Chapter 11

Connecting and Communicating with Intel® Active Management Technology

Disconnecting from change does not recapture the past. It loses the future.

— Kathleen Norris, *O Magazine*, January 2004

Once all of the features of Intel® Active Management Technology (Intel AMT) are understood, it's time to understand how to access them. Connectivity to Intel AMT is a large and important topic. Since Intel AMT uses out-of-band connectivity and a set of strong security measures along with many protocols, a good understanding of this topic is necessary in order to successfully use Intel AMT. Connectivity to Intel AMT is defined in detail in the Intel AMT SDK. This chapter provides an overview of the connectivity features, security features, and protocols used to communicate with Intel AMT. We will also look at connectivity from a software developer's point of view. When writing Intel AMT software, developers may want to support a wide range of Intel AMT versions and simplify as much as possible the process of connecting to Intel AMT. This chapter includes ideas for how to simplify the connection process and how to make the most of every version of Intel AMT going as far back as Intel AMT 1.0. This chapter assumes that Intel AMT has already been provisioned.

Connection

Intel asked and obtained from the Internet Assigned Numbers Authority (IANA) a set of reserved TCP ports for Intel AMT. These are TCP ports 16992 through 16995 and are intended to be used only with Intel AMT. Obtaining these reserved ports is important since Intel AMT will steal these ports from under the operating system.

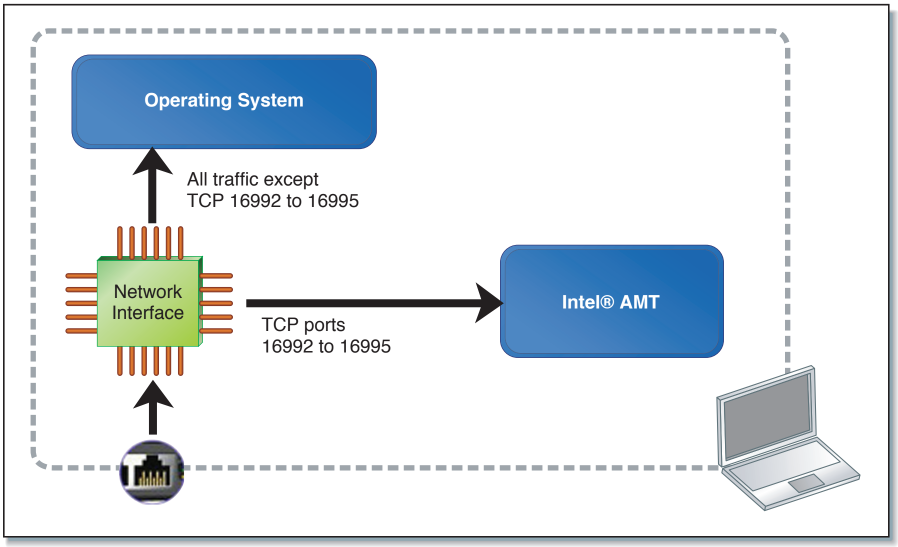

Figure 11.1 Operating System Gets All Traffic Except TCP Port 16992 to 16995

When Intel AMT is enabled in DHCP mode, inbound TCP connections to ports 16992 through 16995 are rerouted to Intel AMT using a hardware filter in the Ethernet adapter. As a result, if an application listens to port 16992 through 16995, it will never receive any inbound TCP connection.

On most versions of Intel AMT, if set to static IP mode, Intel AMT uses a separate MAC address and IP address for out-of-band communication. As a result, inbound TCP connections on ports 16992 through 16995 on the operating system's IP address will still work correctly.

We should also note that an application listening on TCP ports 16992 through 16995 could still receive TCP connections from other network adapters that are not enabled with Intel AMT and from the local OS loop-back adapter.

Port Usages

Now that we know how Intel AMT makes use of four special inbound ports, let's look at function each of these ports performs.

- 16992 – HTTP traffic
- 16993 – TLS secured HTTPS traffic
- 16994 – Serial-over-LAN and IDE Redirect
- 16995 – TLS Secured Serial-over-LAN and IDE Redirect

Ports 16992 and 16993 are identical except that on 16993, Transport Layer Security (TLS) must first be negotiated before useful traffic can flow. The same applies to 16994 and 16995, which are also identical except for TLS.

With Intel AMT, only TCP ports 16992/16994 are used when TLS is not configured; ports 16993/16995 are used when TLS is in use. A management console does not have a choice to use TLS or not. If TLS is configured on a given computer with Intel AMT, any attempts to connect to 16992 or 16994 will fail. The reverse is also true, if TLS is not configured, management consoles can't connect to ports 16993/16995.

The TLS protocol used with the secure communications with Intel AMT is the same TLS protocol used all over the Internet and is also built into most web browsers. When an administrator is attempting to access the Intel AMT Web page, it can do so with the following URL in any web browser:

Without TLS:

```
http://computername:16992
```

With TLS:

```
https://computername:16993
```

In all cases, once a secure TLS session is negotiated, the useful network traffic is the same as the non-TLS equivalent port.

The same TLS versus non-TLS usage also applies to ports 16994 and 16995 but because these ports use a proprietary binary protocol, special software[1] must be used to access these ports.

[1] The IMRSDK.dll library included in the Intel® AMT SDK is specifically intended to make use of port 16993 or 16995 for Serial-over-LAN and IDE Redirect services.

Authentication and Authorization

Once Intel AMT is set up, two of the four Intel AMT management ports are usually open and ready to receive connections from a management console. TCP connections on these ports can occur at any time. Before accepting any command from a management console, Intel AMT must first authenticate that the management console is authorized to perform such an operation. The authorization phase determines who the administrator is, and the authorization phase determines if this individual has appropriate rights to perform this action.

Authentication and authorization are probably the two single most critical operations for Intel AMT. Since some of the management features that are possible using Intel AMT could lead to computer data loss, it's important that only permitted administrators be allowed to perform management operations. Intel AMT uses an authentication system called HTTP-Digest[2] or Kerberos[3] used within the HTTP protocol. At a high level and without TLS, the steps are as follows:

- Receive a TCP/HTTP connection of port 16992.
- Use HTTP-Digest or Kerberos to authenticate the user.
- If the user is not in the Intel AMT user table, reject the connection.
- If the user does not have privileges to perform this operation, reject the operation.
- Perform the management operation.

With TLS, steps are added to the beginning of the session.

- Receive a TCP/HTTPS connection of port 16993.
- Intel AMT sends its own certificate to the console for validation.
- If policy requires, Intel AMT requests and checks that the console has a valid and trusted certificate.
- Use HTTP-Digest or Kerberos to authenticate the user.
- If the user is not in the Intel AMT user table, reject the connection.

[2] Defined in RFC 2617.

[3] Defined in RFC 4120.

- If the user does not have privileges to perform this operation, reject the operation.
- Perform the management operation.

The steps with TLS and without TLS are the same except that with TLS, there is an additional layer of security at the start of the session. Also with TLS, the entire session is fully encrypted, making it impossible for anyone else to listen in on the network conversion.

Ports 16994 and 16995 used for Serial-over-LAN and IDE Redirection use exactly the same steps but use a proprietary binary protocol instead of HTTP. If TLS is not used, password-based authentication on port 16994 will result in the password being sent in the clear on the network. This is why it's highly recommended that TLS always be used when performing serial-over-LAN or IDE Redirect operations.

Environment Detection

Even with all of the security care, authentication and authorization steps taken by Intel AMT, the simple fact that there are open ports waiting for outbound connections makes it possible for an external party to attempt an attack on Intel AMT. If a corporate user were connected on a hotel network, someone in a different room could scan the network for open Intel AMT ports and attempt to log into Intel AMT by guessing the password. Sometimes, just knowing that Intel AMT is present and active on a computer is sufficient to make it a target for other attacks or theft. This scenario is especially relevant for mobile platforms.

In order to protect from this and other types of attacks, Intel AMT 2.5 and higher include a feature called environment detection. The goal of this feature is to close all Intel AMT inbound ports when the computer is determined to be outside the corporate network. During provisioning, Intel AMT can set up one to four domain suffixes. For example: "intel.com" or "openamt.org" would both be valid values. Once set and activated, Intel AMT will only open inbound ports when it gets a DHCP address that ends with one of the known suffixes. In our example: "oregon.intel.com" would be okay, but "intel2.com" would not match and the ports would be closed.

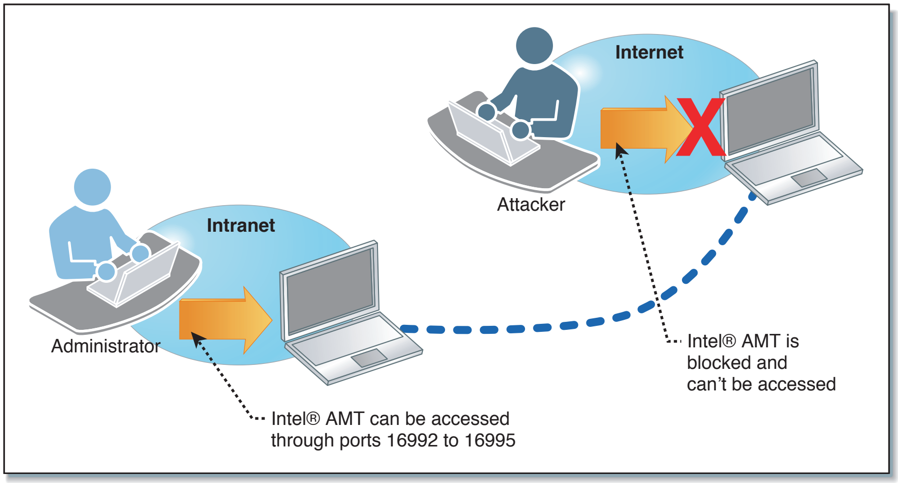
Internet
Attacker
Intranet
Administrator
Intel® AMT is blocked and can't be accessed
Intel® AMT can be accessed through ports 16992 to 16995

Figure 11.2 Computer Moving from Inside to Outside; Environment Detection Blocks Intel® AMT When Outside the Intranet

Proper use of the environment detection can restrict or completely eliminate the possibility of outsiders attempting to attach Intel AMT.

Intel® AMT VPN Flag

If a computer is connected to a network that is outside the managed corporate network and the environment detection feature is blocking inbound ports, it is still technically possible for an administrator to communicate with Intel AMT. When outside the corporate network, most corporations use virtual private network (VPN) software to allow a computer to join back into the corporate network using a secured connection.

Intel AMT 2.5 and above support an additional feature we will call the VPN flag. When provisioning Intel AMT, this flag can be set to enabled or disabled[4]. If enabled, Intel AMT will accept connections from an administration console through a VPN.

[4] Oddly, the VPN flag can be set but its current value can't be read back. Provisioning servers or consoles should simply set to VPN flag to the intended value.

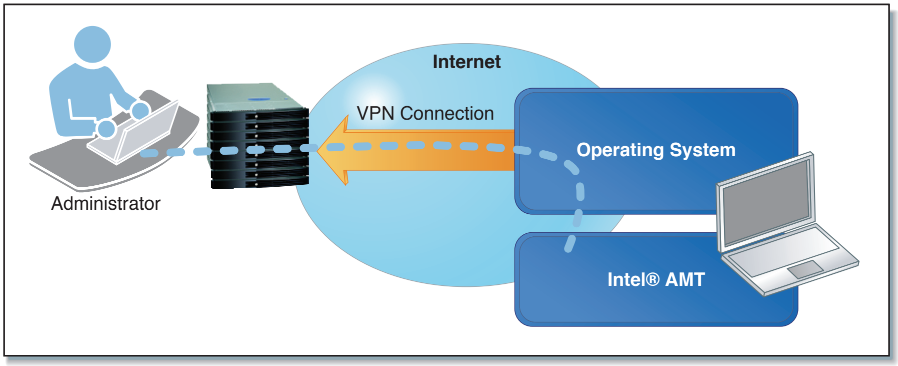

Figure 11.3 Intel® AMT Traffic over VPN

Since VPN software runs within the operating system, the management console would be connected to Intel AMT using an in-band channel. If for example the console reboots the computer remotely, connectivity would be lost. Using this feature is still interesting to configure and obtain monitoring data for Intel AMT, but it should not be used to attempt remote repair.

Starting with Intel AMT 4.0, a new client-initiated connection feature allows Intel AMT to communicate directly with a management console. This feature is covered in Chapter 12, "Internet Platform Management."

Local Host Access

In order for Intel AMT to function correctly, both remote applications such as management consoles and local applications such as agents need to communicate with Intel AMT.

As we indicated earlier in this chapter, Intel AMT intercepts TCP ports 16992 through 16995 for outside communications, but this only works when the network traffic comes from outside the computer and is rerouted to Intel AMT by the network interface. For communication with local applications, a completely different data path is used. Called the Intel Management Engine Interface (Intel MEI), it was also known as the Host Embedded Controller Interface (HECI). These days, Intel uses the name Intel MEI, but HECI may still be found in older documents.

Intel MEI is a driver that has a direct local communication path with Intel AMT. It does not use the operating system network stack; instead it's a direct set of request/response messages that Intel AMT understands. Local applications can use the Intel MEI driver to make a limited set of requests to Intel AMT. These requests are limited, but they don't need any authentication. They include such requests as: "What version of Intel AMT?" and "Is Intel AMT provisioned?" The Intel MEI driver can also route network packets to Intel AMT. Intel provides a background Microsoft Windows service called Local Management Service (LMS).

Both the Intel MEI driver and LMS are provided as part of the software drivers included with a platform. For Intel motherboards, users can find the latest version of the software on support.intel.com. For other vendor's platforms, go to that vendor's support Web site.

As shown in Figure 11.4, the LMS listens on ports 16992 and 19663 of the local computer and routes network traffic to Intel AMT using the Intel MEI. It's tempting to think that once Intel MEI and LMS are properly installed and running, the local port 16992/16993 are exactly equivalent to the same ports accessed from outside the computer, but this is not the case. There are significant differences in how Intel AMT handles local and remote traffic. First, the well known user friendly Web page is not available locally. As a result, pointing a browser to http://localhost:16992 or https://localhost:16993 on the local computer will result in a blank page. One of the biggest differences between local and remote interfaces is the Intel AMT functionality that is available.

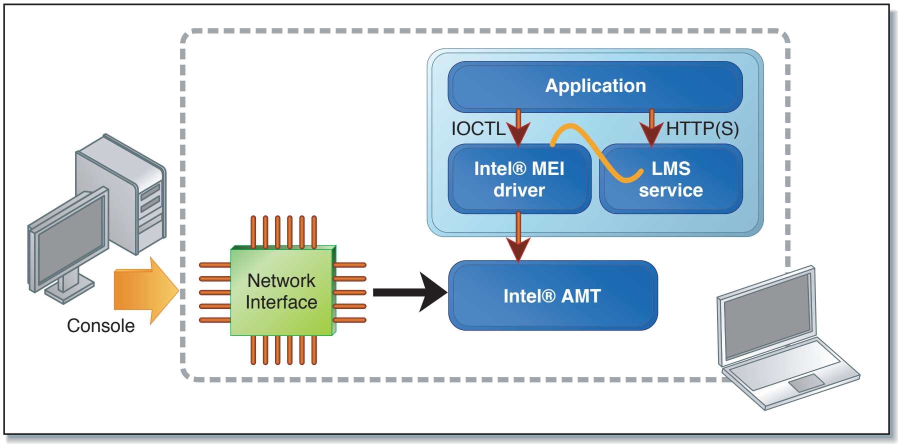

Figure 11.4 Local Management Service (LMS) Using the Intel® MEI Driver to Send Traffic to Intel® AMT

Both Local and Remote Services

- General information
- Third party storage
- Event log reader
- Firmware update
- User access control

Remote-Only Services

- Security administration
- Network administration
- Hardware asset
- Remote Control
- Event management
- Third party storage administration
- Disk redirection

- Remote agent presence
- System Defense
- Network time
- Wireless administration
- Endpoint access control administration
- Audit log
- Remote access

Local-Only Services

- Local agent presence
- Endpoint access control
- Local user notification

A decision was made when designing Intel AMT to restrict access to local services because applications running within the operating system are not trusted. In fact, they are being managed by Intel AMT. By restricting local access to services, we also limit the possibility of rogue applications trying to attack Intel AMT using the local interface.

Access to services provided to the local interface still requires that the local application authenticate to Intel AMT using the same authentication and authorization that is used for the remote interface. The same HTTP digest and optional TLS protocols can used to authenticate and possibly secure the session. Local users must still provide a username and password or Kerberos authentication to use local services. Even if the local user authenticates using the Intel AMT administrator credentials, only local services will be available.

When setting up Intel AMT, it's generally a good idea to create one or more separate, local-only user accounts within Intel AMT. This is because locally running applications may not store the account password properly. If not configured properly, a local user could find an Intel AMT username and password in the local Microsoft Windows registry and use it from a different computer to gain access to Intel AMT remote features. This is why it's especially important not to use a separate local-only account.

By separating the local and remote Intel AMT interfaces and user accounts, we create a separation between what is being managed and who is managing. It is also worth nothing that serial-over-LAN and IDE redirection services, along with ports 16993 and 16995, are not available locally.

Implementation of the VPN Flag

Earlier in this chapter, we covered the VPN flag feature and its benefits. Some readers may be wondering about the relationship between LMS listening on local ports and the VPN flag feature. When a management console connects to Intel AMT through a VPN, it will actually connect to the local LMS port and not the external Intel AMT port. As a result, the console should have access to the limited features offered by the local interface.

If the VPN flag is turned on, Intel AMT will start offering all of the remote services to the local interface only if the packets have a source address that is not a local IP address.

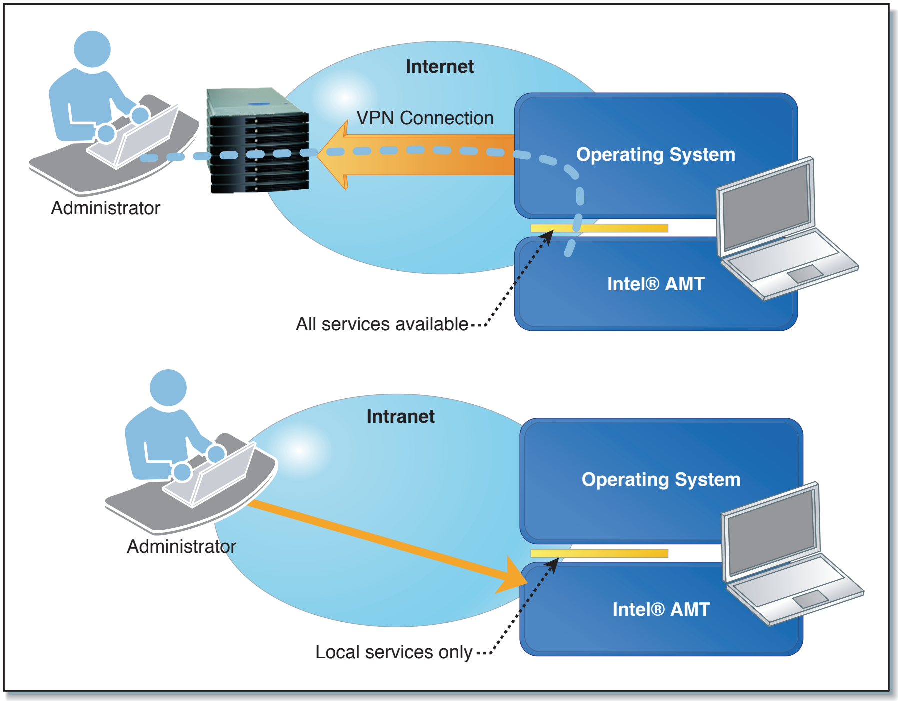

Figure 11.5 VPN Flag Enabled, Local and Remote

In other words, when the VPN flag is enabled, connections that originate from outside the local platform to LMS will be offered all of the remote services. Connections coming from the local loopback interface will still only have access to the limited set of local services.

The VPN flag feature preserves the limitation of the local interface while allowing management consoles to access all of the services and feature of Intel AMT when connecting through a VPN.

Summary

Connectivity to Intel AMT is as easy as connecting to any normal web server on the Internet. As with any web server, security considerations are very important. As we saw in this chapter, Intel AMT provides very robust authentication and privacy, along with an extra layer of protection when the computer is connected on a foreign network. The limited access to Intel AMT features through the local LMS interface/Intel ME interface makes it more difficult for local application to try to cause problems.

A good understanding of Intel AMT connectivity both locally and remotely is crucial for developers building both consoles and local agents that best take advantage of the features offered by Intel AMT.

In the next chapter, we will cover another connectivity option that is new with Intel AMT 4.0 and builds upon the concepts that we covered in this chapter.