

Formatted: Left: 1.25", Right: 1.25"

State of Wisconsin

BadgerNet Converged Network (BCN)

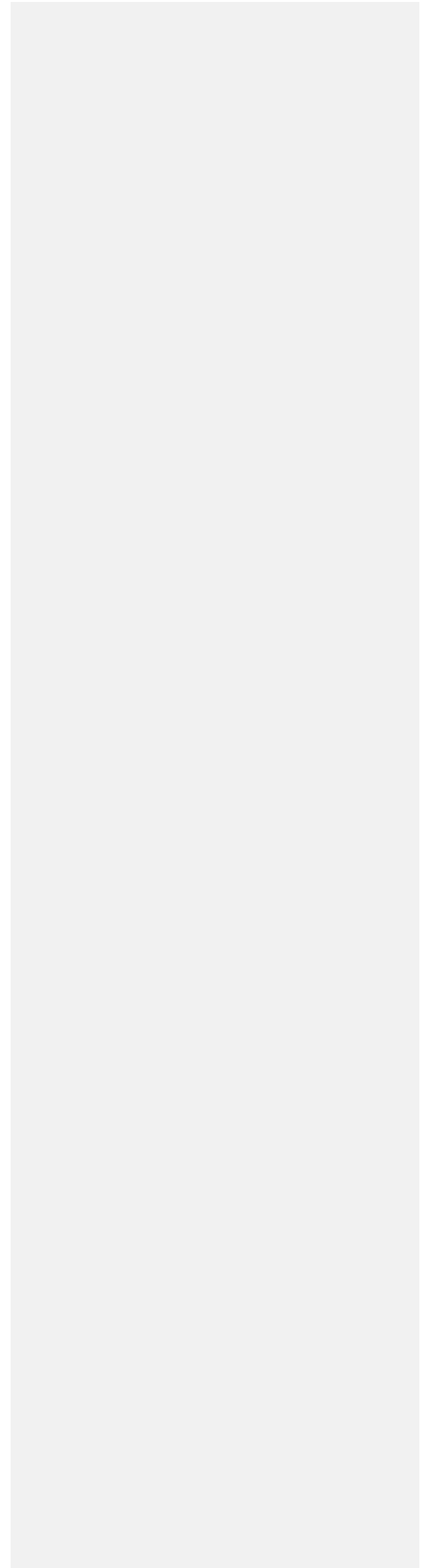
Video Service Offering Description (SoD)



Document Contents

Standard Definition Video Service	4
Standard Definition Service Overview	4
Customer Configuration.....	5
Network configuration	5
<i>Installation and configuration of the BCN firewalls.....</i>	<i>5</i>
<i>MCU Configuration.....</i>	<i>6</i>
Service Parameters.....	6
High-Priority, Low-Latency Video Service	6
1. Physical Connectivity.....	7
<i>Recommended connectivity.....</i>	<i>7</i>
<i>Traffic shaping.....</i>	<i>7</i>
<i>Connecting to BCN Customer Edge (CE).....</i>	<i>7</i>
<i>Catalyst 3550-24 CE.....</i>	<i>8</i>
<i>Catalyst 2950 CE.....</i>	<i>8</i>
<i>Cisco 2821 with the 9 port Ethernet HWIC.....</i>	<i>9</i>
2. Configuration	9
<i>IP Addresses.....</i>	<i>9</i>
<i>Default Gateway.....</i>	<i>10</i>
3. Network Testing.....	10
4. Application Testing.....	11
<i>Video Application Testing.....</i>	<i>11</i>
5. Video Application Testing.....	12
<i>Point to Point Calling.....</i>	<i>12</i>
<i>Multi-point calling (with a BadgerNet classroom).....</i>	<i>13</i>
<i>Multi-point calling (without a BadgerNet classroom).....</i>	<i>13</i>
High-Definition Video Service	13
High-Definition Video Service Overview.....	13
Service Components.....	14
<i>MCU.....</i>	<i>14</i>
<i>Video Codec.....</i>	<i>14</i>
<i>Gatekeeper.....</i>	<i>14</i>
<i>Video Border Proxy (VBP).....</i>	<i>15</i>
<i>Recording Video Sessions.....</i>	<i>15</i>
<i>Renovo Scheduling Software.....</i>	<i>15</i>
<i>Dascom DL Navigator/DL Hub.....</i>	<i>16</i>
System Operation	16
<i>Basic Operation.....</i>	<i>16</i>
<i>Call Matrix.....</i>	<i>16</i>
Video Bridging Service Description	17
Customer Configuration.....	18
Network configuration	19
<i>Installation and configuration of the BCN firewalls.....</i>	<i>19</i>

<i>MCU Configuration</i>	19
Service Parameters.....	19



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 calls. 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, 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 within that VPN. BCN also recognizes the need (Clarify the highlighted portion above) 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 “savvy” end-users to purchase and manage their own and manage their video codecs or VoIP systems. If scheduling or access to an MCU were a requirement for effective use, the end-user would have to purchase them independently. The BCN Video Bridging Service changes that.

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

Formatted: Not Highlight

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. This feature should be attractive to those currently using the Internet and paying usage charges to connect to another BCN site in a different VPN. The Department of Administration has relaxed its policy allowing any combination of Managed Video, HPLL or HPLL with BCN Video Bridging Service to connect to a session 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 purchase BCN Video Bridging Service provide their own codecs, which must be hardware based, H.323 compliant and non-proprietary. 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 officially tested and billed. BCN Engineering will work with the customer to review responsibilities, service demarcation and network configuration (as it relates to BCN). If the codec is not supported, the customer can chose to cancel the service or purchase a different codec. 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. Billing will commence on the day the test is scheduled in the web portal.

Network configuration

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

Installation and configuration of the BCN firewalls

- Configuration of the Cisco ASA 5520s firewall.
- AT&T will purchase the firewalls and take responsibility for physically installing and connecting them to the [Provider Edge \(PE\) router](#) (~~need an explanation of what PE stands for? A lay person might not know~~)
- The firewalls will be installed in administrative space in the Madison 11 CO (MDSNW111)
- Initial configuration may be completed by AT&T and be maintained by the BadgerNet Management Network Center –NMC through a contract service agreement.
- Configuration of the PE device will be completed by the NMC.

MCU Configuration

- The BCN MCU's already has appropriate card capacity – no changes to it are required. If additional port capacity is needed, new IP-48 card(s) can be purchased by the DOA.

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 ~~video conferences~~ [videoconferences](#). Now that you have already identified an application that is suited for ~~BadgerNet's HPLL~~ [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.

Formatted: Indent: Left: 0.5"

Recommended connectivity

BadgerNet recommends that you use a device capable of configuring an IP address which 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.

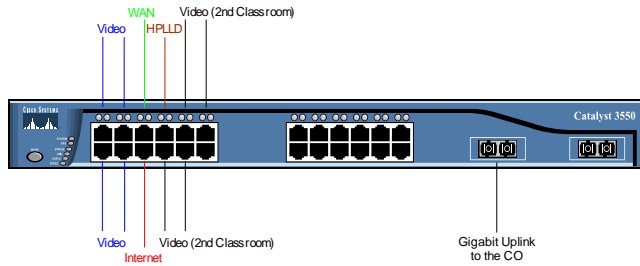
Connecting to BCN Customer Edge (CE)

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.

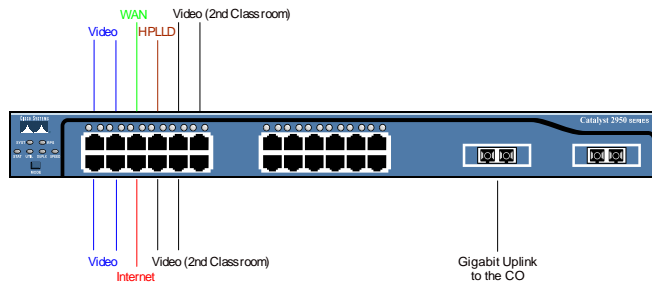
Formatted: Indent: Left: 0.5"

Catalyst 3550-24 CE



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	HPLLD
FastEthernet	0/8	Video (2 nd Classroom)
FastEthernet	0/9	Video (2 nd Classroom)
FastEthernet	0/10	Video (2 nd Classroom)
FastEthernet	0/11	Video (2 nd Classroom)
GigabitEthernet	0/12	CE/PE Uplink

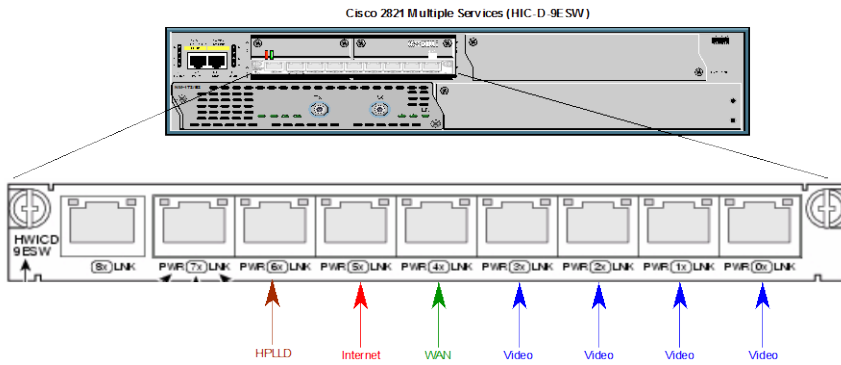
Catalyst 2950 CE



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	HPLLD
FastEthernet	0/8	Video (2 nd Classroom)
FastEthernet	0/9	Video (2 nd Classroom)
FastEthernet	0/10	Video (2 nd Classroom)
FastEthernet	0/11	Video (2 nd Classroom)

GigabitEthernet	0/1	CE/PE Uplink
-----------------	-----	--------------

Cisco 2821 with the 9 port Ethernet HWIC



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.

Formatted: Indent: Left: 0.5"

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

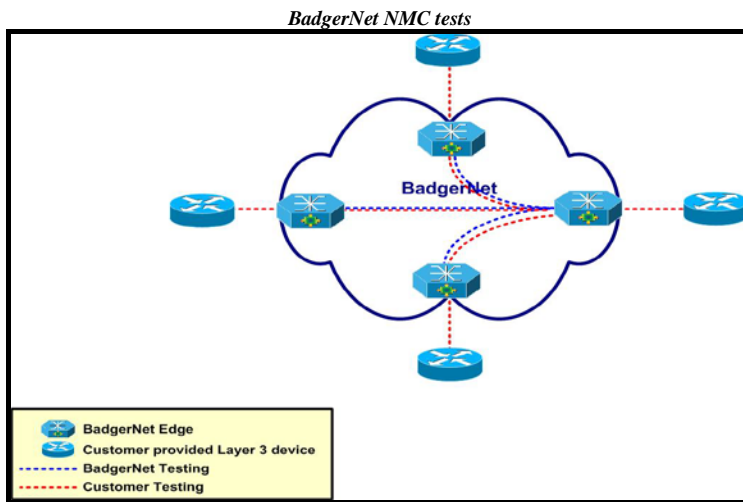
After your equipment is connected to the network, usually on Ethernet port 7, and configured using the addressing information provided by the BadgerNet Lead Engineer, you are ready for testing. Before you begin, verify you have a link light (usually a steadily lit green LED on the port). This confirms 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

Formatted: Indent: Left: 0.5"

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).



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.

Formatted: Indent: Left: 0.5"

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 condition exist, a troubleshooting session ought to ensue.

Formatted: Indent: Left: 0.5"

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.

Formatted: Indent: Left: 0.5"

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. There are no charges associated with this type of call for you.

Formatted: Indent: Left: 0.5"

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.

Formatted: Indent: Left: 0.5"

High-Definition Video Service

High-Definition Video Service Overview

The BadgerNet Converged Network will transition from Standard Definition Video Service to High-Definition Video Service at a point in the near future. The infrastructure supporting BCN video will completely change to support a High-

Definition network. 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 requires 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

MCU

Existing Polycom MGC 100 MCU will be replaced with Polycom RMX 2000 40HD/160CIF MCUs. This MCU accommodates up to 40 High-Definition video calls simultaneously, or as many as 160 standard definition calls. Inherent within the MCU is the ability to transcode connections of various speeds allowing video sessions to operate at the highest, rather than the lowest, common denominator. The RMX 2000 allows for a mix of SD and HD within the same chassis at the same time as well as within the same session. That is, it supports within a single call SD and HD connected codecs.

BCN will place MCUs within each of the four LATAs and initially determined as many as six MCUs may be needed. Six MCUs with 40 ports of HD capacity equals a total of 240 simultaneous HD calls, or as many as 960 SD calls simultaneously. BCN also proposes to accommodate growth within the MCUs as a network responsibility rather than the obligation of the state. As with the aggregation and core layers of the network, capacity will be added by the prime contractor without direct expense to the state. Redundancy will also be the responsibility of BCN.

Video Codec

BCN chooses the Polycom HDX 8000 series codec to deploy at sites that request HD video service. Each site that requests service will receive a single codec versus the three codecs (pizza box style) deployed for legacy SD service. HD codecs will operate at default at 2 Mbps, but could operate at lower speeds if desired. The codecs will be placed within the service providers "blue box". The blue box interface panel is replaced with a modified version to accommodate the digital interfaces and balanced interfaces.

E.164 compliant addresses are assigned to each codec and each will register to the Gatekeeper to establish availability.

Gatekeeper

Polycom Converged Management Application (CMA) has been chosen for the gatekeeper functionality. Each video addressable device within BCN network requires a license to operate within the HD environment. All codecs, both SD and HD have to register to the Gatekeeper to establish availability. As Renovo software establishes a conference, it works in conjunction with the gatekeeper to insure end-sites are licensed and available for calls.

In addition, CMA includes the functionality of Polycom GMS to monitor devices and upgrade them remotely. CMA can also authenticate users, but this functionality has not been incorporated to BCN yet. However, that may be included at a later date.

Video Border Proxy (VBP)

In legacy SD video network, calls originating from off-site locations terminate in the MCU to connect to internal callers. Requiring connections this way insured that BCN remained a closed network free of interference from hackers, viruses, and malicious content. BCN retains that functionality by deploying Polycom's Video Border Proxy. A video specific firewall, the VBP works collaboratively with the Gatekeeper to insure calls entering or leaving the network have permission to do so. The MCU will not participate in off-net calling any longer. Calls without permission to enter or leave the network are denied protecting the internal portion of the network.

BCN will deploy two VBPs for redundancy, each with a throughput capacity of 85 Mbps. During normal operation, calls totaling 170 Mbps can enter and/or leave the network simultaneously, which is a significant increase from the capacity of today's IP-48 cards.

Recording Video Sessions

A ~~N~~ew feature to BCN is the Video Streaming option requested by many of the schools and some agencies. If requested, a video streaming port can be added to any BCN session to record the call. The steaming port provides a point-of-view perspective and records video, audio and content. Process details are still being refined to determine if BCN will send the content to the end-user or if the end-user will retrieve the content after being authenticated. In either event, the offering provides very little storage (which could be modified if requested), so content cannot remain

within the network for long (a day or two perhaps). The capability built into this proposal will accommodate 20 simultaneous sessions without content or 10 sessions with content

Renovo Scheduling Software

Renovo, the BCN Scheduling Software provider, has developed and deployed scheduling software for Polycom's HD codecs. Functionally, the end-user will not notice much change from the current scheduler.

Dascom DL Navigator/DL Hub

DL Navigator, which is used on the BCN Managed classroom settings, must be upgraded to accommodate HD video codecs, but the end-user will not see any difference in the user interface.

System Operation

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

- Only one codec per site, which operates a 2 Mbps video stream
- A single HD student monitor and a single HD teach 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 Gatekeeper (CMA) which validates its license and availability. Before it joins a multi-site conference, Renovo 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 are 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 demonstrates calls from SD-SD, HD-HD or mixed sessions can be accommodated.

Call Matrix

Standard Definition	High Definition	Mixed (SD-HD)
1x1 (pt-pt)	1x1 (pt-pt)	1x1 (pt-pt)
1x3 (standard)	1x3 (standard)	1x3 (standard)
1xN (MCU)	1xN (MCU)	1xN (MCU)
Off-Net	Off-Net	Off-Net

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 "savvy" end-users to purchase their own video codecs or VoIP systems. If scheduling or access to an MCU were a requirement for effective use, the end-user would have to purchase them independently. The BCN Video Bridging Service changes that.

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. This feature should be attractive to those currently using the Internet and paying usage charges to connect to another BCN site in a different VPN. The Department of Administration has relaxed its policy allowing any combination of Managed Video, HPLL or HPLL with BCN Video Bridging Service to connect to a session 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 purchase BCN Video Bridging Service provide their own codecs, which must be hardware based, H.323 compliant and non-proprietary. 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 officially tested and billed. BCN Engineering will work with the customer to review responsibilities, service demarcation and network configuration (as it relates to BCN). If the codec is not supported, the customer can choose to cancel the service or purchase a different codec. 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. Billing will commence on the day of test is scheduled in the web portal.

Network configuration

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

Installation and configuration of the BCN firewalls

- Configuration of the Cisco ASA 5520s firewall.
- AT&T will purchase the firewalls and take responsibility for physically installing and connecting them to the PE router
- The firewalls will be installed in administrative space in the Madison 11 CO (MDSNW111)
- Initial configuration may be completed by AT&T and be maintained by KDL through a contract service agreement.
- Configuration of the PE device will be completed by KDL.

MCU Configuration

- MCU already has appropriate card capacity – no changes to it are required. If additional port capacity is needed, new IP-48 card(s) can be purchased by the DOA.