State of Wisconsin

Division of Enterprise Technology

BadgerNet Converged Network (BCN)

Video Service Offering Description (SOD)

Document Contents

Introduction

BadgerNet Converged Network (BCN) video services offer the opportunity for users in separate facilities to have a face-to-face meeting as if they were in the same conference room. The reliability of the BadgerNet Converged Network, as well as the video equipment needed to make the conference call, provides the end-user with an "easy to use" system that works every time. Additionally, video service offers the opportunity to bridge more than two sites together in a single call. BCN videoconferences routinely include four sites but the bridge can include as many sites as the Multi-Conference Unit (MCU) has ports (hundreds). Coordination of multi-site calls is the responsibility of the BCN Scheduling Office making it easy for anyone to arrange for and participate in multi-site conference. Network features include the capability of participating in calls with users from other agencies both within and outside of BCN.

Standard Definition Video Service

Standard Definition Service Overview

The BadgerNet Converged Network (BCN) is intentionally designed to separate end-user communities into logically separate networks called Virtual Private Networks (VPN). The design addresses the end-user community's need to keep its data private and secure. As a rule, most state government agencies require their traffic to be separate and secure from users outside the system (e.g., hackers). Logically separating traffic in a Virtual Private Network provides security but complicates video connections between VPNs.

BCN offers a turnkey solution for video users called Managed Video in which all users have membership in the same VPN. Membership in a common VPN allows any site to connect to any other site within that VPN. BCN also recognizes the need within the user community to offer the same network Quality of Service (QoS) without all the features associated with Managed Video. The initial intent of BCN's High-Priority, Low-Latency (HPLL) service was to allow end-users to purchase and manage their own video codecs or VoIP systems.

Users who have purchased their own codecs may discover they have the need to expand beyond making point-to-point connections or that they need to connect to a site within BCN but not within their Virtual Private Network (VPN). To accommodate multiple sites in a session (any number greater than two), a Multi-Conference Unit (MCU), also known as a video bridge, must be used. BadgerNet has multiple MCUs with significant port capacity available for users of BCN Video Bridging service. Any session with three or more end-sites can use the bridge under the guidelines established for service by the Department of Administration.

The BCN Video Bridging Service also offers another significant feature; the ability to connect to any other BCN site regardless of VPN membership. The network is designed to insulate user communities from each other by assigning each site to a Virtual Private Network (VPN). For example, the Department of Justice VPN will not allow traffic to co-mingle with traffic from the Education VPN. This design allows user communities to be sure their traffic is virtually separated from and independent of other VPN traffic. While the VPN is an excellent way to separate traffic, it represents a barrier to video users who want to communicate even though they may be in different VPNs.

BCN Video Bridging Service allows video users in unique VPNs to connect to each other either on a point-to-point basis or on a multi-point basis. They may do this by connecting directly to each other or using the BadgerNet MCUs.

To summarize, BCN Video Bridging Service users can utilize the BadgerNet MCUs by:

- Hosting or attending sessions within their VPN
- Hosting or attending with a mix of HPLL sites, HPLL with BCN Video Bridging Service or standard WAN customers.
- Use the BCN MCU to host or attend H.323 or H.320 sessions

Customer Configuration

Customers who provide their own codecs to connect to BCN using HPLL or WAN service must use a hardware based, H.323 compliant and non-proprietary device. Service is not guaranteed until BCN Engineering reviews the codec make, model and version of software to insure compatibility with the BCN MCUs. The customer must also be willing to work with BCN to establish timelines for codec implementation and testing before the service is available for use. BCN Engineering will work with the customer to review responsibilities, service demarcation and network configuration (as it relates to BCN). Order, delivery and installation of the codecs along with LAN modifications are the responsibility of the customer.

The customer must also be willing to establish a formal test session with the BCN Network Management Center. The test will be formally scheduled on the web portal like any other new service within BCN. The site will not be “in-service” until the tests are completed and trouble tickets can officially be opened against that service after that time.

Network configuration

Changes to BCN to allow BCN Video Bridging Service to function properly include:

- Configuration of the BCN firewall.
- Configuration of the BCN PE router
- Configuration of the BCN Converged Management Application (CMA)

High-Priority, Low-Latency Video Service

This section provides the detail necessary to connect, configure, test and turn-up BadgerNet's High-Priority, Low-Latency (HPLL) service and how to successfully complete videoconferences. Now that you have already identified an application that is suited for BadgerNet's HPLL service, we anticipate you'll ask several additional questions regarding the service. The format below attempts to answer the more commonly asked questions regarding HPLL service:

1. What kind of equipment do I need and how do I connect it to BadgerNet's HPLL service?
2. Who configures my equipment with new IP addresses and any application specific configuration?
3. Once I'm configured and connected, how do I test my equipment?
4. After I've verified that all my sites are accessible, how can you help me place test calls?
5. Now that the basic testing is done, how can I establish a video sessions with multiple sites (3 or more)? Which video scheduling office do I call and when?

There are five sections listed below to assist you. Those sections are Physical Connectivity, Configuration, Network Testing, Application Testing, and Video Session testing.

1. Physical Connectivity

You have already determined that you have a latency sensitive (e.g. voice or video) application that is best suited for BadgerNet's HPLL service. Physically connecting to BadgerNet is quite easy, but before you extend an Ethernet cable from your equipment to the BadgerNet Customer Edge (CE) device, which could be a router or switch, there are several items to be reviewed.

Recommended connectivity

BadgerNet recommends that you use a device capable of configuring an IP address that BadgerNet will issue to you. This device could be a video codec, a Layer 3 switch or a router. Regardless of the device chosen, you'll need to configure the BadgerNet IP address on the WAN interface of that device along with a default gateway address, also issued by BadgerNet. These addresses provide you the path to connect to other users in the HPLL Virtual Private Network (VPN).

Traffic shaping

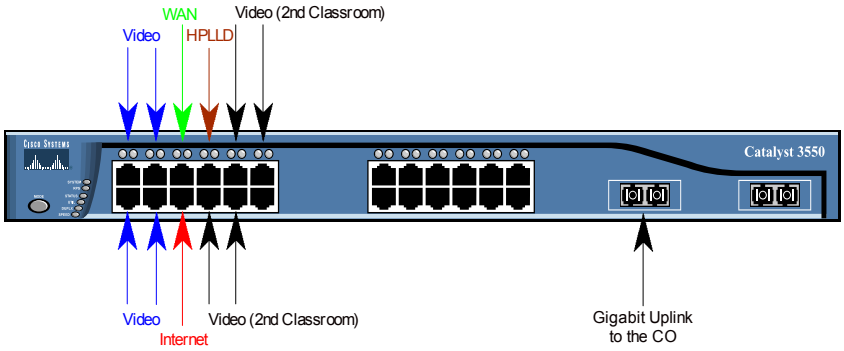
BadgerNet strongly recommends that the device connecting to the BCN Ethernet port have the capability of shaping traffic to the specific increment of bandwidth purchased. Without the ability to shape traffic, periods of burst will likely exceed the increment of bandwidth purchased and packets will be discarded. As is often the case, when the number of discarded packets increase, the application performs poorly and the end-users experience "slow" or "bad" sessions.

Connecting to BCN Customer Edge (CE)

BadgerNet service providers deploy a number of different devices at the customer edge (CE). Sometimes the device is a Layer 3 router, sometimes a Layer 2 switch. Regardless of the device, port 7 is typically allocated for HPLL service. It's possible to have a two-port router as your CE device, in which case either port could be configured for WAN or HPLL service. After you place your order, your CE port assigned will be verified and shared with you by the BadgerNet Lead Engineer.

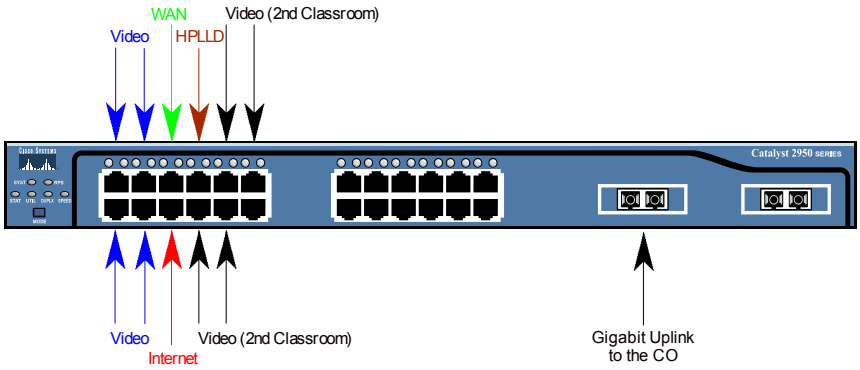
Some examples are listed below, but this is not intended to be a comprehensive list. In the event you cannot determine which port to use, or you do not have a link light when connected to the correct port, please call the BadgerNet Network Management Center (NMC) at 1-888-955-2638. They can access your CE device remotely and assist in establishing connectivity.

Catalyst 3550-24 CE



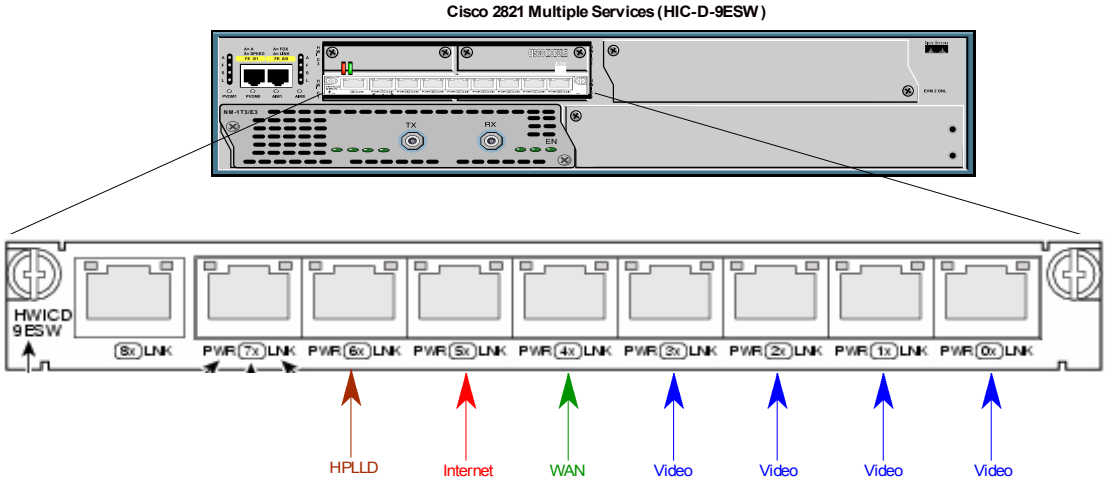
Port Description	#	Service
FastEthernet	0/1	Video
FastEthernet	0/2	Video
FastEthernet	0/3	Video
FastEthernet	0/4	Video
FastEthernet	0/5	WAN
FastEthernet	0/6	Internet
FastEthernet	0/7	HPLL
FastEthernet	0/8	Video (2nd Classroom)
FastEthernet	0/9	Video (2nd Classroom)
FastEthernet	0/10	Video (2nd Classroom)
FastEthernet	0/11	Video (2nd Classroom)
GigabitEthernet	0/1	CE/PE Uplink

Catalyst 2950 CE



Port Description	#	Service
FastEthernet	0/1	Video
FastEthernet	0/2	Video
FastEthernet	0/3	Video
FastEthernet	0/4	Video
FastEthernet	0/5	WAN
FastEthernet	0/6	Internet
FastEthernet	0/7	HPLL
FastEthernet	0/8	Video (2nd Classroom)
FastEthernet	0/9	Video (2nd Classroom)
FastEthernet	0/10	Video (2nd Classroom)
FastEthernet	0/11	Video (2nd Classroom)
GigabitEthernet	0/1	CE/PE Uplink

Cisco 2821 with the 9 port Ethernet HWIC



Port Description	#	Service
FastEthernet	1/0	Video
FastEthernet	1/1	Video
FastEthernet	1/2	Video
FastEthernet	1/3	Video
FastEthernet	1/4	WAN
FastEthernet	1/5	Internet
FastEthernet	1/6	HPLL
Serial	3/0	

2. *Configuration*

The interface to BadgerNet is an Ethernet port on a router or switch provided by a local service provider. The router, switch, codec or VoIP key system that you connect to BCN is a device that you must purchase based on your application requirements. The configuration for that device(s) is also a customer's responsibility. BadgerNet engineering staff, specifically the BCN Lead Engineer, is available to assist you or your vendor when you configure those devices – and to assist in troubleshooting if necessary. However, it must be clear that purchasing, installing, configuring and maintaining those devices connecting to BadgerNet are the responsibility of the customer.

IP Addresses

The addresses of your internal network can remain as you currently have them, but the device that interfaces to the BadgerNet Ethernet port must be modified. The table shown below includes a column called “WAN IP Address” and will be populated with an RFC 1918 address assigned by the BadgerNet engineering team. Assuming you have a Layer 3 device, the address in that column must be configured on the WAN interface of the device connecting to the BadgerNet Ethernet port.

Default Gateway

You may also have to modify the configuration of your Layer 3 device to reflect a new default gateway. Note that the head-end location is assumed to have an ISP connection, and the default gateway IP address is provided by your ISP. The head-end router configuration needs to include an additional route to send traffic back to your remote sites. The default gateway for the remote sites are provided in the column of the same name shown below.

Network-VPN	Position	Site ID	School Name	Due date	WAN IP Address	Default Gateway	Additional Routes
VPN Name	Head-End		Site 1	TBD	10.x.x.x	ISP	10.x.x.x
VPN Name	Remote		Site 2	TBD	10.x.x.x	10.x.x.x	N/A
VPN Name	Remote		Site 3	TBD	10.x.x.x	10.x.x.x	N/A

3. *Network Testing*

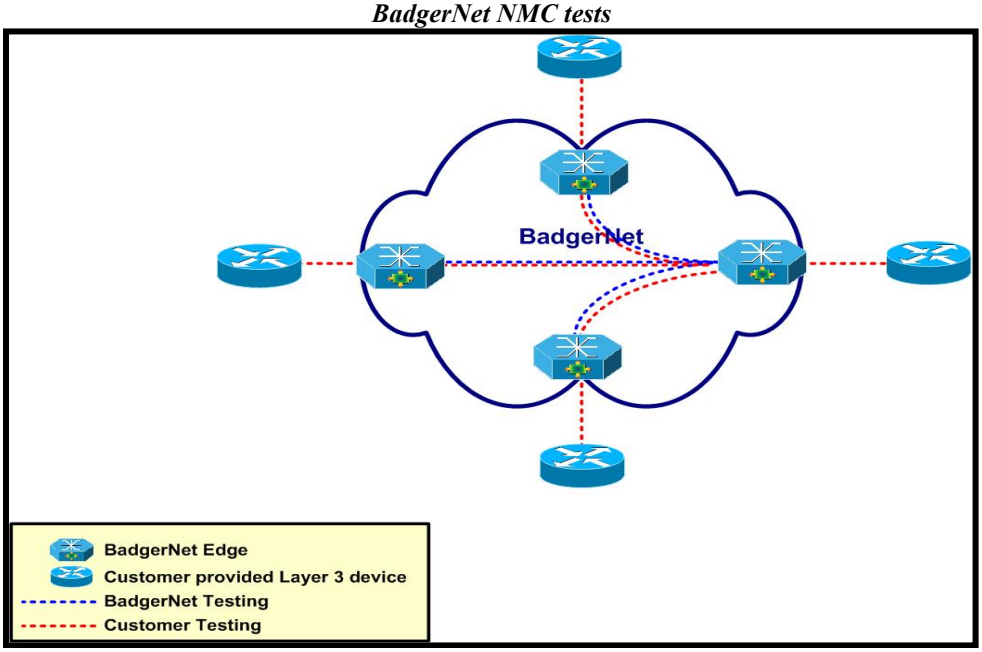
After your equipment is connected to the network, usually on Ethernet port 7, and configured using the addressing information provided by the BadgerNet Lead Engineer, you are ready for testing. Before you begin, verify you have a link light (usually a steadily lit green LED on the port). This confirms you have an active port on the CE device and usually means the network configuration is complete. If you do not have a light, verify you have the proper Ethernet cable. The table below will help you determine which Ethernet cable type you need

Customer device	Ethernet Cable	BCN CE
Layer 2 (switch)	Cross Over	Layer 2 (switch)
Layer 2 (switch)	Straight through	Layer 3 (router)
Layer 3 (router)	Straight through	Layer 2 (switch)
Layer 3 (router)	Cross Over	Layer 3 (router)

After you've connected your device to the BadgerNet CE, call the BadgerNet Network Management Center (NMC) to begin your testing. You can reach them at 888-955-2638. Any of the engineers who answer your call will be able to perform a set of tests with you to verify network connectivity. Provide the NMC engineer with your site ID number or site name.

Once the engineer has reviewed the IP address information for your sites, the engineer will telnet to the BadgerNet CE at your head-end and verify you are physically connected. Next, a test (ping) will be conducted to verify the path from your remote location successfully traverse the network to your head-end or main location. The diagram below depicts the test the NMC will run (shown in blue).

BadgerNet NMC tests



4. Application Testing

Now that you have completed a connectivity test with the BadgerNet NMC, you are ready to conduct your application testing. Consult your vendor to determine the best strategy to fully test your application. Only you and your equipment vendor will know enough about the equipment you've purchased and configured to properly test the application.

If for some reason the application tests do not pass to your satisfaction, call the BadgerNet Network Management Center (NMC) at 888-955-2638. The engineers at the help desk are willing to assist you in determining why the application does not work. We also recommend that you contact the equipment manufacturer to assist in the troubleshooting. BadgerNet engineers spend most of their time working within BadgerNet and do not have expertise that the

equipment manufacture does. It has been successful to engage both when addressing a stubborn problem.

5. *Video Application Testing*

While it may sound intuitive, the test for a video session is a video call that can be placed and received with good quality results. Regardless of the bandwidth available, your HPLL video test calls should proceed without your video frames freezing, losing any portion of video picture, limited blocking and tiling of the image, and free from hissing, popping or clipping in the audio. If any of these conditions exist, a troubleshooting session ought to ensue.

Point to Point Calling

After you have your codec installed and know both your IP address and the address of a codec within your virtual private network (VPN), you can place a call to that codec by following the instructions provided by your video codec manufacturer. Like a telephone call, the network will route the call to the IP address of the codec at the other end of your VPN. Make sure someone is available at the remote location to answer the your incoming call. You may have the option of enabling an auto-answer feature to test remotely without assistance.

You can place and receive a call to any codec within the HPLL VPN as long as you know the IP address of that codec. Other users can place a call to you, but only if they know the address of YOUR codec. You will need to determine who you share your codec address with. We recommend only sharing with users you intend to call. You can only connect directly with users in the BadgerNet HPLL VPN. Calls outside the VPN to a BadgerNet managed video user or the Internet must go through one of the bridges available to the HPLL customers.

BadgerNet Bridges

If you want to participate in a session with more than two sites, you need to place a call to one of the three bridges, also referred to as a multipoint control unit (MCU), available for this use. There is one bridge in each LATA to reduce overall trip latency. Generally, the BadgerNet managed video sites will schedule their sessions with the BCN scheduling office. Once you've tested your site to the BadgerNet MCU, you'll be added to the reservation and automatically be included when the session starts.

Before you join a session with a BadgerNet managed classroom, a test session is required to validate your site. If successful, the individual test only runs for 10 minutes and you do not need to be present for it (although we strongly recommend you be available). To schedule your test session, you will need to coordinate a date and time with the BadgerNet Network Management Center (NMC) at 888-955-2638. Before you call, have your codec IP addresses for each

codec to be tested, the amount of bandwidth you purchased for each site tested, and manufacture and model of the codecs at each location.

High-Definition Video Service

High-Definition Video Service Overview

The BadgerNet Converged Network transitioned from Standard Definition Video Service to High-Definition Video Service in the spring of 2012. The infrastructure supporting BCN video completely changed to support High-Definition videoconferences. Standard Definition service and features (such as traditional 1x3 video calls, off-net ISDN calls, Polycom VSX 8000 codec support) will continue until no longer necessary, or until the end of the contract, whichever comes first. However, the change in the network to support HD is significant and required the transition or retirement of nearly every component of Standard Definition infrastructure.

The outline below provides the components and functionality of the HD infrastructure. It was a design goal to include all existing functionality and add a few new options. Accommodating legacy features and new functionality requires a significantly different design.

Service Components

Multipoint Control Units (MCU)

A multipoint control unit allows two or more video end-points to bridge together on a call. BadgerNet's Video Network includes four (4) Multipoint Control Units with a significant amount of capacity to accommodate standard and high-definition end-points in a single call. The MCUs are physically and logically diverse for redundancy and have additional expansion capacity.

Converged Management Application (CMA)

CMA is a management tool used by AT&T to provision, trouble-shoot and control call flow with the BadgerNet video network. All video devices, standard-definition codecs, high-definition codecs, MCUs, gateways, etc. are registered to CMA. Devices in the network can be tracked and call flow can be defined as a standard procedure with CMA. As a tool, CMA is not available for use to consortiums or individual sites.

Video Border Proxies (VBP)

Video Border Proxies (VBPs) are a specific type of firewall and allow certain types of calls to enter or exit BCN. There are two types of VBPs in the BCN Video network; one specifically for BCN Remote Video Access video end-points to use, and another VBP for all other types of users and

calls. Introduction of the VBPs now allows certain types of calls to leave the network without using the MCU as a gateway.

Polycom RSS

Polycom RSS Service is currently not available.

Polycom RSS is a product that allows recording of videoconferences. The RSS server can be added to a video reservation before or during a call to capture both the people and content portions of an active meeting. Polycom's integration of RSS allows it to be "silently" included, so a blank site does not appear in the viewing window of a multipoint conference.

System Operation

BCN HD video service replicates the functionality of the BCN SD environment, but infrastructure components changed significantly. Some of the changes are:

- Only one codec per site, which operates a 2 Mbps video steam
- A single HD student monitor and a single HD teacher monitor (content monitors optional)
- HD cameras within the classroom are required
- Upgraded video router and cabling
- All multi-site calls connect to the MCU (today 1x3 do not use the MCU)
- All off-net calls go through Video Border Proxy instead of the MCU

Basic Operation

At power-up, each codec is programmed to register to the BCN Gatekeeper (CMA) which validates its license and availability. Before it joins a multi-site conference, BCN scheduling software verifies with CMA that the codec for this session is licensed and available, then launches a request through CMA to connect that codec to the MCU. Since each site only has a single video stream, the MCU provides the viewing format to the HD monitor at the remote site. The HD monitor could be in quad split if only four sites are in the call, or it could be in Hollywood squares mode, lecture mode, etc. These modes are available in the SD environment today. Once the call is in process, the same functionality from a classroom control perspective is available.

Call Matrix

BCN will support a mixture of call types as the end-users transition from SD to HD service. The new HD video components support SD service, so an end-user site that chooses not to upgrade will have support through the life

of the contract. The call matrix below shows services and functionality in the HD environment.

Service or Function	HPLL	RVA	HPLL VB	Managed Video
Participate in a bridged call	Yes	Yes	Yes	Yes
Scheduling Office support	Limited	Limited	Limited	Yes
NMC Support	Limited	Limited	Limited	Yes
Codec included with service	No	No	No	Yes
Access to Renovo	No	No	Yes	Yes
Register to CMA	No	Yes	Yes	Yes
"Host" a bridge call	No	No	Yes	Yes
Max MCU connect speed	1 M	384K	1 M	1 M
Direct Off-Net calling	No	No	Yes	Yes
Pt-Pt with E.164 address	No	No	Yes	Yes

Video Bridging Service Description

The BadgerNet Converged Network (BCN) is intentionally designed to separate end-user communities into logically separate networks called Virtual Private Networks (VPN). The design addresses the end-user community's need to keep their data private and secure. As a rule, most state government agencies require their traffic to be separate and secure from users outside the system (e.g. hackers). Logically separating traffic in a Virtual Private Network provides security but complicates video connections between VPNs.

BCN offers a turnkey solution for video users called Managed Video in which all users have membership in the same VPN as well as access to a number of features previously exclusive to Managed Video. Membership in a common VPN allows any site to connect to any site. BCN also recognized the need within the user community to offer the same network Quality of Service (QoS) without all the features associated with Managed Video. The initial intent of BCN's High-Priority, Low-Latency (HPLL) service was to allow end-users to purchase their own video codecs or VoIP systems.

Users who have purchased their own codecs may discover they have the need to expand beyond making point-to-point connections or that they need to connect to a site within BCN but not within their Virtual Private Network (VPN). To accommodate multiple sites in a session (any number greater than two), a Multi-Conference Unit, also known as a video bridge, must be used. BadgerNet has three MCUs with significant port capacity available for users of BCN Video Bridging service. Any session with three or more end-sites can use the bridge under the guidelines established for service by the Department of Administration.

The BCN Video Bridging Service also offers another significant feature; the ability to connect to any other BCN site regardless of VPN membership. The network is designed to insulate user communities from each other by assigning each site to Virtual Private Network (VPN). For example, the Department of Justice VPN will not allow traffic to co-mingle with traffic from the Education VPN. This design allows user communities to be sure their traffic is virtually separated from and is independent of other VPN traffic. While the VPN is an excellent way to separate traffic, it represents a barrier to video users who want to communicate even though they may be in different VPNs.

BCN Video Bridging Service allows video users in unique VPNs to connect to each other either on a point-to-point basis or on a multi-point basis. They may do this by connecting directly to each other or using the BadgerNet MCUs.

To summarize, BCN Video Bridging Service users can utilize the BadgerNet MCUs by:

- Hosting or attending sessions within their VPN
- Hosting or attending with a mix of HPLL sites, HPLL with BCN Video Bridging Service or standard WAN customers.
- Use the BCN MCU to host or attend H.323 or H.320 sessions

Customer Configuration

Customers who provide their own codecs to connect to BCN using HPLL or WAN service must use a hardware based, H.323 compliant and non-proprietary device. Service is not guaranteed until BCN Engineering reviews the codec make, model and version of software to insure compatibility with the BCN MCUs. The customer must also be willing to work with BCN to establish timelines for codec implementation and testing before the service is available for use. BCN Engineering will work with the customer to review responsibilities, service demarcation and network configuration (as it relates to BCN). Order, delivery and installation of the codecs along with LAN modifications are the responsibility of the customer.

The customer must also be willing to establish a formal test session with the BCN Network Management Center. The test will be formally scheduled on the web portal like any other new service within BCN. The site will not be “in-

service" until the tests are completed and trouble tickets can officially be opened against that service after that time.

Network configuration

Changes to BCN to allow BCN Video Bridging Service to function properly include:

- Configuration of the BCN firewall.
- Configuration of the BCN PE router
- Configuration of the BCN Converged Management Application (CMA)

Contact Information

Group or Title	Contact Name	Contact Information
Network Management Center		888-955-2638
BCN Scheduling Office		800-243-9482 ext. 5236
BCN Lead Engineer	Chris Alberts	calberts@mca-network.com
TEACH Wisconsin	Matt Yeakey	teach@wisconsin.gov
Department of Administration	Connie Bandt	DOADETTelecomAdministration@wisconsin.gov