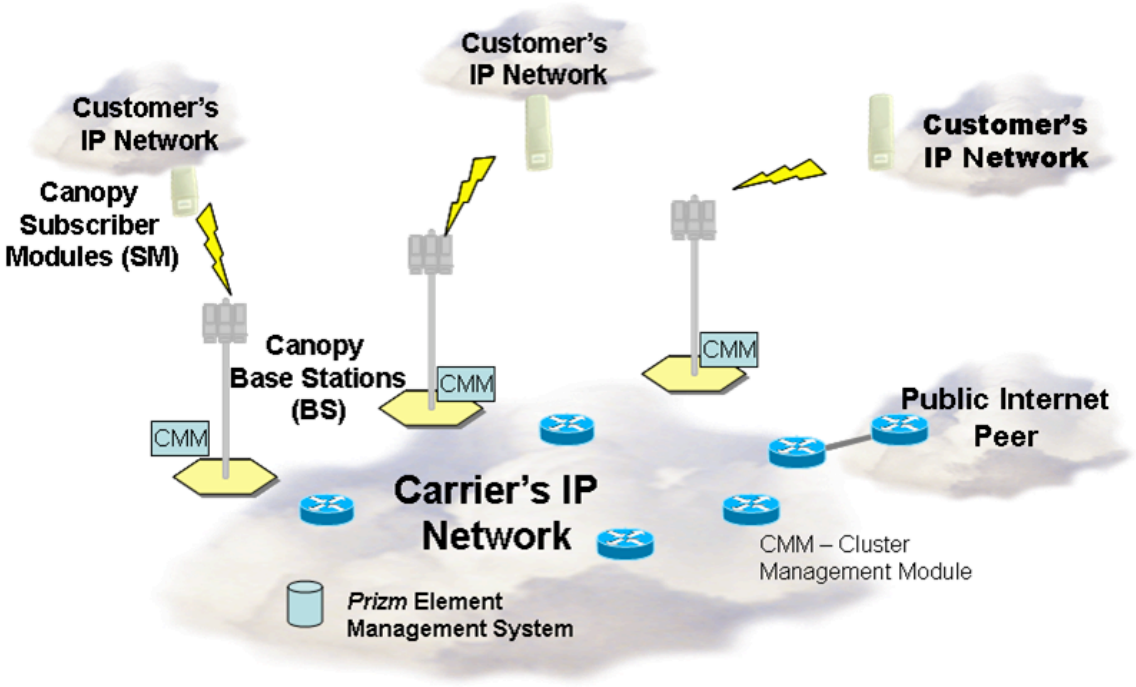


Figure 1. Generic Canopy-based BWA architecture.

Note that Canopy Lite SM has more than enough throughput capacity to handle a one or two VoIP telephone call.

Historically, this network architecture is for data, which excludes applications that have extraordinary performance requirements like end-to-end delay. Now, however, various VoIP "softphones" and "hardphone" are available for computers that support voice. These softphones either have the look-and-feel of a modern cell telephone or that of a modern instant messaging chat application that additional supports voice. Hardphones have the look-and-feel of ordinary digital telephones.

This level of VoIP-based telephony is transparent from the underlying internet infrastructure technology. The Canopy-based BWA and the wired internet infrastructure are oblivious to any peer-to-peer VoIP packet flows. The one exception to this transparency is any Network Address Translator (NAT) between the voice endpoints, for example, such as can be configured in a Canopy Subscriber Module or other customer CPE router.

NAT is a problem because peer-to-peer communication, like voice, requires application signaling end-to-end. This means the applications embed their own IP address in application layer packets, and expect to be communicating directly with the far end. NAT, by definition, breaks this by hiding the actual IP addresses from each other.

This "NAT problem" leads to solutions like STUN (Simple Transversal of UDP over NATs), in which both ends of the potential peer-to-peer communication must first register. This enables the endpoints to know the intermediate public IP addresses of the NAT(s) such that proper exchange of signal can take place. Another solution is to make the voice application into a web application which, because it is widely "open", also defeats NATs and firewalls.

The important point is that Canopy-based customers may be employing voice applications even now without the Canopy operator even knowing or doing anything.

However, at this level of VoIP, the Canopy operator is not functioning as a VoIP Service Provider nor billing for voice services. This paper discusses the VoIP business opportunity alternatives possible for a Canopy BWA operator.

2.1 Alternative VoIP Business Opportunities

Rather than the transparent VoIP use of a Canopy BWA system the Canopy operator has several options for providing value added revenue enhancing VoIP services.

A set of VoIP service business alternatives are listed in Figure 2 below. Note Item 1 is the "do nothing" scenario described in Section 2.0 above.

The first VoIP business alternative is for a Canopy operator to offer a Service Level Agreement (SLA), differentially priced, stipulating Canopy's QoS capabilities. These services levels are often referred to in the "Olympic Model" of Gold, Silver, and Bronze. Prizm 2.0 offers the capability to create service plans to offer multiple service levels.

The next VoIP business alternative is to provide customer VoIP capability to the customer's usual analog telephones. The box is generically termed an Analog Terminal Adaptor (ATA). Motorola and many of vendors make ATA devices intended for the residential SOHO consumer. Here the Canopy BWA operator either sells the ATA or charges a recurring monthly fee to the customer.

1. Offer nothing but BWA; no explicit VoIP service
   - Allow third party-based VoIP service or peer-to-peer voice be transported transparently; no VoIP revenue
2. Offer stipulated QoS and CIR BWA service
   - SLA fee but without reference to "voice"
3. Offer to provide Analog Terminal Device only
   - Or similar CPE device
   - SLA fee but not be a VoIP Service provider
4. Offer and become an "interconnected" VoIP Service provider; fee: bill subscriber per minute
   - That is interconnected to the PSTN (Public Switched Telephone Network); provide E911

Figure 2. VoIP Business Alternatives for Canopy Operators.

The last Canopy operator VoIP business alternative is to become a full-fledged VoIP Service Provider. In this case the Canopy operator literally becomes a telephony provider meaning the providing of "hard" or "soft" VoIP telephone sets, providing both inbound and outbound VoIP calls to regular Public Switched Telephone Network-based (PSTN) subscribers, provide Enhanced 911 (E911) and operator services, and of course provide itemized bills based on a per-minute subscription plan.

The latter alternative is clearly a huge step so the business ramifications are the focus of this paper.

The various business opportunities from a user/customer perspective are shown again in Figure 3. This diagram shows a generic Broadband Modem connecting to a generic

internet icon; of course in the Canopy context the Broadband Modem is the Canopy Subscribe Module (SM) and access is wireless.

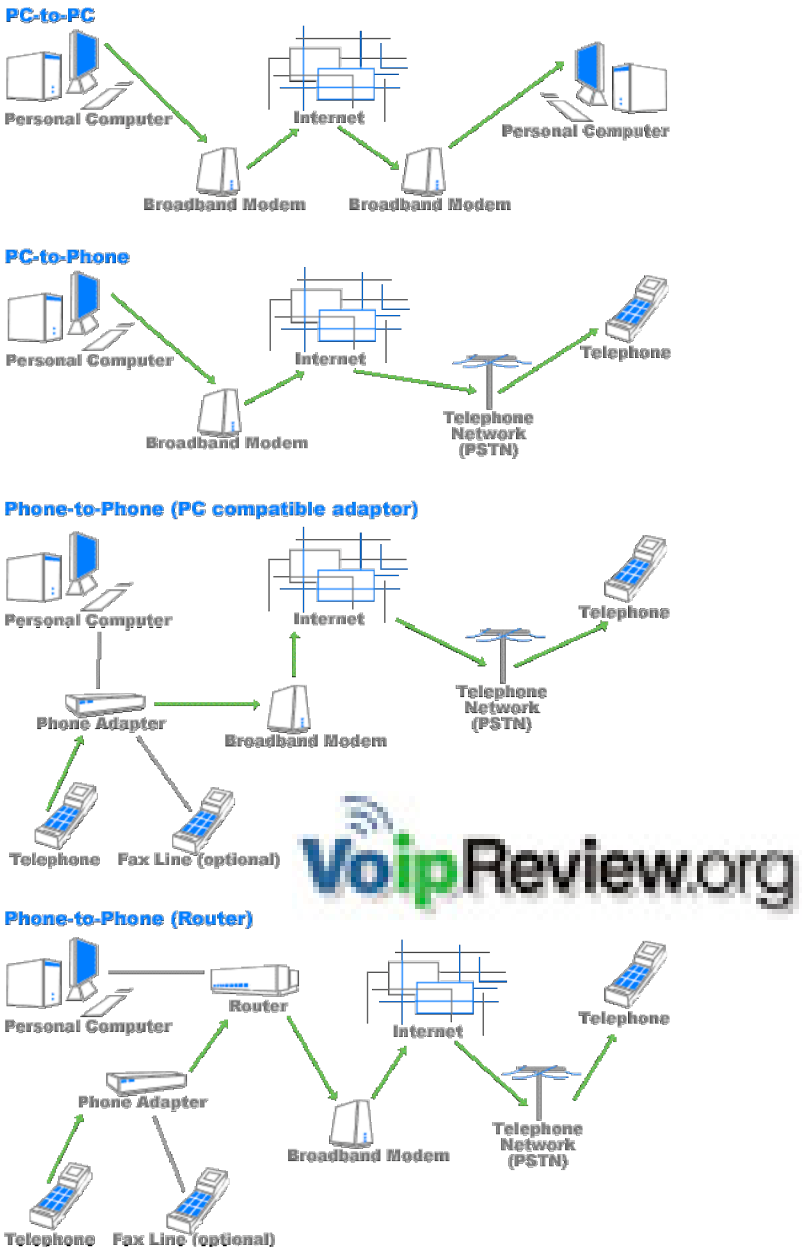


Figure 3. Diagram of Voice Use Alternatives www.voipreview.org.

From the top, the PC-to-PC is the “do nothing” alternative, with VoIP softphones on computers. This is most likely already happening over a Canopy operator’s network.

The second case shown, PC-to-Phone, requires that the Canopy customer has additionally subscribed to a so-called inbound/outbound service. This requires a subscription fee, but of course, the Canopy operator is not participating in this scenario.

The third case, Phone-to-Phone (PC compatible adapter), requires the special ATA device mentioned above. Note, in context, that the ATA is directly connected to the Canopy SM, with both computers and wired analog telephone sets also attaching to the ATA. Because the call could originate or terminate in the PSTN a VoIP Service Provider with an inbound/outbound service is also required; this may or may be the Canopy operator.

The final (bottom) schematic shows Phone-to-Phone (Router) customer networking. Here the Canopy SM is connected to a home IP router, possibly with WiFi capability as well. The latter device is then connected to computers and an Analog Terminal Adaptor (ATA), with ordinary telephones attached to the ATA. This is the case in which the Canopy operator is a full-blown telephony service provider.

There are many VoIP telephony service providers, ranging from all the usual telephone companies to very small independent firms. The latter directly solicit VoIP customers and usually also solicit business partnership relation with other access providers, perhaps with Canopy operators.

For your information a short but very incomplete list of VoIP service providers follows: Vonage, SunRocket, DigiDial-VoIP, Packet8, Cordia, VoIPNet, Myphonecompany, ITP (Internet Telephone People), NetZero, iConnectHere.

The fourth VoIP business alternative is for the Canopy operator to become one of the above.

In the next section, the usual and necessary CPE alternatives are described.

2.2 Overview of Canopy Subscriber Analog Telephone CPE

In this section, the VoIP Architecture components on the Canopy subscriber's premises are described.

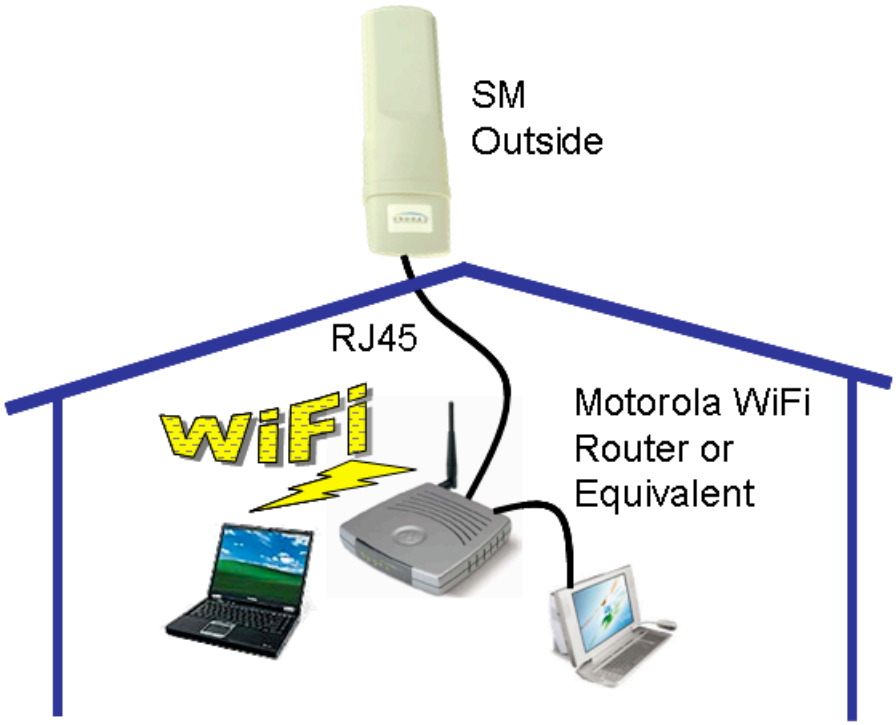


Figure 4 Schematic of typical Canopy Subscriber data CPE.

Figure 4 shows a typical CPE data environment, in which the subscriber has a home network" oriented toward historic data. Note this included a home WiFi capability as shown in Figure 4 by a Motorola WA850 wireless router. Importantly, the subscriber is likely to use and configure a firewall, NAT, and DHCP server in the wireless router rather than expect these functions in the Canopy SM. Thus, for the Canopy SM to be equivalent to a telco's DSL Modem or a cable provider's Cable Modem the Canopy SM would assign a single public IPv4 address to the WAN side of the wireless router. The latter means that any VoIP peer-to-peer problem is a subscriber issue, not the Canopy-based BWA service provider (WISP).

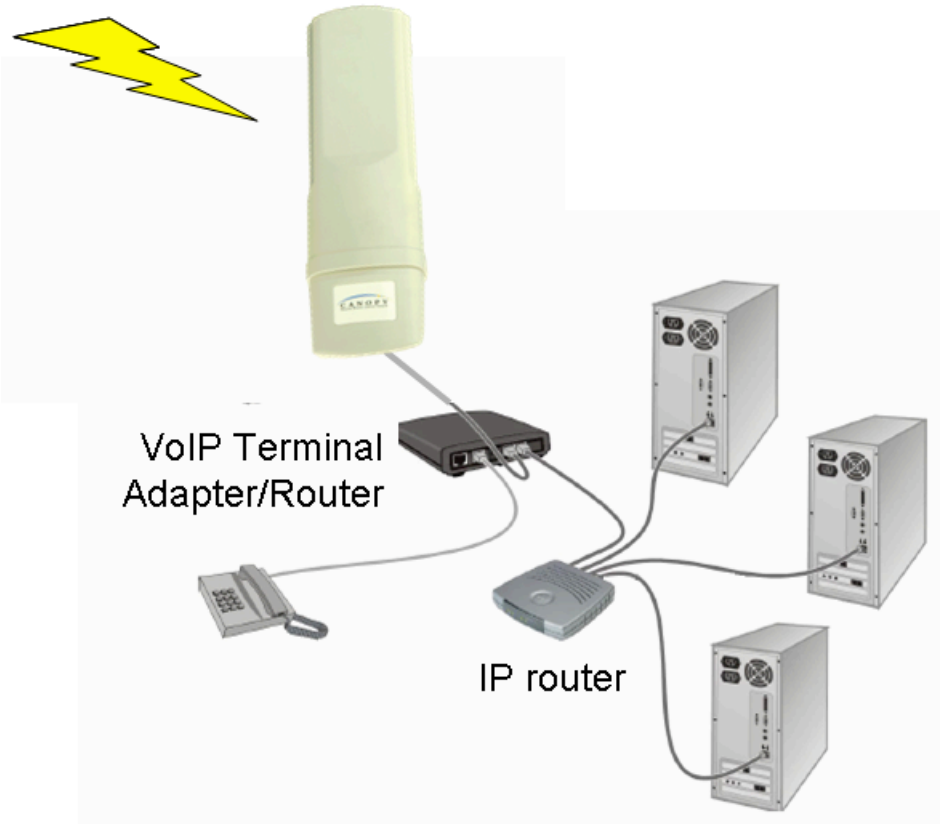


Figure 5 Schematic of typical Canopy Subscriber voice CPE.

Figure 5 extends the CPE data architecture to include voice or VoIP. Note the Canopy SM is now connected to an Analog Terminal Adapter (ATA). Off the ATA are two sets of equipment: a set of one or more ordinary analog telephones, and a set of the usual data equipment. Shown are a Motorola IP router (without WiFi) and several attendant home computers.

Of course, the IP router could have WiFi wireless capability as well, as shown in Figure 6 below.

The main point is that in both cases the ATA comes first; that is, it is connected directly to the Canopy SM. Remember that the ATA is converting analog voice into a stream of VoIP IP packets (and visa-versa). By inserting the ATA box first, it is able to mark the VoIP IP packets with a higher QoS tag than the ordinary computers. When the Canopy SM is correspondingly configured for QoS (described elsewhere in this document) the VoIP packets will be placed into a high priority queue and hence experience less Canopy-induced delay, an important factor in a user's perception of voice quality.

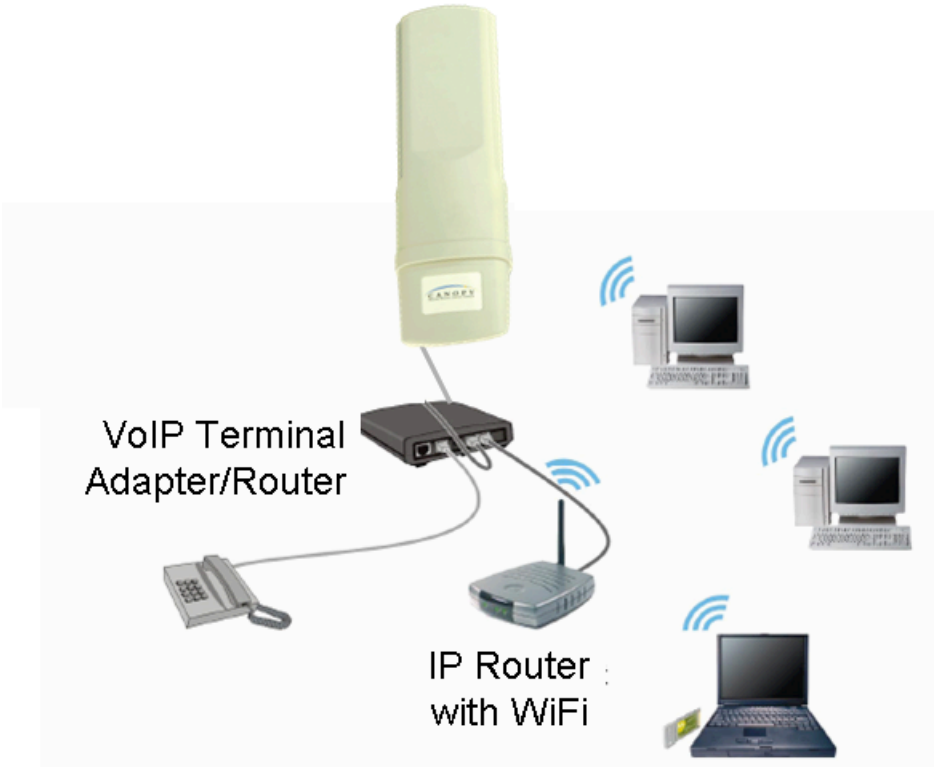


Figure 6 Schematic of CPE with WiFi data capability.

ATAs are available from many vendors and with some number of RJ11 analog telephone jacks and some number of RJ45 Ethernet jacks. For example, three Motorola ATAs are shown in Figure 7 below.

Because telephony service has historic user expectations, every ATA vendor feels it necessary to qualify their ATA products. Motorola's ATA, for example, states:

> ***"Be advised that any services provided through this equipment are not intended to replace or be a substitute for primary line voice services or Plain Old Telephone Service (POTS) and are not meant to provide guaranteed 911 or E911 services or to permit access to 411 directory assistance services. Your service provider, not Motorola, is responsible for the provision of Voice over IP (VOIP) telephony services through this equipment. Motorola shall not be liable for, and expressly disclaims, any direct or indirect liabilities, damages, losses, claims, demands, actions, causes of action, risks, or harms arising from or related to the services provided through this equipment. Important: be aware that you will not be able to make any calls using this Voice over IP (VOIP) device if your broadband connection is not functioning properly. You will also not be able to make any calls using this Voice over IP (VOIP) device if you have lost electrical power."***

The issue of E911 and other considerations are discussed elsewhere in this document.

Figure 7 Three Motorola Analog Terminal Adapters (ATA), one with WiFi.

As time and technology advance, it may be that historic data IP wireless routers and ATA with data ports devices will functionally merge, with a single device being an IP router with WiFi and RJ11 analog telephony ports.

Of course, many vendors produce ATA devices of various capacity and capability and integration with traditional data elements.

2.3 Subscriber Hard Digital Telephone CPE

In this section we describe wired digital VoIP "hardphones".

It may be that the Canopy subscriber will independently purchase new digital VoIP telephone sets to replace the telco historic analog station sets. These new digital VoIP telephones have the "look & feel" of ordinary analog telephones but with superior displays. Unfortunately these new digital telephones are quite pricey but they do obviate the need for an ATA.

Motorola doesn't sell digital wired VoIP telephone stations so we illustrate only one other vendor (of about twenty) that does, namely Cisco. Figure 8 shows a conference room telephone (retails at about $1000) and color display feature rich telephone (retails at about $450).

At the low end (retailing at under $100), there are a number of "brand X" vendors of very basic VoIP digital telephones.

These telephones have RJ45 Ethernet jacks so are connected directly to a data network. For example, one could be directly connected to a Canopy SM. However, this arrangement is unlikely, as usually the digital telephone would connect to a local IP router port, along side other local computers.

Figure 8 Example of two Cisco high end digital VoIP telephones.

2.4 Subscriber's Computer as a "Soft VoIP Telephone"

A VoIP user need not have either real analog telephones or a special purpose digital VoIP telephones.

Alternatively, if ordinary data computers are available and left on, they can be configured with "soft telephones" (or "softphones").

Many softphones exist from many vendors and most are even "free". Initially these had the look and feel of cellular telephones as is shown in Figures 9 and 10.

These softphones are typical in that they assume the user wants the cellular experience; now video is an added feature.

Note a particular VoIP Service Provider may stipulate or at least "feature" a particular softphone, as Vonage does with X-Ten (now owned by Counterpath).

Figure 9 Cell-like softphone by X-Ten used by Vonage.

Increasingly softphones are adopting the "look & feel" of instant messenger (IM) chat applications. Originally, IM chat tools didn't have voice capability, instead only communicating short typed sentences and emoticons. But they did have presence capability, in which a user knows if a potential chat partner is there and available. For example one maintains a buddy list of potential chat partners, and each can mark themselves as "online", "busy", "away", etc.

Consequently, it is a small step to generalizing IM chat tools to include two-way VoIP voice. One of the first was Skype which has been extremely successful even though it is a closed (not standard) system, only communicating with other Skype chart endpoints.

Subsequently, we will discuss the issues of calling an ordinary PSTN telephone.

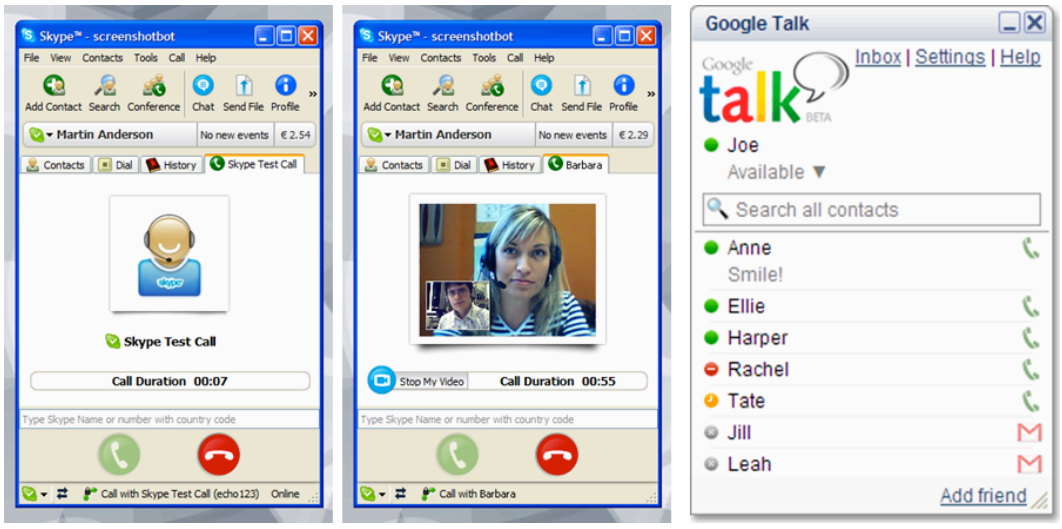


Figure 10 Examples of Skype and GoogleTalk softphones.

Figure 10 shows two Skype screen captures, one voice only and the second with video. The third IM-type voice tool is Google's GoogleTalk. The latter has opened its technology to other competitors and so is capable of communicating to other non-

GoogleTalk endpoints. The ramifications of this are discussed elsewhere in this document.

Not shown are the many other chat-like tools that are only now developing the additional voice capability.

2.5 Wireless VoIP Technology for the Subscriber

As nice as computer-based softphones are, they can only be used at the desktop or laptop computer, typically with an optional wired headset (that breaks the speaker to microphone feedback loop).

Increasingly, IEEE 802.11 WiFi is being used for “softphones gone hard” and for special hardphones. For example, Figure 12 shows a Microsoft Pocket PC loaded with X-Ten’s softphone.

Alternatively some vendors are building special WiFi-based VoIP telephones having the look and feel of a traditionally cellular telephone. Usually these special WiFi telephones are actually dual mode -- meaning they additionally support CDMA and GSM cellular technology.

Figure 11 X-Ten's softphone on a Microsoft Pocket PC; uses WiFi.

Figure 12 UT Starcom's F1000G WiFi telephone.

3.0 FCC Requirements for "Interconnected VoIP Service Providers"

If the Canopy operator wishes to become a "real" VoIP Service Provider, enabling interconnection with the PSTN, the national government will impose requirements. In the USA, this agency is the Federal Communications Commission (FCC).

The concern is the mandates already placed upon real telephony providers like historic telephone companies. These requirements are expensive but mandated as the telephone, over the decades, has evolved into a "life line" device. This means contacting emergency services like police, fire, and medical.

Consequently, the telephony industry expects these government mandates to apply to their VoIP competitors as well. In particular, mandates are for Enhanced 911 services in which the physical location of a telephony subscriber is maintained in a database.

3.1 FCC Order Applicable to "Interconnected" VoIP Providers

For reference we quote the FCC Order:

> *"The ability to access emergency services by dialing 911 is a vital component of public safety and emergency preparedness.*
>
> *Recent reports of consumers' inability to access life-saving emergency services while using Voice over Internet Protocol (VoIP) services have highlighted a critical public safety gap.*
>
> *The Federal Communications Commission (FCC) has taken steps to close this gap by imposing Enhanced 911 (E911) obligations on providers of "interconnected" VoIP services, i.e.*
>
> > *VoIP services that allow users generally to receive calls from and terminate calls to the public switched telephone network (PSTN), including wireless phone networks."*
>
> *Source: www.fcc.gov/cgb/consumerfacts/voip911.html*

The Enhanced 911 obligation requires that such VoIP operators must obtain from their customers their physical location, have that information entered into the appropriate E911 service center, and to either provide or subscribe to E911 services.

4.0 VoIP Signaling Technology

In this section, the internet-based signaling alternatives are briefly discussed, followed by the soft-switch and media gateway.

Like in traditional PSTN telephony the VoIP telephones, both "soft" and "hard" or via an ATA, must signal some pre-determined place in the network of their call request (which includes the destination telephone number). The initiates the call setup phase.

In the case of VoIP telephony service the telephony application must know the IP address of that special place which is generically called a soft-switch. Additionally, the soft-switch must signal the destination end of the VoIP call which might include a media gateway if the termination is in the real PSTN.

The soft-switch may signal other soft-switches, but eventually a soft-switch will signal the final VoIP telephone or its ATA agent. In particular, if the call attempt is an outbound call, terminating on the PSTN, the soft-switch signals a media gateway or VoIP gateway. If a real PSTN telephone is calling a VoIP terminal, then it too must transit the gateway (GW).

In other words, a VoIP call that either originates or terminates in the PSTN must transit a GW, with special VoIP signaling on the internet side and traditional telco signaling on the PSTN side. As stated in the previous section, such a service makes the VoIP service provider interconnected and so obligated to provide E911 service as well.

While the soft-switch and GW are logically distinct devices, they may in fact reside on the same hardware package.

This is a large and very technical subject so this is only an overview; Motorola does not claim expertise or completeness in what follows, and has no direct Canopy-related knowledge of any particular products.

4.1 VoIP Internet-based Signaling

In this section, both VoIP internet-side signaling is briefly described. This discussion is generic and not in the terminology of specific vendors or industry. In particular, we keep it simple. Appendix A shows the International Telecommunications Union definition of the Next Generation Network which is all IP-based – note the complexity.

In all cases, signaling is an application layer task from the perspective of the internet. That is, nothing in the intermediate internet, including the Canopy-provided wireless access, need to know anything of VoIP signaling. Only the VoIP telephones (hard or soft), ATAs, soft-switches, and a GW get involved in signaling.

Figure 13 shows a list of common VoIP (internet side) signaling technologies. A Canopy operator must have at least a working knowledge of these protocols.

- ITU telco industry: H.323 and adjuncts
  - "Bellheads"
- Internet IETF: Session Initiation Protocol (SIP)
  - "Netheads"
- Java-based JAIN set of APIs
  - *JAIN: Java APIs for Intellignet Networks*
  - Java implementation of SIP
- XML-based like "open" JINGLE
  - JINGLE started as Google's *GoogleTalk* signaling
  - XMPP (called "Jabber") – *Extensible Messaging and Presence Protocol* RFCs 3920/21
  - Skype uses proprietary XML-based signaling

Figure 13 List of VoIP Signaling Protocol Alternatives.

The first organization to define telephony signaling for use on the internet is the International Telecommunications Union (ITU) with its "H series" of specifications.

Almost in parallel, the Internet Engineering Task Force (IETF) began work on its Session Initiation Protocol (SIP). The two camps are sometimes referred to as "bellheads" and "netheads" respectively, and approached the signaling implementation differently. In Figure 13, these are the top two bullet items.

Defining a protocol, like SIP in this case, is independent of its implementation. Normally, a protocol is programmed in a traditional programming language. However, SIP was also implemented in Java under the auspices of Sun MicroSystems, Inc. This is the third bullet item in Figure 13.

It seems like SIP won in the sense that it is by far the most used and is the establishment's choice. However, a third surprise entry into the signaling arena has recently appeared. This is in the form of signaling via Extensible Markup Language (XML), indicated in the last bullet item of Figure 13.

This is derived from the unrelated "chat" or sometimes "talk" application which is text-based communication in near real-time. In particular, chat applications typically use

Extensible Messaging and Presence Protocol (XMPP) which is XML-based, defined by the IETF and so it is “open”.

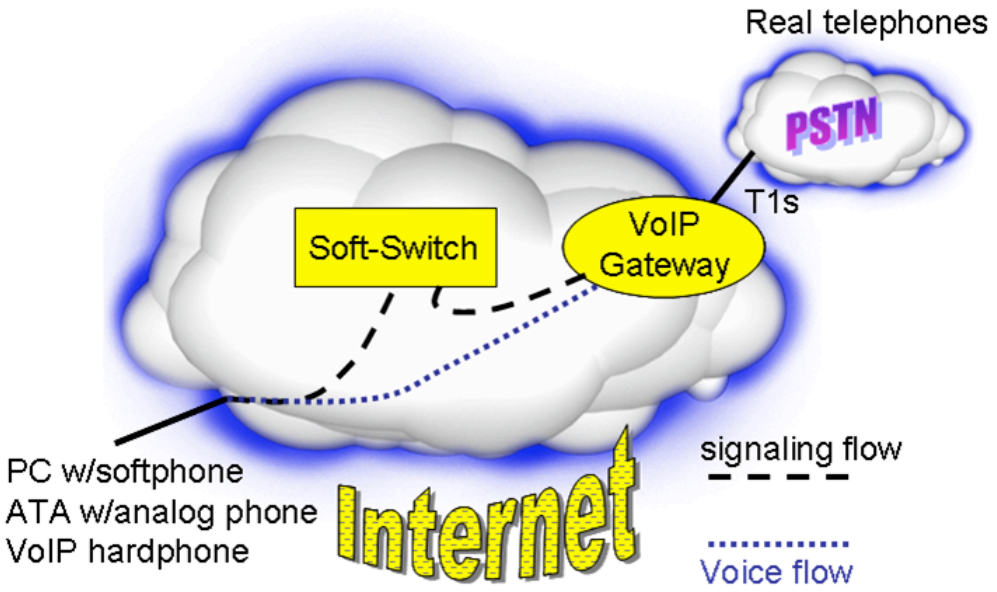


Figure 14 Schematic of packet flows for Interconnected Call

The most popular instant messaging signaling protocols are proprietary like those of Microsoft, Yahoo, etc. However, these where reverse engineered so now just about any chat application can communicate with other chat applications.

The above is relevant because Skype added voice to its chat application and defined its own proprietary voice signaling. With its immediate popularity, others (principally Google) also added voice capability to become “GoogleTalk”. While initially proprietary, Google then placed its XML-based voice signaling into the public domain (open) where it has emerged as JINGLE. Expect almost all of the chat based tools to incorporate VoIP via JINGLE XML-based signaling (see www.jabber.org specification JEP-166).

Consequently, it appears that JINGLE will be a surprise competitor for SIP. This is particularly true for PC-to-PC voice communication; the issue is that a PC-PSTN telephone call must transit a media GW and as of now, these do not support JINGLE (but do support SIP and H.323). Thus, both Skype and GoogleTalk both deploy SIP signaling with a softphone-initiated VoIP call to be terminated in the PSTN.

4.2 Soft-Switch and Media Gateway

In this section, a very brief explanation is provided for the soft-switch and media gateway VoIP components.

According to Wikipedia.com:

> *A softswitch is typically used to control connections at the junction point between circuit and packet networks. A single device containing both the switching logic and the switching fabric can be used for this purpose; however, modern technology has led to a preference for decomposing this device into a Call Agent and a Media Gateway. Well-known manufacturers of Softswitches include Veraz Networks, Data Connection, Ericsson, Huawei, Lucent, Motorola, Nortel,*

Marconi, Siemens, Sonus, Alcatel, Santera, Avaya, Cisco Systems, Cirpack and Xener Systems.

The Media Gateway connects different types of digital media stream together to create an end-to-end path for the media (voice and data) in the call.

Figure 14 illustrates the general idea of a VoIP signaling and subsequent voice flow – in this case, a Canopy subscriber on the left communicating to a real telephone on the right. Note if the Canopy subscriber initiated this call attempt, it would be an "outbound PSTN" call; if the real telephone party initiated this call attempt, it would be an "inbound PSTN" call. To cover both possibilities this general situation is call an "interconnected call" – that is, the Internet and PSTN are interconnected via the VoIP Gateway (GW).

Notice in Figure 14 the Canopy-based BWA is not explicitly shown. This is because Canopy is not directly involved, nor is any other internet infrastructure. The caveat here is that Canopy's performance will impact the caller's perception of voice quality in that both packet delay and packet jitter are imposed on the voice flow. Recall that Canopy's modern Time Division Duplex (TDD) method of operation adds an additional delay element.

To mitigate Canopy performance impact, the Canopy subscriber could be configured to have a Committed Information Rate (CIR) and high priority queuing (refer to section 5.0 in this document).

The VoIP Media Gateway is only involved if a call has real PSTN telephone at the far end.

Figure 15. Mediant 2000 media gateway by AudioCodes Inc.

Motorola does not make a VoIP Media Gateway but all the usual telecommunications vendors do (like Lucent, Nokia, Nortel, Alcatel, etc.). These Media Gateways are larger and of "central office" quality; hence, they are large and expensive.

Alternatively, a number of smaller Media Gateway vendors have come into existence. For example, a Canopy operator may need to provide a maximum of say 96 PSTN interconnected calls at any one time. This means a Media Gateway would need four T1 or three E1 voice trunks into a PSTN provider, paying for this interconnection of course.

At this level, a picture of a relatively modest Media Gateway of that capacity is shown in Figure 16. Note that this device is likely less than central office quality. Many other vendors exist; note the Reference URLs in Appendix B.

On the internet side of a Media Gateway are one or more Ethernet ports that would connect to the Canopy operator's internet infrastructure, and eventually to Canopy Base Station CMMs.

4.3 Call Admission Control

As stated above, all VoIP signaling call setup and subsequently, call teardown is via the Soft-Switch server. This is done by one of several possible signaling protocols which, from the perspective of Canopy (and all network infrastructure) is an "application". In some instances, the VoIP signaling is encrypted. Consequently, Canopy is unaware of VoIP signaling and of a call setup or teardown.

Call Admission Call (CAC) means a determination of whether network resources are available for the next incremental call. For example, an operator may determine that through operational experience, no more than X number of VoIP calls should be permitted in a single Canopy sector. Should an operating company have such a determination, the next X+1 call attempt is denied by signaling to the calling party as a so-called fast busy condition. This orders the VoIP device to play a particular busy tone to the calling party that tells the calling party to hang up and try later.

In the case of VoIP, any such determination is necessarily statistical in nature as other non-voice packet flows exist over the same access link (say a Canopy AP sector).

If a VoIP operator wants to implement a CAC scheme based upon call signaling, this task must necessarily be handled by the Soft-Switch as only it knows when a call setup attempt is initiated. In particular, Canopy and Canopy Prizm do not know this and so can not accomplish the CAC task. Such goals must be tempered by understanding that VoIP calls are not the only packet flows; additional ordinary "data" devices can be attached to an ATA or VoIP hardphone.

As discussed below, Canopy can do priority queues and committed information rate (CIR) to assist in high user perception of VoIP calls. Given the larger broadband wireless packet access context, CAC should be considered a priority queuing and CIR task as distinct from an incremental count of calls in session.

4.4 VoIP Codecs

Physical speech is a variation of air pressure which is then converted to an electric analog by a microphone. In modern telephony, the analog electrical equivalent is further converted to an equivalent digital stream format; the device that does the analog to digital conversion is called a coder/decoder or "codec".

There are many possible codecs so a Canopy operator must have at least a working knowledge of the most common codecs.

The historic telephone industry makes use of the ITU codes, defined as a series of "G.7xx" recommendations. Ordinary PSTN digital voice is G.711μ (North America) or G.711a (Rest of World); this is uncompressed voice consuming 64Kbps on a real circuit (not packet). Of course, this G.711 coding may be packetized and made into VoIP, but packet overheads considerably more than 64Kbps is necessary.

Consequently, VoIP often employs a compression codec; the ITU defines G.723.1 (5.3/6.4 kbps) and G.729a (8 kbps).

Media Gateways will always support the ITU codecs. However, many other codecs exist, some of which are proprietary. A notable exception is the open Internet Low Bitrate Coder (iLBC). This is popular with the newer chat-based VoIP tools. It consumes about 33Kbps and is known for its superior robustness when particular payload packets are discarded (due to router queue overflows). Another is Speex (www.speex.org).

All codecs must package their voice output into a number of milliseconds of voice suitable for one packet payload. Almost without exception, 20ms of voice is placed into one packet. Note that this action by itself induces 20ms of delay compared to real circuit switched voice. This in turn implies 50 packets per second.

Skype is known to employ iLBC but encrypts the packet flow effectively prohibiting any analysis of their encapsulation. However, each direction, in one capture, consumed 39Kbps of bandwidth, each packet being 144 octets long, and sent 33+ packets per second. Apparently, more than 30ms of voice was in each packet.

Generally, VoIP packets consist of the IP header, a UDP header, an RTP header, followed by the coded voice. Note that packet overheads are relatively large compared to the voice payload. There are ways of compressing the packet headers over wireless links but Canopy, at this time, does not support this (i.e. Robust Header Compression – ROHC).

5.0 Overview of Canopy for VoIP

VoIP is an application sensitive to the packet flow's end-to-end bandwidth and delay. The discussion here only relates to the Canopy-specific flow path, namely the radio link between a sector AP and a subscriber's SM.

Canopy supports two features that are applicable here: priority queuing (lowers delay) and Committed Information Rate (CIR) which "guarantees" bandwidth. The latter is in quotes because any statistical circumstance, like packet switch, can provide only a "soft bound" on any performance criterion. In particular, a Canopy operator wishing to explicitly support VoIP should configure their VoIP subscriber accordingly.

First, however, we mention Canopy's Maximum Information Rate (MIR). This is a bandwidth limiting capability so it is not directly applicable to the VoIP scenario. It is indirectly applicable only in the sense that "capping" other subscriber's bandwidth (in a sector) will statistically improve throughput and delay of another particular VoIP subscriber. Consequently, we expound only on Canopy's CIR and priority queue features.

The CIR capability feature enables the service provider to statistically guarantee to any subscriber that bandwidth will never decrease below a specified minimum. However, an important caveat must be clearly understood by the Canopy operator: unless CIR is "oversubscribed."

Oversubscription of CIR within an AP sector means that the sum of the SM's CIR exceeds the actual throughput of the AP sector. Clearly, if this is the case, each SM cannot simultaneously receive its CIR performance measure. In regular Canopy Classic, the effective AP sector throughput is about 7Mbps; with Canopy Advantage, it is about 14Mbps out to about half the cell radius. Consequently, the sum of SM CIRs within an AP sector supporting VoIP services should not exceed these limits.

Of course, actual bandwidth can be, and typically will be, higher than the CIR minimum, but this guarantee helps the Canopy operator attract and retain VoIP subscribers.

Priority queuing is implemented by a network device, like between a Canopy AP and Canopy SM, having two parallel virtual channels on the radio link. The first is the normal or usual “regular priority” channel which in this context will be called the “low priority” channel. The second is the new “high priority” channel supported on P9 hardware or later and Release 7.3 and higher. All Canopy equipment manufactured after the Summer of 2004 is P9 and is capable of high priority queuing.

Before getting into specific Canopy configurations, we describe IP’s DiffServ “codepoints”, or DSCP.

The DSCP is a 6-bit IP header field replacing the now obsolete Type Of Service (TOS) field. Of the 64 possible DSCPs, labeled by Canopy CP0 through CP63 (decimal), only a “pool 1” of 21 codes is currently defined. These consist of eight Class Selectors (CS0-CS7), 12 Assured Forwarding levels (AF11 through AF43), and one Expedited Forwarding (EF). Sometimes these are also called Per Hop Behavior (PHB).

The following 21 Per Hop Behaviors are defined by the Internet Assigned Numbers Authority (IANA) and Internet Engineering Task Force (IETF) RFCs as follows:

The set of eight Class Selector (CS) Codepoints MUST yield at least two independently forwarded classes of traffic, and PHBs selected by a Class Selector Codepoint SHOULD give packets a probability of timely forwarding that is not lower than that given to packets marked with a Class Selector codepoint of lower relative order, under reasonable operating conditions and traffic loads. A discarded packet is considered to be an extreme case of untimely forwarding. In addition, PHBs selected by codepoints '11x000' MUST give packets a preferential forwarding treatment by comparison to the PHB selected by codepoint '000000'. Source: RFC2474.

The set of twelve Assured Forwarding (AF) Codepoints provides delivery of IP packets in four independently forwarded AF classes. Within each AF class, an IP packet can be assigned one of three different levels of drop precedence. A DS node does not reorder IP packets of the same microflow if they belong to the same AF class. Source: RFC2597.

The intent of the single Expedited Forwarding (EF) Codepoint is to provide a PHB in which suitably marked packets usually encounter short or empty queues. Furthermore, if queues remain short relative to the buffer space available, packet loss is also kept to a minimum. Thus EF is for low loss, low delay, and low jitter services. Source: RFC3246.

The remaining 43 DiffServ codepoints are reserved for experimental use and so applications should never mark packets with these DSCPs. Consequently, there should be no need for Canopy to classify based upon these 43 undefined DSCPs either.

In particular, DiffServ employs Expedited Forwarding for VoIP as it means “low delay”. This is DSCP 46 (decimal). It is critical that any VoIP application or ATA or GW set DSCP 46 marking into each IP packet carrying VoIP payload. Canopy APs and SMs look for this marking to classify packets into their appropriate “high” or “low” priority queue.

ATA product user guides typically indicate that they set the DiffServ field to hexadecimal 0xb8. This is an 8-bit representation, so includes the two non-DSCP bits to the “right” of the DSCP 6-bit field. These other 2-bits are IP’s Explicit Forward Congestion Notification (EFCN) bits, and for VoIP (which uses UDP) these should both be set to binary “0”. Consequently, the EF code is properly expressed as 0xb8 when consider all eight bits.

Some industry VoIP phones also set the signaling packets to one of the AF coding, usually AF31; this is not really critical.

5.1 Canopy's Use of VLAN QoS

Canopy can employ IEEE VLAN technology two ways. First, Canopy can be configured to assume that arriving Ethernet frames are in fact VLAN frames which already have a 3-bit QoS code setting marked as per Ethernet 802.1d. Alternatively, Canopy can be configured to modify an ordinary non-VLAN Ethernet frame to include the 16-bit 802.1q VLAN tag. The latter employs the 802.1d semantics derived from the IP DiffServ header.

In this section, we describe these circumstances in the VoIP context and the IP header DiffServ markings.

A review of 802.1d priority semantics is warranted. Eight possible codes are defined. In order from lowest priority to highest priority they are: *Background*, *Spare*, *Best effort*, *Excellent effort*, *Controlled load*, *Video*, *Voice*, and *Network control*. Note that "best effort" is not the lowest, and that "voice" is not the highest.

Recently, the IEEE overhauled the Ethernet QoS by redefining 802.1d semantics in the IEEE 802.11e-2005 standard. The eight QoS classes are now termed *Background, Background, Best Effort, Best Effort, Video, Video, Voice*, and *Voice* respectively.

In case 1, the Ethernet frame arriving into the Canopy complex is already VLAN tagged. In this case, the IP DiffServ DSCP markings are ignored as the VLAN QoS marked takes precedence over IP DiffServ. The details concerning DiffServ in the following section can be ignored.

In case 2, the Canopy AP/SM is configured to construct the VLAN tag which will remain on the Ethernet frame even after leaving the Canopy complex. This VLAN tag construction, which includes setting the 3-bit QoS setting, is accomplished after Canopy has already classified the IP DiffServ priority mark into Canopy's two classes. As will be discussed at length in the next section, Canopy actually classifies into eight classes, with 0-3 being "low" priority and 4-7 being "high" priority.

Consequently, when constructing the VLAN QoS bits, Canopy inserts its internal 3-bit classification directly into the VLAN QoS field. Thus, Canopy takes any previously classified 0-3 priority into the equivalent VLAN set "Background, Spare, Best effort, and Excellent effort" classes. Likewise, Canopy takes any previously classified 4-7 priority into the equivalent VLAN set "Controlled load, Video, Voice, and Network control" classes.

5.2 Configuring Canopy Elements for VoIP

There are two approaches to configuring and administrating a Canopy network. The traditional way is by browsing into each Canopy element (via its built-in Web Server) and manually setting its configuration parameters. The newer and suggested way is to employ the Canopy Prizm 2.0.

Motorola strongly recommends the latter approach. In this regard, Prizm 2.0 now incorporates the previously distinct Bandwidth and Authentication Manager (BAM) functionality. This new Prizm 2.0 greatly eases the configuration and administration of a Canopy network.

In particular, Prizm 2.0 allows the operator to define service classes which can be differentially priced. This might include a special VoIP service class.

As mentioned earlier, the primary need is to reduce packet delay and to ensure sufficient bandwidth to a VoIP subscriber. Consequently, we concentrate on the CIR and priority aspects of Canopy configuration.

The discussion that follows assumes that the operator has Canopy Advantage APs, runs hardware scheduler, and has P9 SMs or later running firmware Release 7.3 or higher.

P8 SMs support CIR but not priority queuing; this is not discussed further as all Canopy elements manufactured since mid-2004 have been P9. Another Motorola Application Note discusses VoIP Pre-P9 Configuration.

In the following section, for completeness, we describe the traditional way Canopy SM configuration via screen captures. In the next section, we describe the new and suggested way via Prizm 2.0.

5.3 Manually Configuring Canopy for VoIP

To support low-latency traffic such as VoIP (Voice over IP), the Canopy system implements a high priority virtual channel. The high-priority pipe separates low-latency traffic, like VoIP, from ordinary data traffic that is latency tolerant, such as standard web traffic and file downloads. This high priority can then be associated with a stipulated CIR.

As stated earlier, the Canopy system separates this traffic by recognizing its IPv4 DiffServ codepoint bits. These IPv4 packet header bits are set by a device outside the Canopy system such as a VoIP application. If particular DiffServ codepoints are set to a particular Canopy priority queue, the system correctly classifies the packet into the high-priority channel and services this channel before any normal traffic. If high priority CIR is additionally configured, then that throughput rate is statistically guaranteed.

As stated above, the IP DiffServ field is a redefinition of the now obsolete original IPv4 Type of Service (TOS) field.

Canopy assumes that VoIP traffic is marked such that, for the Canopy DiffServ classification process, it is placed in Canopy's high priority queue. In general, VoIP packets are likely marked Expedited Forwarding, CP46, prior to entering the Canopy complex.

While DiffServ has many levels of priority defined, Canopy implements only two levels of priority queues. Therefore, a Canopy AP or SM maps DSCP CP codes into one of two queues depending upon configuration. Note that Canopy is, therefore, unable to fully comply with the above DSCP semantics.

However, administratively ,Canopy has eight settable levels of priority, namely 0 to 7. Since Canopy supports two queues – "high" and "low" (meaning "ordinary") – levels 0, 1, 2, and 3 map to "low" priority and levels 4, 5, 6, and 7 map to "high" priority. At some future date, Canopy may implement additional levels of priority queues.

Canopy does have a default DSCP configuration which can be changed as the Canopy operator wishes. The Canopy defaults are shown in Figure 16. Note the DSCP are labeled "CPxx" where "xx" is decimal. The number following is the current priority queue setting corresponding to that particular CP. By default these are stipulated either "0" (low) or "4" (high), with the exception of CP48 and CP56 which are set to "6" and "7" respectively. As indicated in the previous paragraph, 4-7 are all "high priority". Both the CP under assignment and its stipulated priority level are via the drop down boxes illustrated.

Note the VoIP CP46 Expedited Forwarding mark defaults to the high priority queue.

A Canopy operator can set any one CP or any set of CP to whichever Canopy priority class by explicitly employing the two dropdown menu items shown and then “saving changes”.

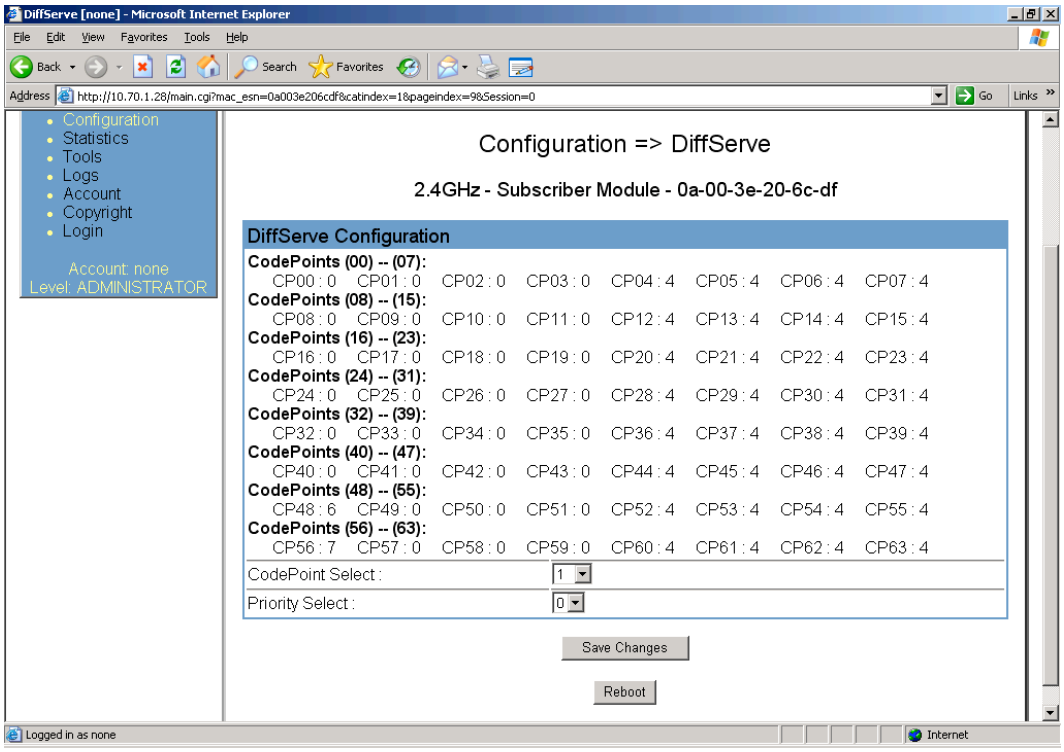


Figure 16. Canopy SM mapping of DiffServ codepoints to queue priority.

Note in Figure 16 the Canopy SM default configuration screen capture is of a P9 Canopy Release 8 SM’s DiffServ tab. Earlier Release versions look much different and are not shown here.

Manually setting a Canopy SM’s CIR (a SM Lite CIR is pre-set) requires going to the Quality of Service tab. Note both MIR and CIR settings are on this screen as is shown in Figure 17. Only if the “Hi Priority Channel” enable button is checked, then “saved”, will you see the “Hi Priority” prompts. To set high priority CIR enter the throughput desired. In general a single VoIP call needs anywhere from about 20kbps to about 100kbps depending upon the codec used (and whether it performs voice compression).

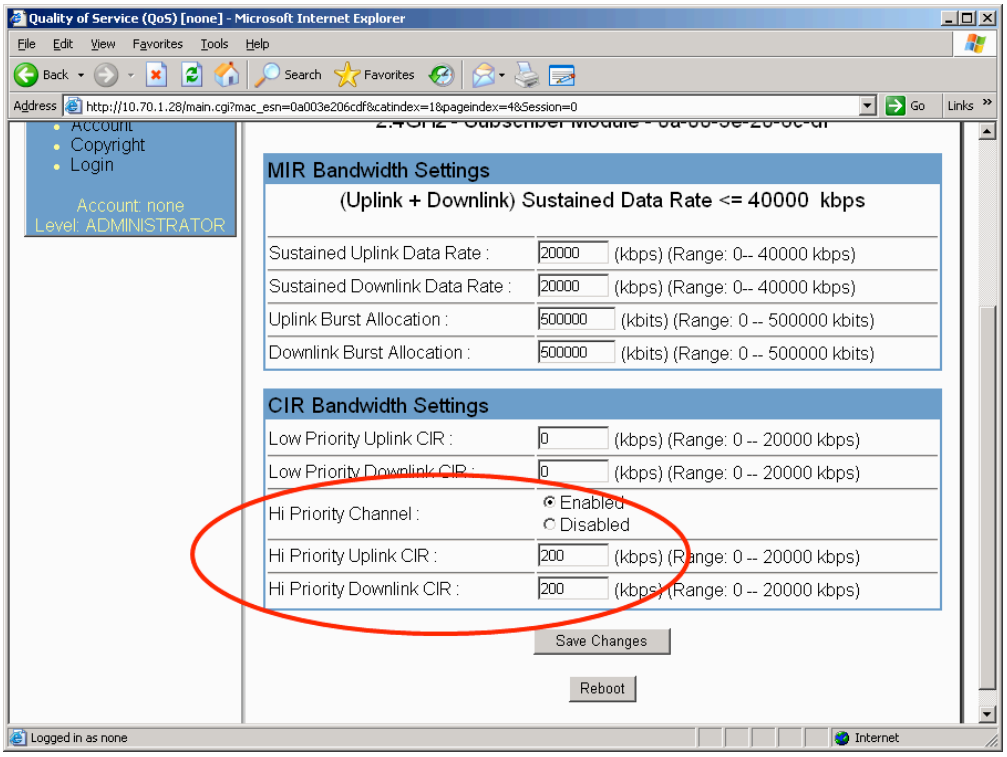


Figure 17. Configuration of SM High Priority queue.

Importantly, note that the SM QoS tab sets both the uplink and downlink CIR. In general, set both directions identically as voice is a symmetrical bandwidth application.

Figure 17 shows the Hi Priority CIR set to 200kbps both for uplink and downlink.

In general, you will not be concerned with CIR for the low priority channel so this can remain unstipulated.

Be certain to “save” and “reboot” the SM. After the SM re-registers with its AP, the configuration is complete.

Now consider the AP of that SM’s sector.

The AP’s behavior is quite different from the SM. For example, the AP has a DiffServ tab just like the SM’s shown in Figure 16. Like the SM, the AP needs to classify packets coming in from the core network (via the CMM). It is recommended that operators use CMM Release 2.2. The AP must then be DiffServ-configured in the same manner as the SM, such that the AP correctly classifies packets into one of its two possible queues.

These AP queues are per-SM specific. Note, however, that the DiffServ classification rules apply to all IP traffic entering the AP (from the CMM) and going to the SMs. That is, the same Diffserv rules for “high” and “low” priority service apply to all incoming (from the CMM) IP packets, but then the classification places the packets in SM-specific queues. This is not a problem because the DiffServ rules should be applied uniformly to all IP traffic.

Likewise, the AP has a QoS tab as shown in Figure 18. Note that the label (in the blue band) is “AP Bandwidth Settings” (not MIR) and CIR is not mentioned. However, the prompts are for “Sustained” uplink/downlink data rate and uplink/downlink “Burst Allocation” which are normally associated with MIR. Consequently, these values are a sector MIR. In the Pre-P9 SM VoIP context, the two “Sustained” values can be set to

3Mbps and 1Mbps downlink/uplink respectively (as an example). The two "Burst Allocation" values can be set to full throughput, say 5.25Mbps and 1.75Mbps downlink/uplink respectively.

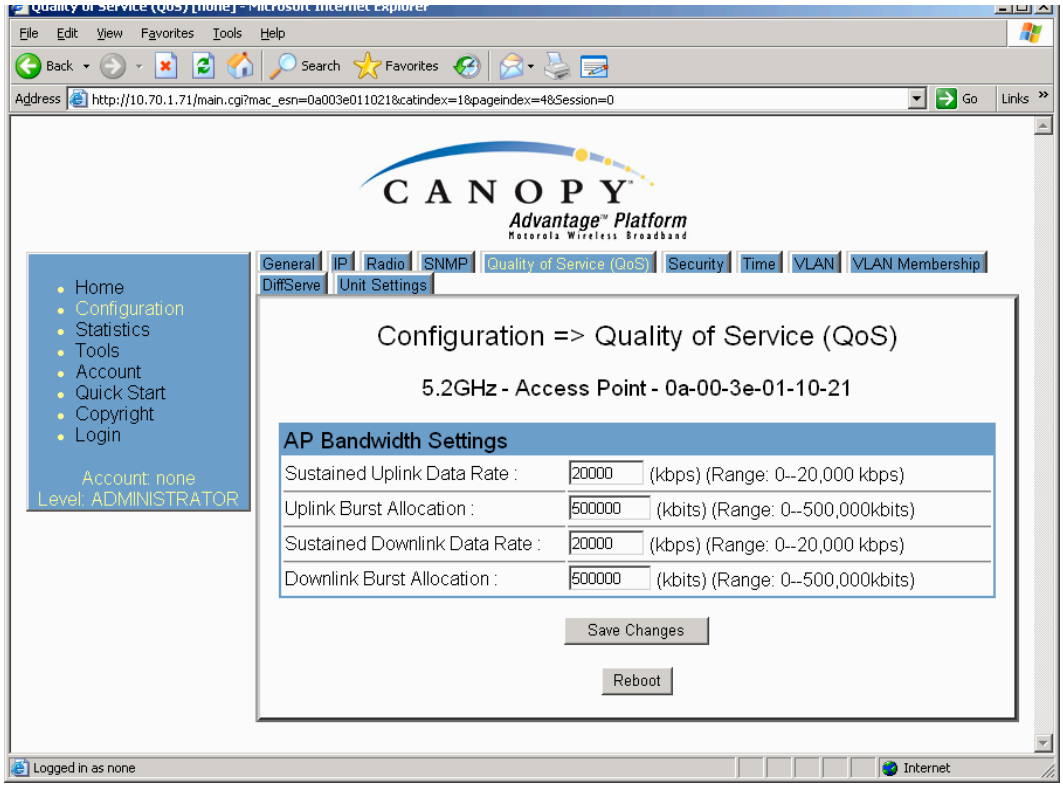


Figure 18. Advantage P9 or greater AP QoS Tab

The effect of these AP settings is to cap the AP's various SMs throughput consumption. This lessens the probability of any one SM bandwidth hog from disrupting a particular SM's VoIP call quality.

In summary, for the AP, configure the AP's DiffServ to correspond to the DiffServ setting applied to its constituent SMs, and cap the MIR of all sector SMs. No AP CIR setting is possible or needed.

After setting the AP's DiffServ configuration, save the configuration and reboot.

At this point, the manual direct configuration of both the AP sector and a particular SM is complete. What remains is the need to verify that the SM and AP both recognize each particular SM's VoIP high priority queue and its associated high priority CIR.

This verification is accomplished by viewing the AP's Session tab. Figure 19 shows a screen capture of an Advantage AP facing the SM configured for high priority CIR. The AP's session screen enumerates, for each of its SMs, exactly what is configured in the priority and CIR regard. Note the items highlighted in the red ellipse. Scroll over the set of registered SMs and make sure that all SMs serving VoIP are configured as desired.

Note the AP's Session tab does not indicate a SM's DiffServ priority classification configuration; that can only be verified by viewing the SM's DiffServ tab.

For completeness, we mention the purposefully restricted capabilities of the SM Lite (all SM Lite's have a "6" in the third digit of the model number, as in SMxx60). Figure 20 shows the five levels of QoS capable by a SM Lite. A SM Lite ships at the lowest level

(at a very low “entry level” price) but can be upgraded via purchasing a new license key in Prizm 2.0. The important point is that even at the SM Lite’s highest performance level, it is still less than an ordinary SM.

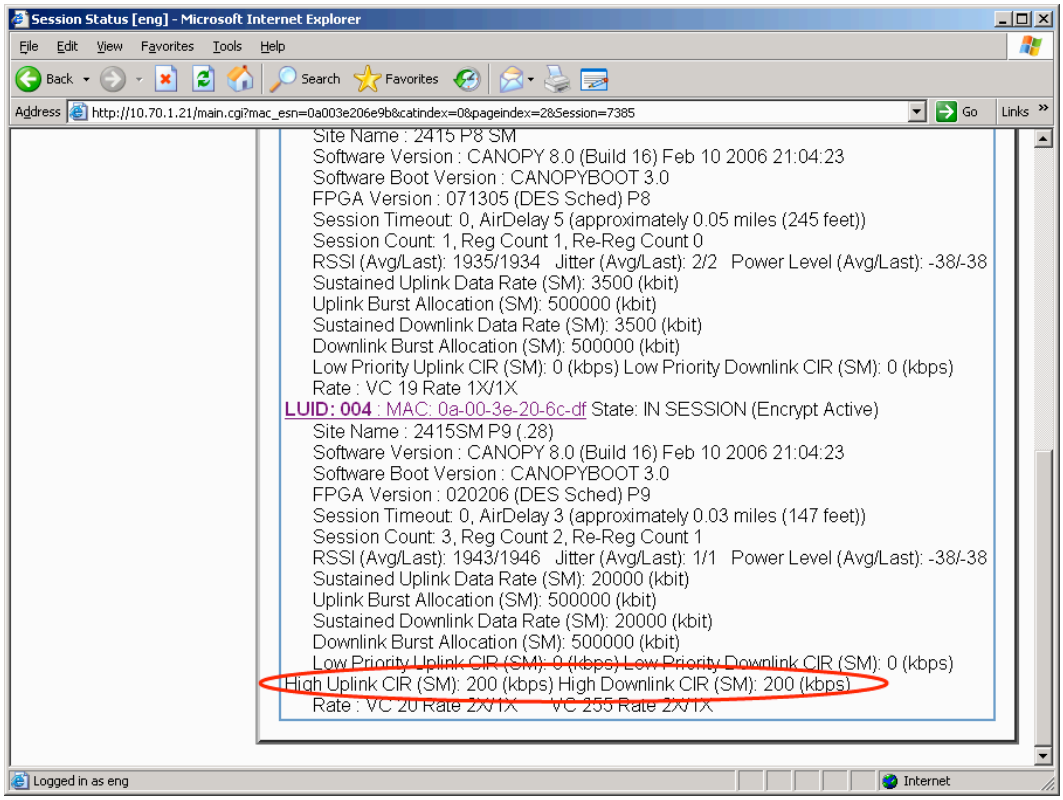


Figure 19. Canopy AP Sessions tab verifying a SM’s Hi Priority CIR configurations.

This has an impact on an SM Lite’s capability to support VoIP.

A SM Lite has exactly the same screens as shown above for regular SMs, but you will not be able to enter MIR or CIR values that exceed the restrictions shown in Figure 20.

Level	MIR[1] (kbps)	CIR[2] (kbps)	Burst[3] (kb)	VoIP Calls Supported
1	512	100	768	1
2	1000	100	1500	1
3	2000	200	3000	1
4	4000	200	6000	2
5	7000	200	7000	2

Notes:

1. Aggregate
2. Each direction, each priority
3. Each direction

Figure 20 Canopy SM Lite performance restrictions.

5.4 Prizm 2.0 - Configuring Canopy for VoIP

As previously indicated, the preferred way to configure and administer a Canopy network is using the Prizm 2.0 element management system. Recall that Prizm 2.0 combines the formerly separate BAM functionality into Prizm along with floating license key functionality.

Of course, at any time, a Prizm administrator can access element web pages to view data and change element configuration parameters, even where the element is not directly accessible from the client machine. This access is secure through the Secure Sockets Layer (SSL) protocol and the HTTPS standard, which supports certificates for the Prizm server web proxy functionality. In this way, all the Canopy web pages as described above in Section 5.3 are accessible.

In this section, we concentrate on how a Canopy operator might define, establish, and "automatically" deploy multiple service levels. The examples are generic VoIP and with screen captures from Prizm 2.0.

In Prizm Release 2.0 and later, either of the following modes is available for the server, subject to licensing:

- BAM-only, which manages only
  - authentication, bandwidth service plans, and VLAN profiles of SMs.
- Prizm, which manages attributes and data for all elements and manages authentication of SMs.
- Prizm floating license keys enable Canopy Lite SMs to be upgraded from 512Kbps to 1, 2, 4, or 7 Mbps.

We assume here that the Prizm user has "Network Manager" level of authority, and is in Internet communication with the Prizm server.

Subject to licensing, you can change an element at any time from BAM-only operations to management functions of Prizm.

Note when managing via Simple Network Management Protocol (SNMPv2c) a device's master acts as a SNMP proxy from the perspective managed device (e.g. a managed SM). Master device here means either an AP (with respect to SMs) or a BHM (with respect to a BHS).

The Prizm server can communicate with SMs or Powerline LV modems in either of two ways:

- by routing the communication to an IP address.
- by SNMP proxy, with requests sent through the proxy in the master device and responses sent directly from the slave device to Prizm.

Prizm always checks first for a routable IP address and, finding one, communicates in that way, regardless of whether the *Use SNMP Proxy If Available* option is checked when the network is defined. However, the Prizm system falls back to SNMP proxy if all the following conditions are met:

- The *Use SNMP Proxy If Available* option is checked when the network is defined.
- The AP is capable of SNMP proxy (requires Canopy System Release 8.0 or later).
- No routable IP address is associated with the SM.

The adjective “routable” in the phrase “routable IP address” means that the device’s IP address is a public IP address (as opposed to private IP address). The latter “non-routable” addresses consist of the following IP address blocks: 10/8, 169.254/16, 172.16/12, 192.168/16. While not technically correct, all other IP addresses can be assumed to be routable.

This SNMP Proxy feature is useful for an operator who wants to manage slave devices (SMs and BHSs) without defining or managing an IP address allocation scheme for SMs or BHSs. Note the operator must configure an IP address scheme for the less numerous AP, BHM, and CMM elements. Again, we stress that this feature requires Release 8.0 or later Canopy firmware.

Where SNMP proxy is used, it uses TCP/UDP Port 61002 on the AP and outbound communication from Prizm on that port must be enabled. No configuration steps are required on the master device, which is (if SNMP proxy-capable) always enabled for it. However, the following caveats apply to the slave devices (e.g. SMs):

- The slave device (e.g. SM) must be configured to send traps directly to Prizm, because the proxy in the master device does not forward traps.
- The community string for SNMP requests is that of the slave device.
- The SNMP subnet configuration (security) is configured such that the SM will respond to the IP address of the Prizm for SNMP requests. The private IP address (associated with the Ethernet port of the slave device) must not be in the same subnet space as Prizm, because if it is, then the slave device sends its responses to Prizm through that port, and those responses never arrive at the EMS.

Figure 21 shows a subset list of Canopy element attributes known to Prizm. All these attributes can be configured via Prizm in addition to directly through the element’s web interface as shown above. Additionally, VLAN attributes are configurable but not shown in Figure 21.

Perhaps the best way to configure perform attributes into SMs is to pre-define a service plan (SP). For example, there might be a SP for VoIP called locally “VoiceService”. Prizm allows this definition as the operating company wishes.

The procedure is explained in detail in the Prizm 2.0 User Guide Section 7.8.5 and summarized here. Please download the Prizm 2.0 User Guide from http://motorola.canopywireless.com/support/software.

Figure 22 shows the initial naming and categorizing of a new Service Plan.

These values then appear in the Define Configurations tab as shown in Figure 23.

BAM Parameter	PrizmEMS Attribute	Function in PrizmEMS
Authentication Key	Authentication Key	The hexadecimal string stored in both the database and the SM. This string is 32 or fewer characters, prepended with zeros if needed when the system reads it. The SM interface contains a toggle to **Use This Key** or **Use Default Key**.
Sustained Uplink Data Rate	Bandwidth Uplink Sustained Rate	The rate that the SM(s) are replenished with credits for transmission. This imposes no restriction on the uplink.
Sustained Downlink Data Rate	Bandwidth Downlink Sustained Rate	The rate at which the AP should be replenished with credits (tokens) for transmission to the SM(s). This imposes no restriction on the uplink.
Uplink Burst Allocation	Bandwidth Uplink Burst Allocation	The maximum amount of data to allow the SM(s) to transmit before being recharged at the **Sustained Uplink Data Rate** with credits to transmit more.
Downlink Burst Allocation	Bandwidth Downlink Burst Allocation	The maximum amount of data to allow the AP to transmit to the SM(s) before the AP is replenished at the **Sustained Downlink Data Rate** with transmission credits.
Allow Higher Bandwidth	Bandwidth Allow License Use	Toggles whether PrizmEMS should ask License Manager for floating Cap 2 licenses for the selected SM(s), to the extent that the licenses are available.
Low Priority Uplink CIR	Bandwidth Low Priority Uplink CIR	The committed information rate for transmissions from the selected SM(s) on the low-priority channel.
Low Priority Downlink CIR	Bandwidth Low Priority Downlink CIR	The committed information rate for AP transmissions to the selected SM(s) on the low-priority channel.
Is High Priority Channel Enabled	Bandwidth High Priority Channel Enable	Toggles whether the high-priority channel is enabled for all SMs that are configured to the particular service plan.
High Priority Uplink CIR	Bandwidth High Priority Uplink CIR	The committed information rate for transmissions from the selected SM(s) on the high-priority channel.
High Priority Downlink CIR	Bandwidth High Priority Downlink CIR	The committed information rate for AP transmissions to the selected SM(s) on the high-priority channel.
Is CIR Feature Enabled	*NONE*	

Figure 21. Prizm 2.0 priority settings screen capture.

Enter the attribute values desired into the items shown in Figure 23, thereby associating these values with the particular Service Plan. The values would be identical to those discussed above in the direct SM configuration.

The particulars in Figure 23 imply that the High Priority Channel is set to “Disable” but, of course, for VoIP, it needs to be set to “Enable”. Enter the high priority CIR values.

Save the changes. As a result, the window shown in Figure 24 appears prompting for confirmation. At this point, no set of SMs has been associated with the particular Service Plan. However, these new values could have been revisions to a Service Plan that already had associated SMs so the opportunity to update these SMs now is provided by the check box.

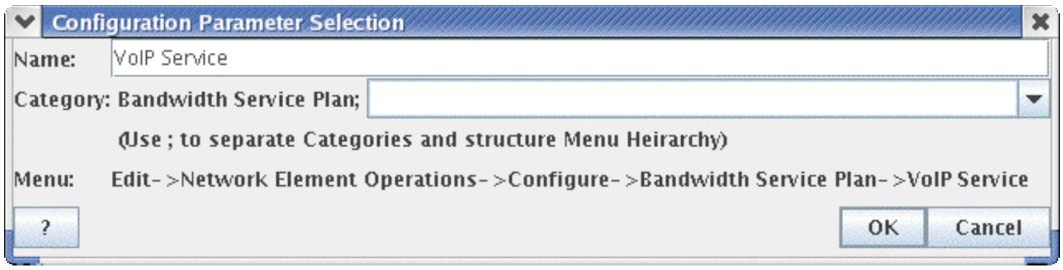


Figure 22. Example Configuration Parameter Selection for a Service Plan.

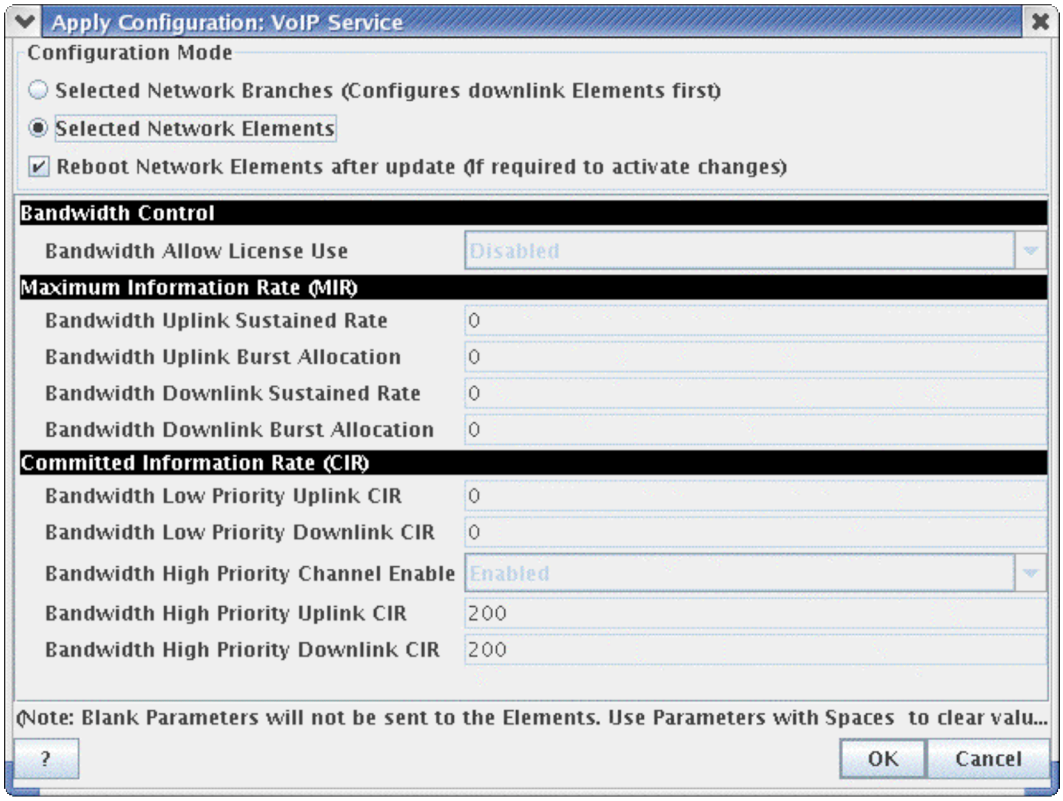


Figure 23. Prizm 2.0 configuration parameters in a Service Plan.

At this point, the Updating Confirmation window appears as shown in Figure 25. This means that the Service Plan is configured and is ready to be applied to selected Canopy network elements.

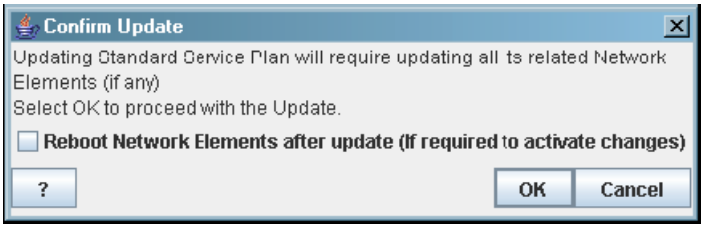


Figure 24. Example Confirm Update window.

At this point, the Service Plan can be applied to network elements by opening the Bandwidth Service Plan tab and selecting the particular Service Plan, say “VoIP Service”.

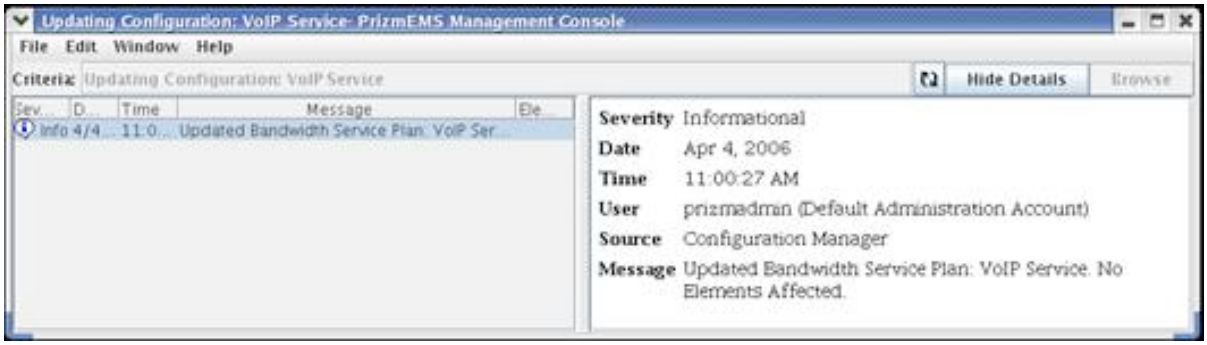


Figure 25. Configured Service Plan window.

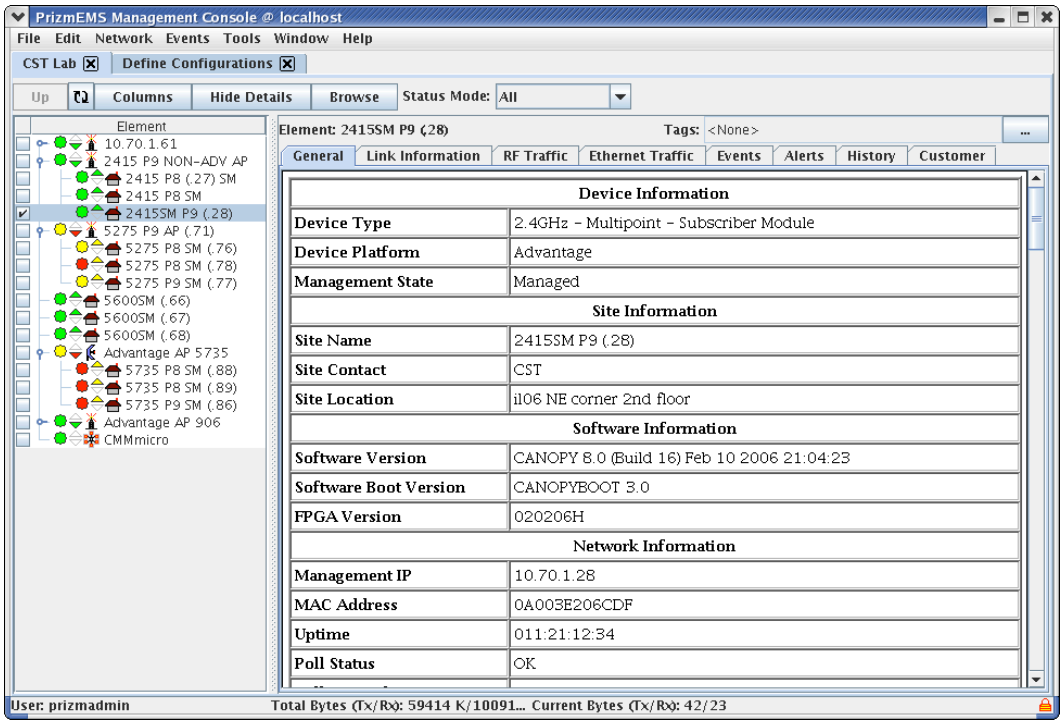


Figure 26. Selecting the elements to be assigned the Service Plan.

Figure 25 shows that the Service Plan may be applied to individual network elements or to a branch of network elements (according to the particular network's hierarchy). Setting the "Selected Network Elements" button will enable the enumeration of the particular elements, in context of those SM sproviding VoIP service.

Figure 26 shows the operator selecting a particular SM for assignment to the particular service plan.

If OK, then the window shown in Figure 27 appears, asking for confirmation before proceeding with the element updates. A "no" means that the Service Plan will not take

effect until the network elements are rebooted at a later time, say at a scheduled Maintenance Window.

If the “yes” button is selected, a window like that shown in Figure 28 appears, showing progress. This window is informational only and may be closed anytime.

This completes the configuration for VoIP services using Prizm 2.0.

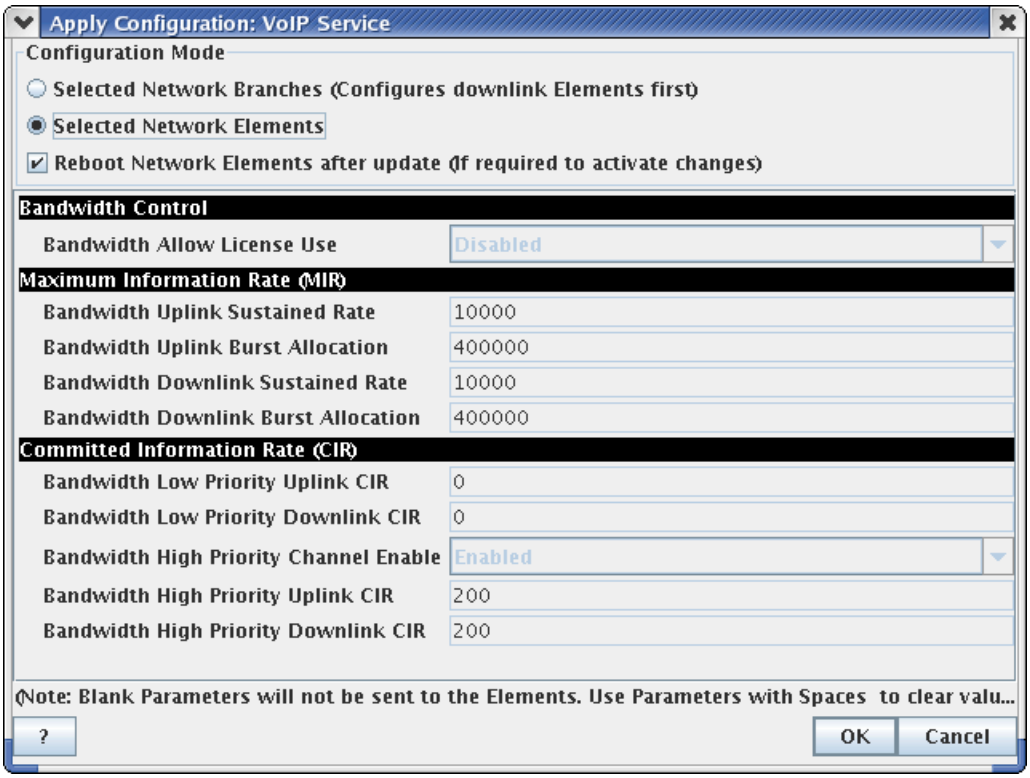


Figure 26. Example Apply Configuration window for a Service Plan.

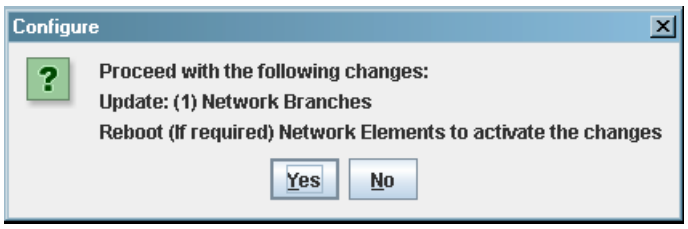


Figure 27. Example Configuration window.

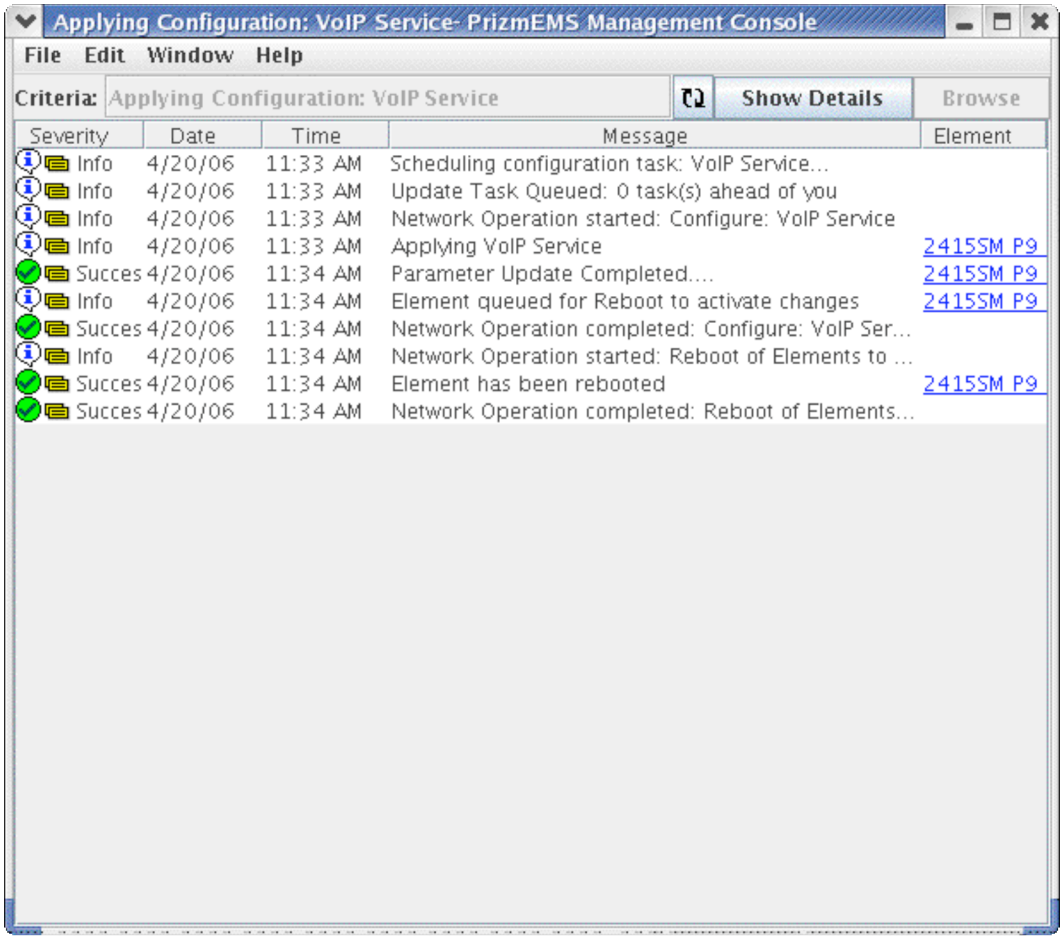


Figure 28. Example Applying Configuration window for a Service Plan.

6.0 Summary and Conclusion

In this Application Note, an overview has discussed many basic aspects of deploying Canopy Advantage APs with Canopy SMs, Advantage SMs, and Lite SMs for VoIP services. In particular, the VoIP business scenarios open to existing Canopy operators were highlighted.

Should a Canopy operator wish to become an interconnected VoIP service provider, an FCC order applies, as stated.

In that vein, VoIP CPE elements were described and illustrated. Particular stress is placed on the Analog Terminal Adapter (ATA) and its network position in regard to the Canopy SM. In addition, the network-based VoIP Media Gateway and VoIP signaling were described.

The concepts of specializing, via configuration, Canopy's performance in the VoIP context were discussed with illustrated examples, reviewed in Figure 29.

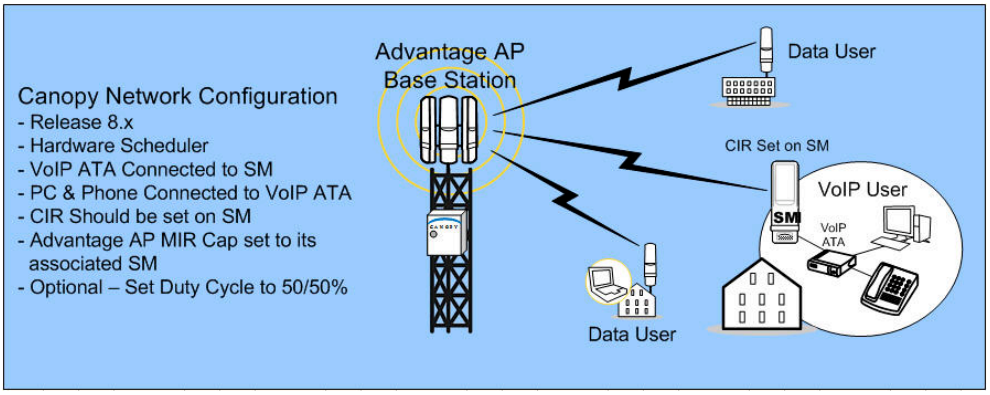


Figure 29 Summary illustration of Canopy in VoIP service context.

Additional Resources

Canopy provides two additional resources where you can raise questions and find answers:

- Canopy User Community at http://motorola.canopywireless.com/support/community.
  This resource facilitates communication with other users and with authorized Canopy experts. Available forums include General Discussion, Network Monitoring Tools, and Suggestions.
- Canopy Knowledge Base at http://motorola.canopywireless.com/support/knowledge

  This resource facilitates exploration and searches, provides recommendations, and describes tools. Available categories include
  - General (Answers to general questions provide an overview of the Canopy system.)
  - Product Alerts
  - Helpful Hints
  - FAQs (frequently asked questions)
  - Hardware Support
  - Software Support
  - Tools

Sending Feedback

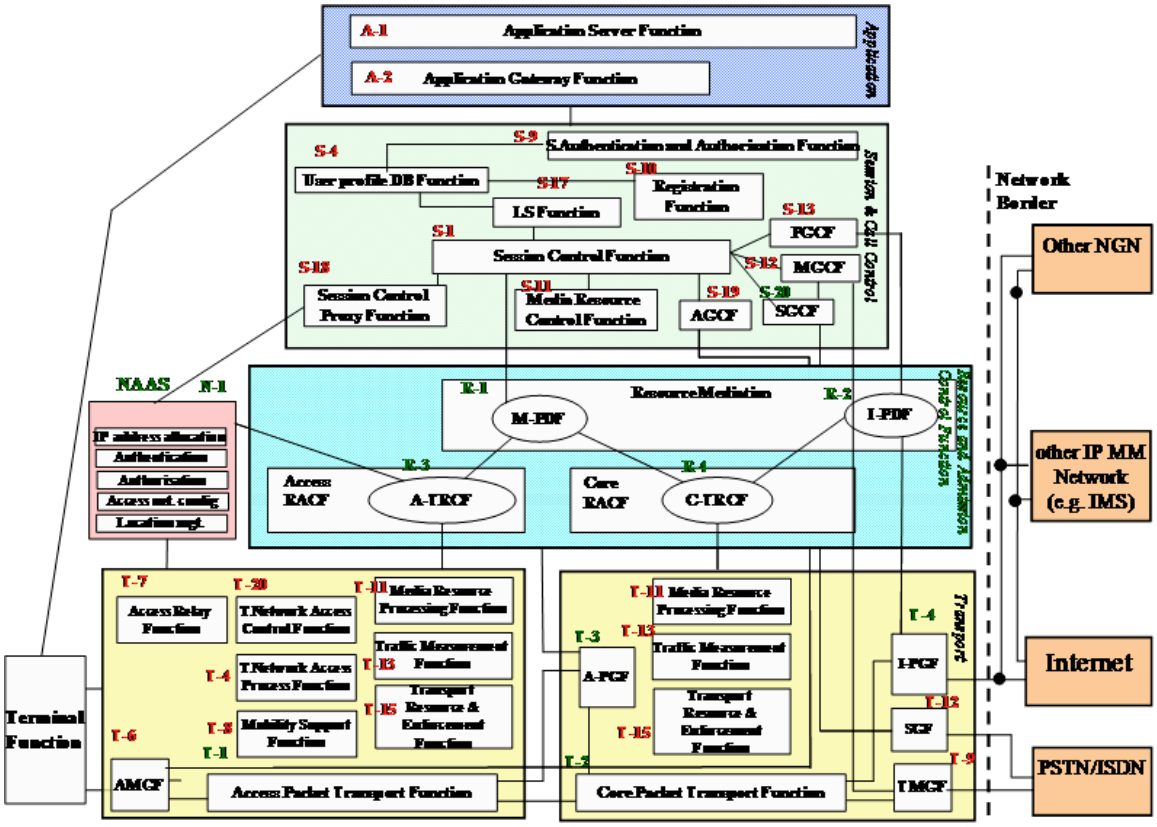
We welcome your feedback on Canopy system documentation. This includes feedback on the structure, content, accuracy, or completeness of our documents, and any other comments you have. Please send your comments to technical-documentation@canopywireless.com.

Appendix A. ITU's Next Generation Network

For completeness, this is the International Telecommunications Unit Next Generation Network definition. Source: ITU-T Rec. Y.2001:

A packet-based network able to provide telecommunication services and able to make use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies.

It enables unfettered access for users to networks and to competing service providers and/or services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.



Appendix B. Selected Useful Reference Sites

www.voipconsortium.com

www.wirelessvoip.org

www.ipphonedirectory.net

www.myvoipprovider.com

www.internetphonesoftware.com

http://www.tmcnet.com/scripts/magsub/free-subscriptions.aspx

Voip-finder.com

Voipreview.org

www.pulver.com

www.pulver.com/products/sip/

www.voipsupply.com

Appendix C. Glossary of Terms

SOHO	Small Office, Home Office
ATA	Analog Terminal Adapter
BAM	Bandwidth and Authentication Manager
BWA	Broadband Wireless Access
CDMA	Code Division Multiple Access
CIR	Committed Information Rate
CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
E911	Enhanced 911
EFCN	Explicit Forward Congestion Notification
FCC	Federal Communications Commission
GSM	Global System for Mobile communications
GW	Gateway
HTTPS	HyperText Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IM	Instant Messenger
ITU	International Telecommunications Union
MAC Address	Media Access Control Address
MIR	Maximum Information Rate
NAT	Network Address Translation
PHB	Per Hop Behavior
PMP	Point-to-MultiPoint
PSTN	Public Switched Telephone Network
PTP	Point-to-Point
QoS	Quality of Service

RJ	Registered Jack
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
STUN	Simple Traversal of UDP through NAT
ToS	Type of Service
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VoIP	Voice over IP
WiFi	Wireless Fidelity
WISP	Wireless Internet Service Provider
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol