WBMM Scenarios

1 Introduction

This document identifies a series of scenarios which have been generated to typifying the application of the WBMM capability and which exemplify the requirements. The scenarios are groups into three areas:

Service Provider Based Monitoring
Intra-enterprise Device/Service Management
Extra-enterprise Device Management

The WBMM capability involves two functional enitities and the communication between them. On one side is the WBMM agent, either internal to the device being managed or a proxy for that device. On the other side is the Managing Application. These two elements communicate over a network, perhaps the internet, using standard protocols and services.

2 Service Provider Based Monitoring

There is increasing use of manufacturer-associated or independent service providers that maintain imaging devices within an enterprise. The effective implementation of such a service requires some way to address the many circumstances where limited extra-enterprise access to imaging functions for maintenance and device service purposes is necessary to properly support the enterprise, to allow effective supply and maintenance of imaging equipment, and to provide usage information for billing purposes. This need to address extra-enterprise access to equipment isolated by a firewall is a key requirement of WBMM.

This area differs from extra-enterprise management in that the monitoring function not only requires limited management access, but WBMM must be able to provide built-in controls to limit access to the minimum objects necessary for monitoring. This enterprise-controlled limiting capability is necessary to ease security and network integrity concerns.

The following scenarios provide several different use cases implying increasing depth of access.

2.1 Scenario A1

2.1.1 Description A

IKA, an office equipment leasing company, leases and services printers and copiers from several manufacturers to a wide range of customers. One specific customer is an insurance company, American Casualty Ensurence (ACE). ACE is very concerned with security but also is demanding no more that 0.5% downtime for the equipment. Under different circumstances, IKA would have resident service people checking the equipment, keeping usage figures for billing, and ready to react if a user reported a problem. But because of the security issues, ACE will give service people access to the facility only when there is a problem. Security also prevents IKA from access to the ACE network to use standard equipment monitoring programs. Indeed, between traffic and security concerns, ACE does not allow programs using broadcast SNMP to be on its network.

ACE does allow its employees EMAIL and Internet access though an HTTP proxy but ACE does not allow any other Internet access. ACE will not support EMAIL accounts for the imaging machines but will allow IKA to communicate status and usage information using the WEB access structure in place, provided that ACE MIS has the ability to monitor the communications. Nothing that reflects anything about the network or the business can be communicated: this includes IP addresses, device names, and of course, any job information.

2.1.2 Description B

IKA has a customer similar in all respects to ACE, except that they severely restrict WEB access from their enterprise. They can be persuaded to assist IKA by providing one email account. Mail can be sent out via ESTMP with authentication and received via APOP.

2.1.3 Discussion

Many requirements are implicit in these scenarios.

1. For variation A, operation should emulate a PC browser at the device side and a Web server at the management side, including:
    a. use of HTTP transport.
    b. Compatibility with HTTP proxies, including authentication.
    c. message format and coding compatible with Web services
    d. Non-encryption of data so communications can be spot checked by a monitor.

2. For variation B, operation requires either a proxy which interfaces between the mail system and all of the devices, or a means by which multiple devices can use the same email account, with each device erasing only those messages intended for it. In either case, this would require:

   a. Support of Authenticated ESMTP and APOP on the agent side, with corresponding email support at the management server
   b. Message format and coding compatible with EMAIL
   c. Information in the header or easily determined from the body as to the actual intended recipient of a message sent to a shared mail account.

3. Accommodation of policies preventing any configuration changes and restricting the data that may be communicated.

4. Reliable detection and commutation of alert conditions, probably with moderation, and with sufficient data or the ability to obtain sufficient data to reliably define the alert condition.

5. Periodic communication of usage data, aligning with billing periods

6. Ability of the management service to request specific information and to modify reporting periods and alert conditions, subject to enterprise-determined policies

7. Ability to interact with an existing base of imaging equipment as well as new equipment. This means that the communication with imaging equipment may be through:
   a. a facility built into the imaging equipment
   b. a proxy device that potentially services many existing networked imaging devices
   c. software running on computers which have locally-attached imaging equipment

The implicit configuration is represented below. The managed equipment communicates though an embedded WBMM agent, a proxy device communicating with networked imaging equipment, or some other networked interface device or PC communicating with non-networked imaging equipment. The Management Application is running in a Server accessible on the web.

All communication is initiated by a WBMM Agent, acting as a compliant Web client on the enterprise network.
Communication with the Management Server is initiated:

a. at predetermined times or on local stimulus to query about instructions, contact schedule, definition of alert conditions and moderations, and contents of alert and usage reports. (Command Query)

b. on detection of an alert condition to issue a report and accept a request for Command Query. (Alert Report)

c. to issue a usage report (Usage Report)

Communication is initiated by a POST from the agent of identification, time and connection type. The Management application responds as appropriate.

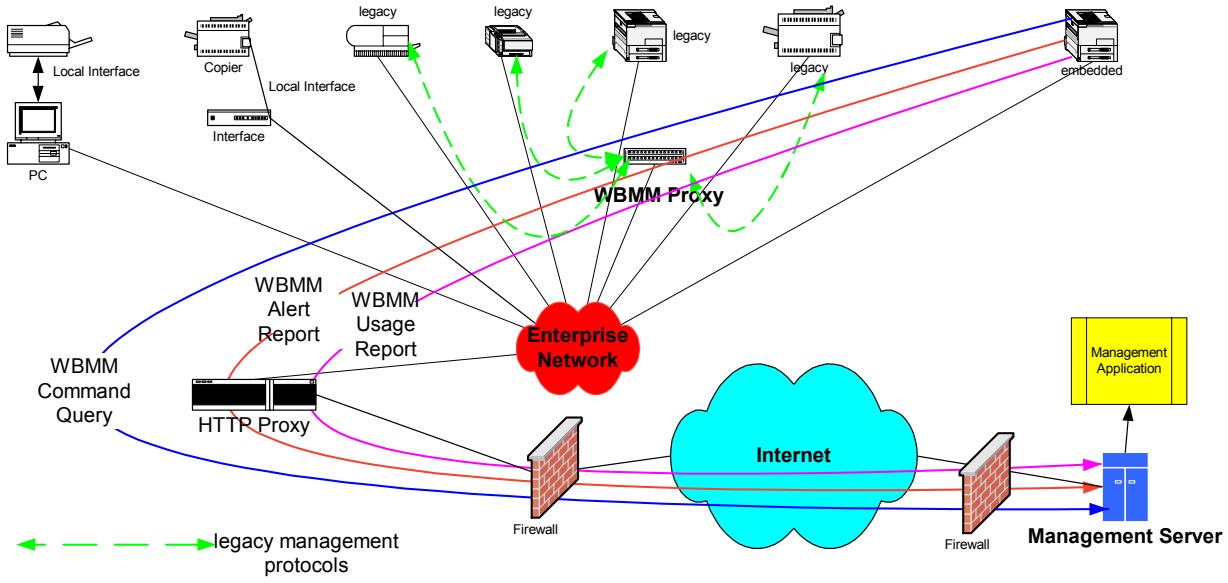


Figure 1a - Scenario A1A - Monitoring Remote Enterprise/HTTP

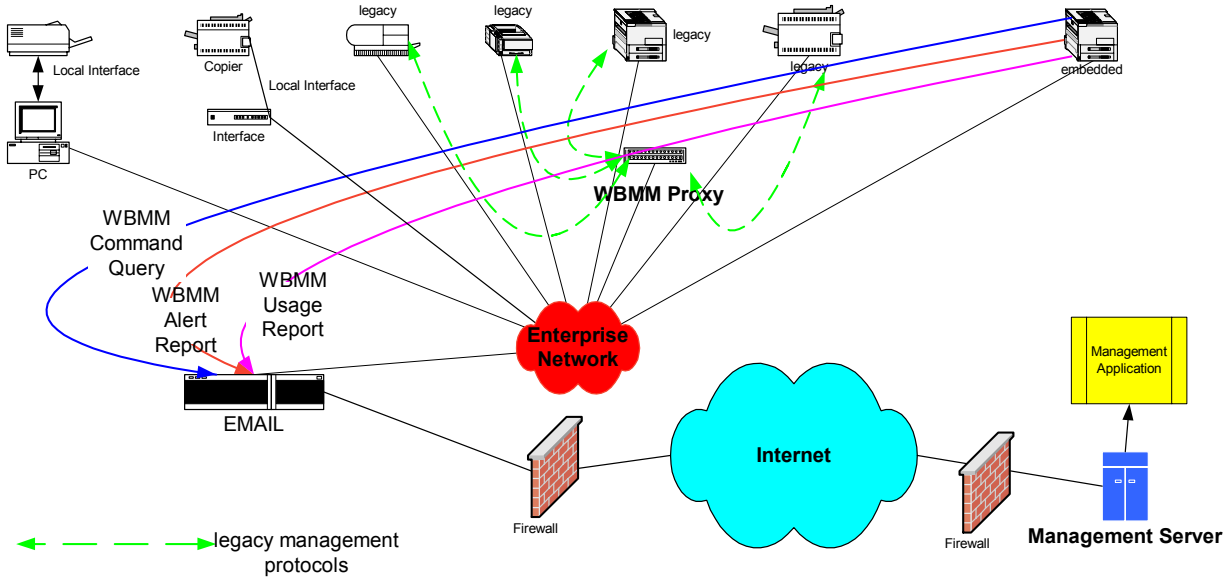


Figure 2b Scenario A1B - Monitoring Remote Enterprise/EMAIL

2.2 Scenario A2

2.2.1 Description

DAKON, an office equipment leasing company, sees a market opportunity in the small to mid-sized office market. They believe that if they can get service contracts to maintain the 2-10 printers and copiers characterizing each site, they will make money on the consumables and eventually will get to lease equipment to these companies as the equipment in place ages out. In the short term, they need automatic reporting of low supplies and problems for the rapid response they are advertising. In the longer term, they will need to use the web service to get copy counts for billing and the capability of remote update/upgrade.

2.2.2 Discussion

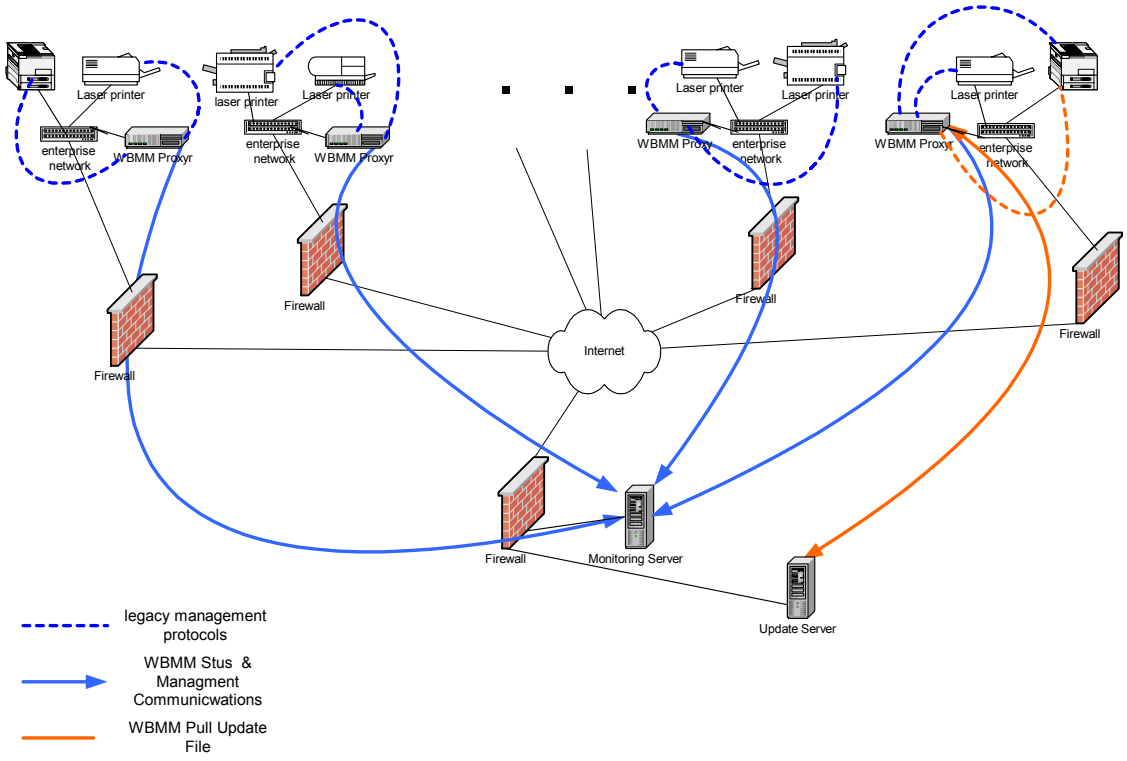
This scenario is similar to A1, but differs in that the Enterprise sites are much smaller and the enforced security constraints are much less (but the requirements may still be there.) There is no specified demand on up time, although the customer must be kept happy for business reasons. The immediate stress is on providing effective alert reporting for the existing equipment with minimum cost. In the projected long term, the equipment will be replaced by DAKON-supplied units for which more access capability must be supported, including remote firmware update/upgrade.

In the diagram, sites are represented with two networked imaging units each, supported by a WBMM proxy device. The proxy device communicates with the imaging units using existing supported methods, probably SNMP. In the initial configuration, the proxy devices communicate status and alert information through the firewall to the internet-resident server. In the later configuration (shown by the rightmost site), the instruct ructions from the monitoring server include commands for the proxy to pull an update file from a specified URL and apply it (by whatever means are appropriate to the end device) to an imaging unit.

There are other requirements implicit particularly as relate to a WBMM proxy. Some of these may not be an integral part of WBMM, but must be considered. These include:

1. ability of WBMM to communicate to a WBMM proxy instructions for monitoring several units
2. ability of a proxy to be set up with the characteristics of networked imaging units so that it can translate from WBMM instructions to the management protocol supported by the device
3. ability of a proxy to be set up so that it can pull a file at a URL identified in an instruction and present that file to an imaging unit in a manner required by that device to accept a code update. When dealing with end devices that already have the capability to pull an update file, that native capability can be used.

However, particularly for dealing with WBMM proxies, the mannor by which they pull a file to be sent to a proxied printer should be defined.



Monitor

Figure 3 - Scenario A2 - Monitoring Small Sites

2.3 Scenario A3

2.3.1 Description A

Better Pinter Manufacturing (BMP) is marketing a high-reliability networked printer/copier, and bundling the unit with a supply and service contract. Their information suggests that the profit on supplies will be substantial, and with remote reporting and monitoring, the service aspect should at least break even. They need to set up their customers so that supplies and failure information is quickly communicated to one of their centralizes depot facilities. But the capability must be easy to install, requiring no unusual effort from the often-

limited MIS groups. The solution must address concerns about network, equipment and information security from increasingly squeamish companies.

2.3.2 Description B.

BMP has a printer with all the bells and whistles, but at a high end price. Marketing fears that the price will hurt sales, but believes that, if they disable some of the features and sell the product at a lower price, they can make it up later by "upgrading" the units in the field to have full features. Of course, the upgrades need to be easy and must not require either customer service visits or any technical action on the part of the customer. They would like the ability up upgrade device firmware using the Web Monitoring and Management Capability put in place for service and supply maintenance.

2.3.3 Discussion

These scenarios manifest the requirements in Scenarios A1 and A2. WBMM would be built in to the devices. The additional features are;

a. stress on ease of installation of the monitoring feature (and probably the imaging features as well) This suggests some semiautomatic on-site registration method of units with the monitoring server

b. the scenario has the security constraints of a1, but also the ability to download upgrades, which is a more invasive capability than simply monitoring. Indeed, this probably is a manifestation of Extra-Enterprise Management.

3 Intra-enterprise Device/Service Management

3.1 Scenario B1

3.1.1 Description

A device that supports a web services based job submission protocol is deployed at a customer's site. Buzz Lightyear Green invokes the client software that submits a job to the device via web services based protocols. The device-based printing service enters an error state due to a paper jam. It is unable to accept the job so it fails the client's request to initiate a job. An exception is sent back to the client.

An event is sent to the management application that is monitoring the device and its services. Woody Blue, the administrator, uses the management application to query the device/service to determine its state and to invoke corrective operations. Depending upon the policy restrictions in the device/service, corrective operations may include sending commands via WBMM or an existing protocol, or having someone physically fix the device depending on the type of error. Management events and state queries conform to the WBMM protocol. In this case, although device policy restrictions allow Woody to institute

configuration changes via WBMM, the nature of the error requires that Woody phone Seville Orange, near the offending device, and ask her to clear the jam.

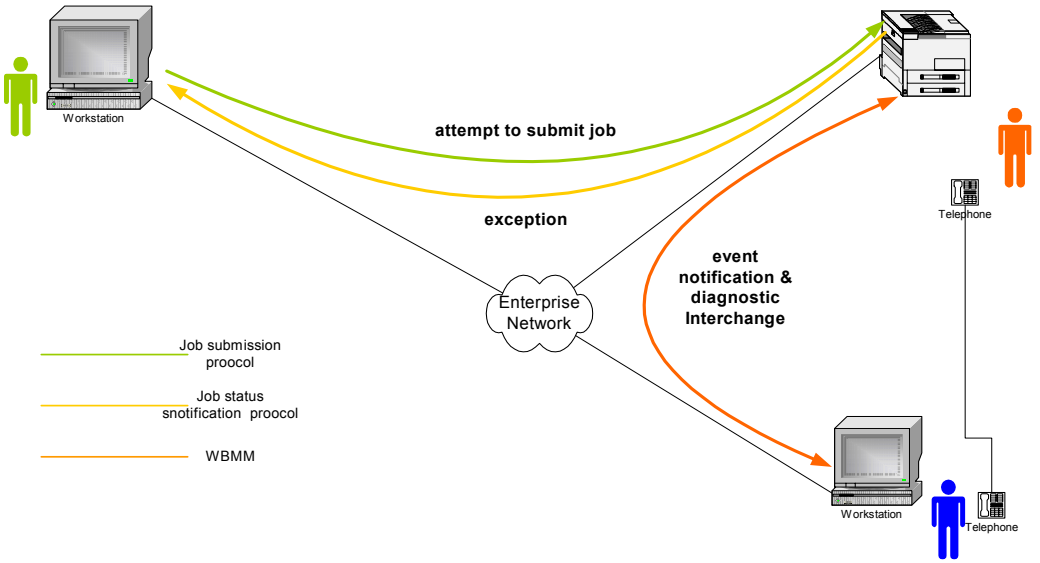


Figure 4 - Scenario B1A - Management Support of Print Services Printing

3.1.2 Discussion

Although this is a typical device management scenario that could use various management capabilities, the use of a web services print service suggest the use of a web services type management service as well.

The Scenario defines the management interface as device based. But the advantage of using a compatible web services may be more apparent if one considered co-locating the Print Service and Management Service. The use of a similar transport, the common basic form of data and coding method, and the relation to an expanded semantic model act to simplify this implementation.

It should also be considered that the Print Service/Management Service might be extra-enterprise.

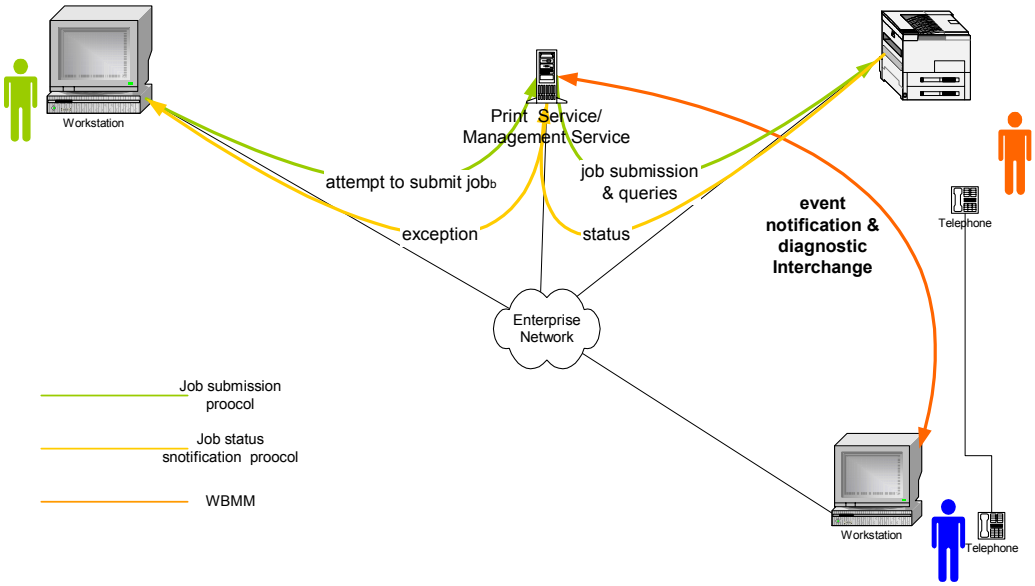


Figure 5 - Scenario B1B - Management Support of Print Services-Based Printing

3.2 Scenario B2

3.2.1 Description

Save-the-Trees Ornate Plastic Toothpick company (STOP Toothpicks) manages various different imaging devices from an internal management application that uses a Web Services type capability. The capability is embedded on some units, supported via a PC application on direct-connected printers, and implemented via a proxy device for some network attached printers. Although Manny Blue, the administrator, can set up the units to contact the managing server at a preset period, he wants to have virtually immediate management access to the imaging units as he had with his old management program.

3.2.2 Discussion

A premise of the web based management is that the connections are always initiated by the device/service or its proxy. This may not be necessary when operating within a intranet. Like Manny Blue, some managers will not want to wait until the device makes contact before performing a management operation. However, rather than providing for a full bi-directional protocol, it seems better to allow the management station to issue a unicast “tickle” packet that will cause the addressed unit to log-in to the server and request instructions, essentially providing a tickle to prompt the normally periodic instruction request connection.

This is illustrated below.

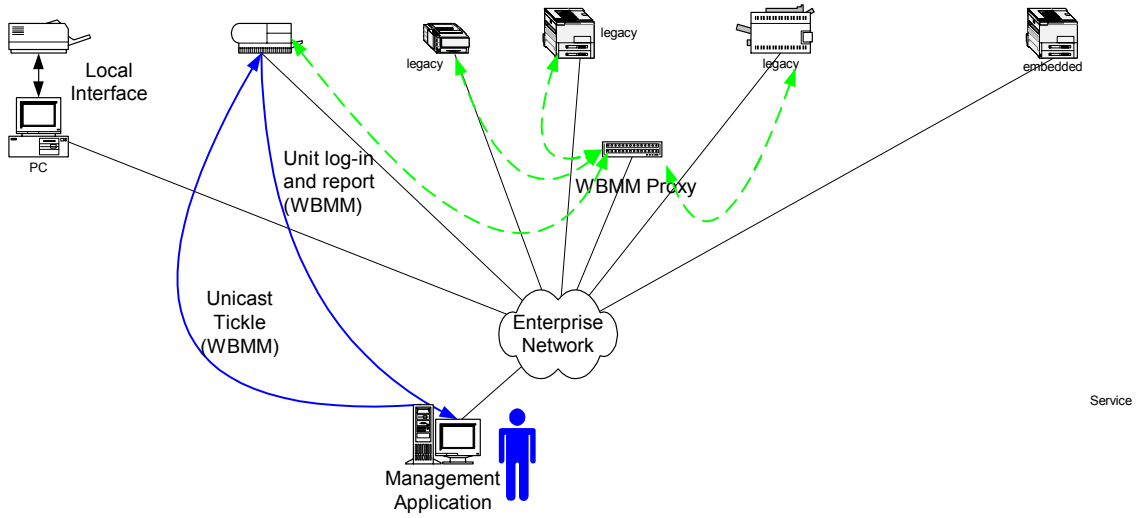


Figure 6 - Scenario B2 -Getting Units Attention

3.3 Scenario B3

3.3.1 Description

Because plastic solvent in the atmosphere causes toner to cake and jam the machines, STOP Toothpicks has high turnover in their imaging units (and personnel). During Manny's illness, imaging units have been replaced and reconfigured. His replacement, Rose Red, does not have good records of what has happened and needs some way for the management application to automatically locate all manageable imaging devices.

3.3.2 Discussion

Just as the unicast tickle causes a specific device to response to the querying management station, a multicast tickle (or broadcast) causes each device receiving and understanding the tickle to report to the identified management station. In later discussions, it was observed that the proposed method of multicast tickles would probably not be passed by many routers, It was suggested that although WBMM can suggest discovery protocols, actually defining a discovery mechanism is out of scope. However, referencing an effective mechanism to be used with WBMM remains a requirement.

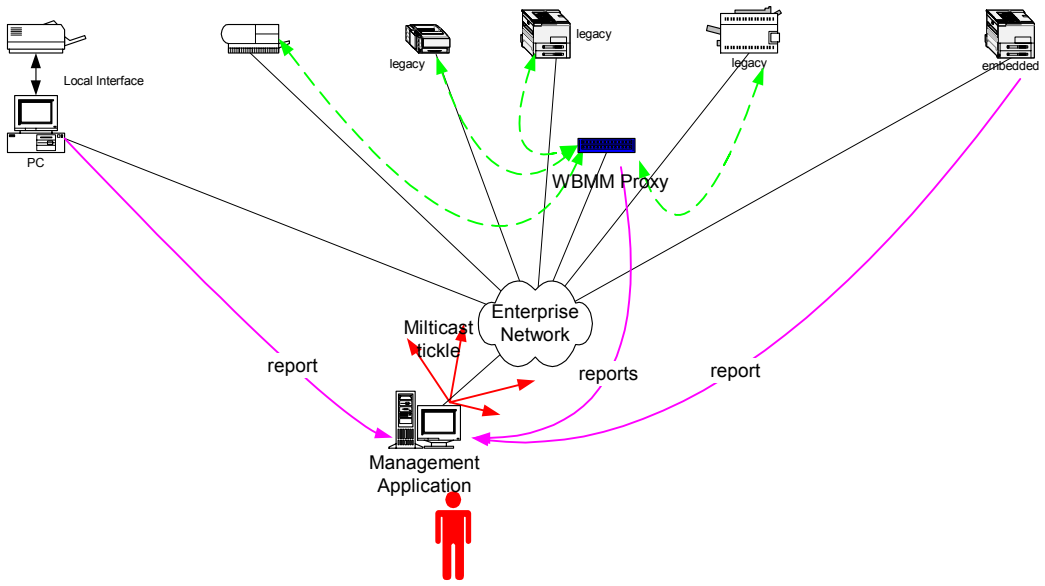


Figure 7 - Scenario B3 - Discovery

4 Extra-Enterprise Device Management

As was described in the scenarios, requirements for remote monitoring may include functions such as downloading update code and eventually will include full remote management. Therefore, although the previously identified subset of remote monitoring should be addressed, the WBMM capability must encompass full remote device management ("set" as well as "get").

In addition, there is another variation in which management may be distributed between local and remote agents. Management applications have traditionally consisted of a single application that is deployed at the location where the management operations are performed. Just like other types of applications, management applications are starting to be deployed as a set of distributed components. A common deployment scenario consists of some amount of basic functionality that is deployed locally on the site and enhanced or extended functionality is deployed in a remote location. This allows the extended functionality to be consolidated in a single web site. This enables a hybrid model that fits between the traditional self managed and service provider environments. The customer manages their devices but can take advantage of centralized functionality from an external provider. In this model, a management application or a device will extract a snapshot of its functionality, configuration and state and pass that information onto a back-end web site. The web site performs the processing and returns the result.

4.1 Scenario C1

4.1.1 Description

W Coyote Inc has ten small sites that each has a single device. W Coyote has hired Acme, a service provider, to manage these devices. Included in the contract is a minimum guaranteed uptime of 90%. Acme is penalized when a device fails to maintain the contracted uptime. Since each site only includes a single device, it is cost prohibitive for Acme to install an application/appliance at the customer sites. They decide to directly monitor and manage the devices remotely using WBMM. The service provider's portal remotely monitors each device to determine its uptime and any errors. If an error does occur, Acme will either manage the device remotely to fix the error or contact someone at W Coyote to make the correction. At the end of the month, Acme provides a report on the uptime for each device to justify their charges. If there is a disagreement Acme can provide a log obtained through a secure, authenticated connection of the monitoring activity.

4.1.2 Discussion

There are several requirements implicit in this scenario.

1. The managed devices support WBMM natively.
2. The device's activity log must be transported to the service provider's portal via a secure, authenticated connection. The log must not be corruptible.
3. The monitored devices are configured to contact the service provider's portal at a specified interval.

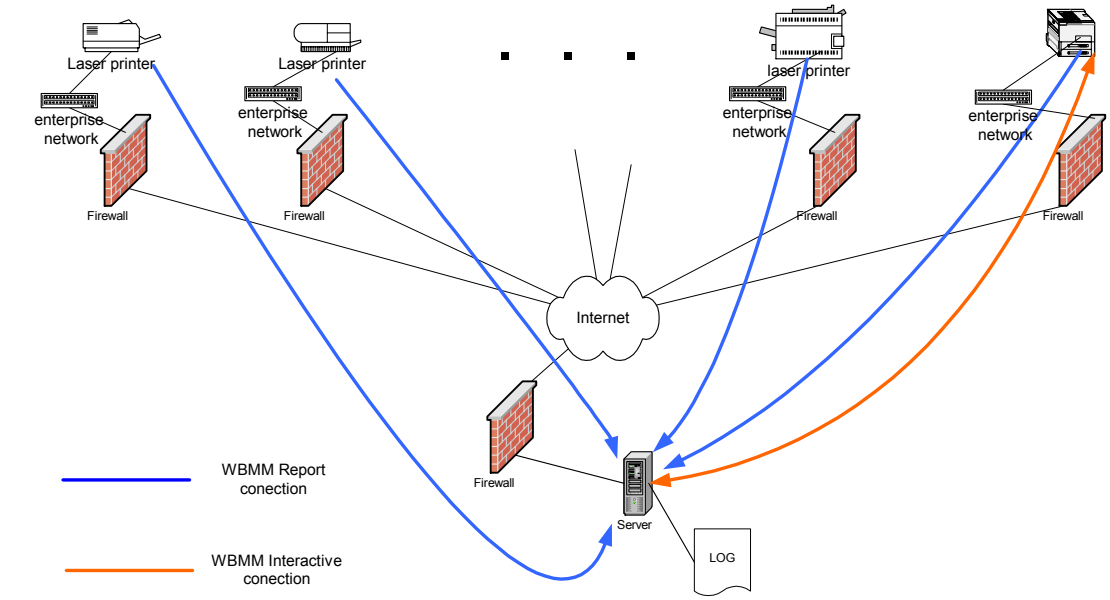


Figure 8 - Scenario C1 - Remote Management

4.2 Scenario C2

4.2.1 Description

Fred submits a job to a print service running on a device. After the job is submitted, an error occurs and the device enters an error state. Its status indicates that a service error, number xxx.xx, has occurred. Barney, the administrator, is notified of the error via an event that is sent to his management application. Barney uses the management application to attempt to determine the cause of the error by communicating with the device using WBMM, SNMP, or another existing protocol. The management application doesn't contain information concerning service error codes. It grabs a snapshot of the current device configuration and state, formats the data into a XML document that conforms to the WBMM standard XML device model (if device supports it directly

then it acts primarily as a forwarding agent) and then forwards onto the external support web site. The web site processes the information and then provides an explanation of the cause and the steps correct the error. The management application presents the data in its user interface. Barney follows the directions generated from the support site to correct the error.

4.2.2 Discussion

There are several requirements implicit in this scenario.

1. The WBMM agent can convert device-data obtained using existing protocols into WBMM-compliant XML documents.
2. To illustrate the Extra-Enterprise Device Management scenarios being described in this section, the support web site is external to the enterprise. WBMM will also support the scenario where the support site is internal to the enterprise.
3. The management application can be a general Network Management System (NMS), such as Tivoli or OpenView, or a Print Management Application, such as Mark Vision or Web JetAdmin. The hope is that existing management applications can be augmented to support WBMM.

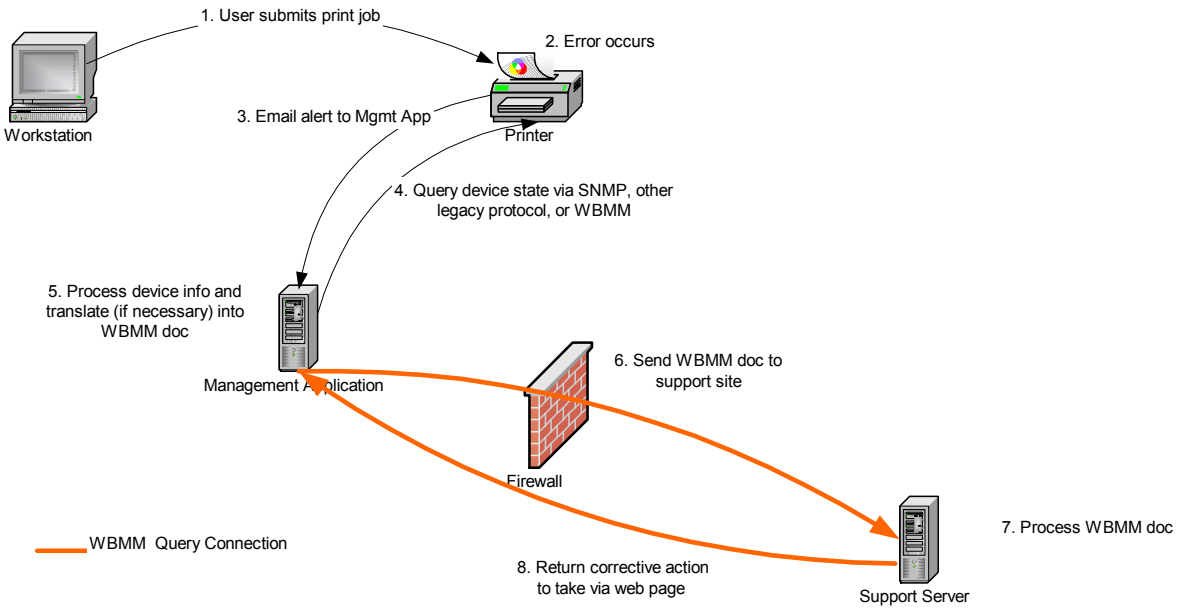


Figure 9 - Distributed Management

4.3 Scenario C3

Print Mgmt Outsourcing, Inc. (PMO) is managing 25% of the Printing and Imaging resources for Company X. They just signed a contract with Company X to take over the remaining 75% of the P&I resources.

4.3.1 Descriptions

4.3.1.1 Situation A

In order to know what types of devices are needed, PMO needs to analyze the usage metrics for the existing MFDs installed at Company X. PMO wants to find out the following:

a. *how many pages were digitally sent that were Color and were input via an ADF.*
b. *what percentage of copies made are color versus mono and 1-sided versus 2-sided.*

4.3.1.2 Situation B

PMO also wants to enable the automatic reorder of maintenance kits for MFDs as needed. In order to do this, they need to be able to identify the many different components that make up the device. They will also need to be able to compare the current operating status of each component with defined thresholds (or based on time) to know when a maintenance kit is needed.

4.3.1.3 Situation C

PMO needs the ability to set configuration attributes across the entire fleet of MFDs in Company X.

a. *Set the default number of copies to be printed for a job to be 1. (for example: SetFleetConfig(defaultCopies, 1))*
b. *Set all copy functions to default to simplex, and all print functions to default to duplex.*
c. *Set all the High Capacity Output (HCO) for all MFD's to be in stacker mode.*

4.3.2 Discussion

Situation A is similar to other scenarios where the requirement is to periodically collect use parameters from an existing equipment base. It is not clear that the statistics themsekleves are available, but use figures probably are. Of course, if use information is not available, other means could be used to collect the necessary data, including user and network monitoring. Such means are out of scop e for WBMM; However, they could use the WBMM messages to forward collected data to the management application.

Situation B, is also similar from the WBMM viewpoint, except that it may require better instrumenting and communicating of the MFD's critical components, their status and their life expectancy.

Situation C has several implications. Although it could be maintained that a fleet is just a a group fo devices that are accessed indidvually, there are other interpretation.

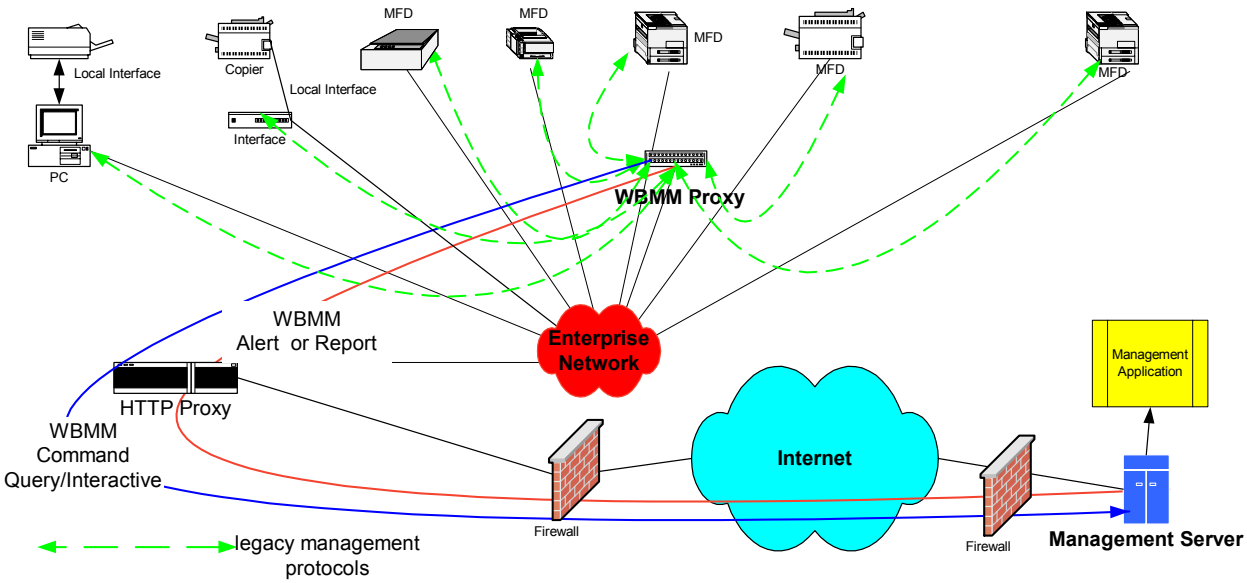
If the agents are embedded, and the management is external, there seems little alternatice but set each unit up as it calls in. However, if the WBMM agent is in a local management server or in a proxy, a "group" set could be done from the remote management application. This would certainly decrease internet traffic.

The proxy could then communicate to the devices in their native protocols, for which multicast may or may not be allowed.

This approach also has the possible advantage of fewer devices needing internet access and running though the firewall.

The requirements implicit in this scenario set, beyond previously expressed requirements, include:

Ability to indicate that a WBMM command set is applicable to a defined group of equipment rather than just one specific unit.


Local Interface
PC
Copier
Local Interface
Interface
MFD
MFD
MFD
MFD
MFD
WBMM Proxy
WBMM
Alert or Report
Enterprise
Network
HTTP Proxy
WBMM
Command
Query/Interactive
Internet
Management
Application
Firewall
Firewall
Management Server
legacy management
protocols