WHITE PAPER
Intel® vPro™ Technology
Embedded Computing

Managing Digital Signage Over 3G Using Intel® Active Management Technology (Intel® AMT)

Implementing out-of-band (OOB) secure advanced remote management - practically anywhere

Lower the TCO of digital signage with remote management over 3G

Digital signage displays are everywhere, even in out-of-the-way fuel stations in the countryside. Today, the widespread availability of 3G and emerging 4G cellular-based wireless broadband networks enables digital signage to be deployed virtually anywhere.[1] This is a good alternative when wired broadband service isn't available to provide a connection for downloading and updating content.

Network connectivity is also used by technicians who monitor and manage displays centrally from a remote console. Compared to sending someone onsite for ongoing support and repairs, remote management saves cost and time. For a display that's so secluded as to need a 3G connection, the savings are even greater.

Advanced Remote Management

Taking remote management to a new level, Intel® vPro™ technology with Intel® Active Management Technology (Intel® AMT)[2] allows consoles to fix a wider range of systems issues, even when the operating system is down. For example, it's possible to repair corrupted drivers, application software or the operating system for a non-responsive signage system that won't run or boot. This can be done on an Intel vPro technology-enabled display through a capability called out-of-band (OOB) management, which is described in the following section.

The advanced capabilities of Intel AMT can help reduce the total cost of ownership (TCO) for digital signage, especially when systems are deployed at distant locations. For such cases, this paper describes how to set up Intel AMT over 3G using permanent site-to-site IPSec VPN tunnels. VPN tunneling virtually extends the network of management servers to managed devices, thus allowing the management console within the corporate firewall to discover and communicate with digital signage systems outside the firewall more securely. In addition to digital signage, this approach is applicable to other embedded devices, such as vending machines, kiosks and medical devices, that may be located outside the corporate firewall and connected through wired or wireless high speed network. There are additional ways to utilize Intel AMT for managing devices over 3G or other networks outside corporate firewall that will not be discussed here.

Table of Contents

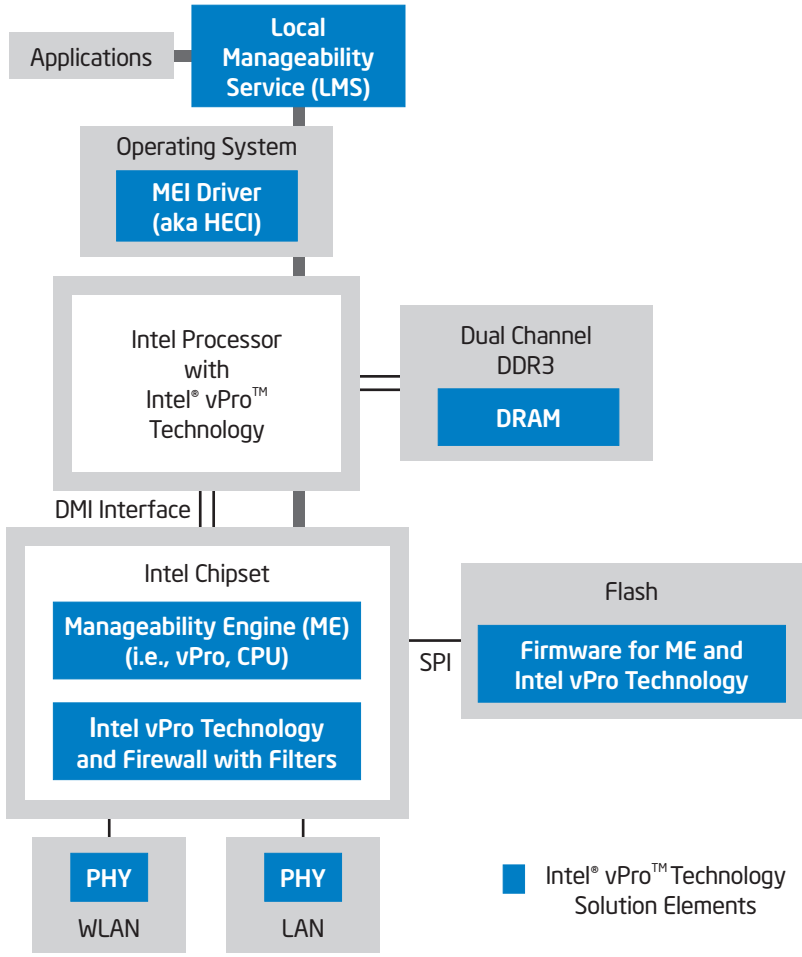

Figure 1. Key Intel® vPro™ Technology Components

What Makes Intel® Active Management Technology Different?

Intel vPro technology with Intel AMT is built into select Intel® processors and chipsets. Intel AMT employs a silicon-resident management mechanism for remote discovery, healing and protection of computing systems. This circuitry establishes a new communications channel, using an "out-of-band" link that operates independently of the "in-band" channel of the computing system and provides persistent connectivity.

This out-of-band link employs a dedicated manageability engine (ME), shown in Figure 1, which enables control over non-functioning systems. Other Intel vPro technology elements include a small amount of memory residing in the FLASH device and a firewall with filters supported in the Intel® Ethernet Controller and the Intel® chipset. When the system is functioning properly, the Intel processor runs local manageability service (LMS) software that is used to interface with the ME over its local interface. ME executable code and data are stored in the FLASH, and the ME runs from internal memory in the chipset or from host memory, using a dedicated region that is not visible to host.

In contrast, traditional remote management consoles communicate with devices using their standard networking capability, called an in-band link, which utilizes the device's operating system, CPU and network drivers. When equipment fails, the in-band approach has the drawback of relying on the continued operation of many equipment components, significantly limiting the types of problems or failures that can be fixed remotely.

Intel AMT includes a feature called KVM redirection over Internet Protocol (IP), permitting the keyboard-video-mouse (KVM) for an IT console to control and display the graphical user interface (GUI) of signage systems in the field. No additional hardware is required. Intel AMT 6.0 KVM support requires a 2010 Intel vPro technology-enabled platform with Intel® integrated graphics.

Intel AMT KVM also enables proof-of-play, the ability to confirm an ad actually played on a digital signage display. The feature captures screen shots and time stamps at regular intervals, thereby providing evidence of what the system played throughout the day. Before proof-of-play, it was difficult for advertisers to verify the ads they paid for actually ran. Besides the expensive option of sending auditors to physically check displays, advertisers had to rely on receiving playlists, which could not prove the signage system was functioning or what was actually displayed.

Intel® Active Management Technology Over 3G

This paper furthers the discussion about Intel AMT by providing a configuration example for a management console within a corporate firewall communicating securely via site-to-site VPN tunnels over 3G Network with systems outside the firewall. Any VPN technology capable of establishing a site-to-site VPN, such as SSL VPN, PPTP and L2TP, can be considered in this application. VPNs are mature technologies and can be based on IPsec, MPLS, ATM, Carrier Ethernet or other networking technologies. Regardless of which of those network technologies is used to carry IP traffic, the key is to achieve direct, IP-level network visibility between the Intel AMT-enabled console and Intel vPro technology-enabled signage device so that all signage devices are "visible" from the console. In fact, by using VPN, a remote LAN supporting digital signage systems becomes virtually an extension of the corporate network; thus, digital signage devices on one side of the tunnel can be made visible to and discovered by the management console on the other side. The reason for using permanent site-to-site VPN instead of client VPN is to keep the tunnel alive even when the device is turned off or not functioning; this is needed to take advantage of the OOB manageability features provided by Intel AMT.

In the simplest form, the key components of the implementation are a VPN-capable router or appliance connected to a management console and a VPN-capable 3G modem/gateway connected to one or more Intel vPro technology-enabled digital signage systems, as depicted in Figure 2. In a real world implementation, there could be additional IT infrastructure, like DNS, DHCP, CA, AD and more routers and switches, depending on the security and IT policies, and the number of devices and VPN connections required. The selection of devices for this proof of concept does not imply an Intel endorsement or guarantee for these devices and their associated manufacturers. Digital signage vendors should select devices that satisfy their security and usability requirements.

Configuration Example: Intel® Active Technology Management Over 3G

Intel constructed the network shown in Figure 2 and demonstrated Intel AMT over 3G using a Sprint* wireless network. This section and Appendices A-D describe the configuration details for the router and the 3G model/gateway, and although specific network elements are discussed, the information is applicable to other networks and network devices as well.

Sierra* Wireless AirLink* Raven XE Ethernet Gateway

The Raven XE can operate as a 3G modem/gateway device with DHCP and VPN tunneling capability. Compared to a simple 3G modem, this device offers a simpler, lower cost solution by avoiding the need to add a router with VPN capability between the modem and the digital signage devices. The Raven XE supports two

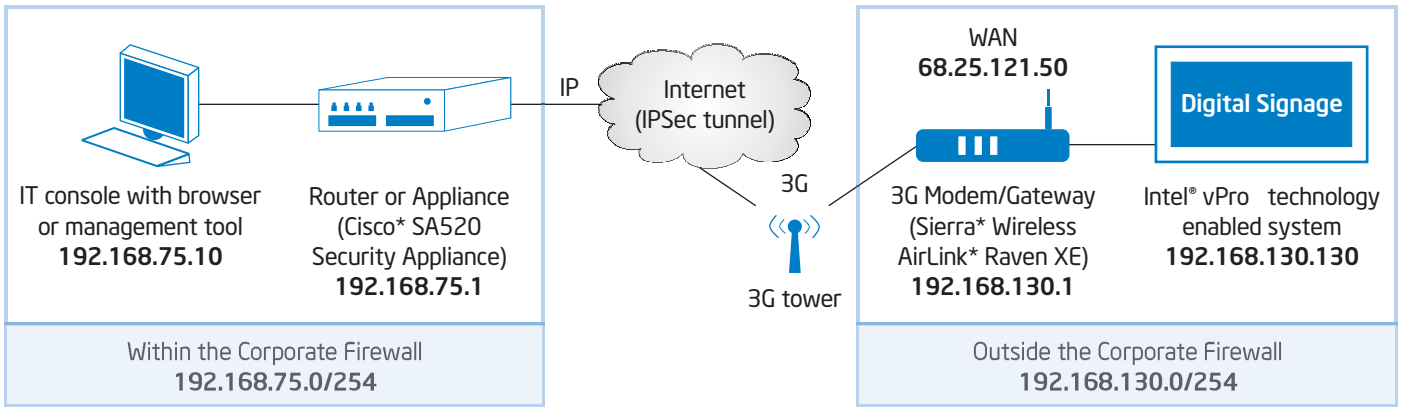

Figure 2. Network Diagram for the Configuration Example

modes of operation: modem and gateway. In modem mode, a system plugged into the Raven XE's Ethernet port will have the same IP address as the 3G WAN interface. In gateway mode, there is the option to set local static IP addresses for signage devices or enable its DHCP to assign dynamic IP addresses to one or more devices connected directly, or through a switch, to Raven XE. Consequently, gateway mode with DHCP enabled provides each digital signage system a dynamic IP address on the LAN behind the gateway, eliminating the need to add a router in order to create private LAN behind the Raven XE.

The configuration example uses gateway mode, which is the preferred option even though both modes were tested and are feasible. In modem mode, a VPN tunnel may not be required for discovery, but it is still preferable to have one for secure and encrypted communication. Also in the gateway mode, the IP addresses of the devices on the private LAN behind the gateway are only visible to console and devices on the other side of the tunnel; however, the IP address of a device connected directly to Raven in modem mode is visible to everyone over the network, which is not desirable from a security point of view.

This issue can be addressed by putting a router between the Raven XE and the device and making a VPN tunnel mandatory, but this solution is more expensive than using the gateway mode.

Cisco* SA520 Security Appliance

In its experiment, Intel used the base SA520 routing functions with VPN capability, whereas other implementations may be better served by a more comprehensive secure routing device with the capability to establish hundreds of VPN connections.

Provision the signage devices

An Intel vPro technology-enabled device must be Intel AMT provisioned before it can be managed using Intel AMT. This experiment provisioned the signage devices in manual mode with DHCP enabled. Other provisioning methods may be more appropriate, or selected as well, depending on the IT infrastructure, security requirements and other factors.

A list of recommended settings for a more secure configuration can be found in the Intel® AMT SDK. Some examples include using Kerberos authentication, utilizing redirection port rather than remote frame buffer (RFB) for KVM, and disabling KVM listener (to be enabled only when a session needs to be opened).

The router configuration steps are summarized in Table 1.

Results

Intel successfully managed a digital signage device across a VPN tunnel over a Sprint 3G network using WebUI and different consoles. Some of the use cases that were tested included OOB inventory and asset management, KVM, Boot to Bios, power control features, network isolation and IDE-R.

Signage Practically Anywhere

The return on investment for digital signage can drop significantly if even one onsite repair visit is required. With Intel AMT, technicians can fix more problems remotely, thus saving cost. This paper offers useful information for configuring and managing Intel AMT-enabled signage devices connected by 3G networks, which opens the door to deploying digital signage in areas where a wired Internet connection is not available.

For more information about Intel digital signage solutions, visit

www.intel.com/go/digitalsignage

Configuration Steps	Actions
Provision the signage devices	▪ Test the provisioning with WebUI to make sure the system is configured correctly.
Activate the 3G modem and configure it	▪ Connect the signage device to the modem. ▪ Set to use modem or gateway mode. ▪ Set static IP address or DHCP mode (applicable only in gateway mode). ▪ With DHCP mode, set local LAN address parameters.
Configure the router	▪ Connect the management console to the router. ▪ Setup WAN and LAN address parameters.
Configure VPN tunnel parameters on both the 3G Modem/Gateway and the router	▪ Make sure to use the correct local and remote WAN and LAN IP addresses. ▪ Use similar security protocol and algorithm parameters on both sides. ▪ Check the status to ensure the tunnel is established. Log files can be used to debug possible issues
Test the setup	▪ Ping the signage device and console from each other and verify the responses. ▪ Use WebUI or any Intel AMT-enabled management console to manage the signage device across the VPN tunnel.

Table 1. Router Configuration Steps

Overview of Appendices

The LAN/WAN and VPN configuration steps for the Sierra* 3G gateway and the Cisco* security appliance are described in appendices A-D. Since the gateway and firewall must communicate with each other, there are required certain fields in the VPN configuration tables that should contain the same information, as indicated by the "Match Value" columns. In other words, configuration steps having the same Match Value number should have the same value in their associated configuration fields. Additional information about the configuration steps is provided in the following text.

Appendix A: LAN Settings - Sierra* Wireless Airlink Raven XE 3G Modem

Step	Tab	Configuration Field	Value
1	LAN	Host Public Mode	"All Hosts Use Private IPs" (Gateway mode)
2	LAN	Starting IP	192.168.130.100
3	LAN	Ending IP	192.168.130.254

Step	Notes :
1	Host Public Mode: This field sets whether the device functions as a modem ("Ethernet Uses Public IP") or as a gateway ("All Hosts Use Private IPs").
2	Starting IP: Start of IP address range of the LAN for digital signage systems.
3	Ending IP: End of IP address range of the LAN for digital signage systems.

Table 2: LAN Configuration Example: Sierra* Wireless Airlink* Raven XE 3G Modem

Appendix B: WAN and LAN Settings - Cisco* SA520 Security Appliance

Step	Tab	Configuration Field	Value	Match Value
1	IPv4 WAN Configuration	IP Address Source	"Use Static IP Address"	
2	IPv4 WAN Configuration	IP Address	10.10.0.1	1
3	IPv4 LAN Configuration	Starting IP Address	192.168.75.100	
4	IPv4 LAN Configuration	Ending IP Address	192.168.75.254	

Step	Notes :
1	IP Address Source: This configuration example used "Use Static IP Address"; implementation dependent.
2	IP Address: Static IP address of the WAN for the router.
3	Starting IP Address: Start of IP address range of the LAN for the management console.
4	Ending IP Address: End of IP address range of the LAN for the management console.

Table 3: LAN Configuration Example: Cisco* SA520 Security Appliance

Appendix C: Modem VPN Settings - Sierra* Wireless Airlink* Raven XE 3G Modem				
Step	**Tab**	**Configuration Field**	**Value**	**Match Value**
1	VPN	VPN 1 Type	"IPSec Tunnel"	
2	VPN	VPN Gateway Address	10.10.0.1	1
3	VPN	Pre-shared Key 1	<Password>	2
4	VPN	My Identity	68.25.121.50	3
5	VPN	Peer Identity	10.10.0.1	1
6	VPN	Local Address Type	"Use the Host Subnet"	
7	VPN	Local Address	192.168.130.0	4
8	VPN	Local Address - Netmask	255.255.255.0	5
9	VPN	Remote Address	192.168.75.0	6
10	VPN	Remote Address - Netmask	255.255.255.0	7
11	VPN	IKE Encryption Algorithm	3DES	8
12	VPN	IKE Authentication Algorithm	SHA1	9

Step	Notes :
1	VPN 1 Type: Select "IPSec Tunnel".
2	VPN Gateway Address: This is the IP address of the WAN associated with the corporate router. Note: matching field in the router.
3	Pre-shared Key 1: Authentication key set by the user. Note: matching field in the router.
4	My Identity: IP address of the WAN associated with the Raven XE. Note: matching field in the router.
5	Peer Identity: This must match the value entered for step #5.
6	Local Address Type: Select "Use the Host Subnet".
7	Local Address: This is the IP address for the digital signage system. Note: matching field in the router.
8	Local Address - Netmask: This is the Netmask address of the LAN for the digital signage systems. Note: matching field in the router.
9	Remote Address: This is the IP address of the management console. Note: matching field in the router.
10	Remote Address – Netmask: This is the Netmask of the LAN for management console. Note: matching field in the firewall.
11	IKE Encryption Algorithm: 3DES used in the configuration. Recommend using AES128 or stronger encryption algorithm, if supported. Note: matching field in the router.
12	IKE Authentication Algorithm: SHA1 used in the configuration. Recommend using at least SHA2, if supported. Note: matching field in the router.

Table 4: Modem VPN Configuration Example: Sierra* Wireless Airlink* Raven XE 3G Modem

Appendix D: Router VPN Settings - Cisco* SA520 Security Appliance				
Step	**Tab**	**Configuration Field**	**Value**	**Match Value**
1	VPN Wizard	VPN Type	"Site-to-Site" (IPSec)	
2	VPN Wizard	Connection Name	<Name of 3G Modem>	
3	VPN Wizard	What is the pre-shared key?	<Password>	2
4	VPN Wizard	Remote WAN's IP Address/FQDN	68.25.121.50	3
5	VPN Wizard	Remote LAN IP Address	192.168.130.0	4
6	VPN Wizard	Remote LAN Subnet Mask	255.255.255.0	5
7	VPN Policy Configuration	Start IP Address	192.168.75.0	6
8	VPN Policy Configuration	Subnet Mask	255.255.255.0	7
9	VPN Wizard	Encryption Algorithm	3DES	8
10	VPN Wizard	Authentication Algorithm	SHA1	9

Step	Notes :
1	VPN Type: This configuration example used "Site-to-Site", IPSec tunnel.
2	Connection Name: Any name.
3	What is the pre-shared key?: Authentication key set by the user, and it must match the password for the 3G gateway.
4	Remote WAN's IP Address/FQDN: The IP address for the WAN associated with the 3G gateway.
5	Remote LAN IP Address: This is the base IP address of the LAN for the digital signage systems.
6	Remote LAN Subnet Mask: This is the subnet mask of the LAN for the digital signage system.
7	Start IP Address: This is the IP address of the LAN for the management console.
8	Subnet Mask: This is the subnet mask of the LAN for the management console.
9	Encryption Algorithm: 3DES used in the configuration example. Recommend using AES128 or stronger encryption algorithm, if supported.
10	Authentication Algorithm: SHA1 used in the configuration. Recommend using at least SHA2, if supported.

Table 5: Router VPN Configuration Example: Cisco* SA520 Security Appliance

[1] Source: DigitalSignageToday.com, "3G/4G Cellular-Based Digital Signage", 2010 NetWorld Alliance LLC.

[2] Intel® Active Management Technology (Intel® AMT) requires the computer system to have an Intel® AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see www.intel.com/technology/platform-technology/intel-amt/

Printed in USA 0311/TB/TM/PDF ♻ Please Recycle 324958-001US