Welcome to SNMP Research and thank you for investing the next few minutes of your time in this presentation.

Yes, we truly are located on a farm in the foothills of the Great Smoky Mountains.

Our company began in 1988. Today, SNMP Research is 'the' leading vendor of Internet Management technology based on industry standards.

Our primary business is creating, licensing, and supporting software for the management of networks, applications, and systems.

Our products are based on the SNMP protocols, v1, v2c and v3, and our products are available for both open systems such as LINUX, Windows, and Solaris and on over 30 embedded systems.

Now let's explore three main topics for a moment. (Next Slide)

The Simple Network Management Protocol (or SNMP) is the standard operations and maintenance protocol for the Internet. The Internet Engineering Task Force promoted the SNMPv3 protocol to full standard in 2002. This latest version of the SNMP protocol provides secure network management that goes beyond monitoring.

Dr. Jeff Case, our founder, is a recognized industry leader in the development of the SNMP protocols and his company, SNMP Research, is a name synonymous with secure Internet and network management based on industry standards.

Internet Protocol version 6 (IPv6) is a network layer protocol for packet switched networks. IPv6 is designated as the successor of the current Internet Protocol (IPv4). There are published government directives today requiring deployment for IPv6 in 2008. The Internet Protocol is the network communication layer that provides transport for SNMP protocol messages.

IPv6 support is included in SNMP Research core products on supported operating systems.

Our Distributed SNMP Security Pack with Remote Forwarder is an example of our implementation of Secure Internet Management using the SNMP protocols. The DSSP product family will be covered in greater detail later.

**Secure Internet Management
with SNMPv3 Protocol**

- **Authentication**
  What: Purported sender is in fact the sender
  How: MD5 or SHA-1 hash functions

- **Privacy**
  What: Message interpreted only by sender and recipient
  How: AES, DES and 3DES encryption algorithms

- **Administration**
  What: Protection level on a transaction by transaction basis
  How: Reconfiguration rather than redeployment

3

The SNMPv3 Protocol is an important enabling technology for Secure Internet Management.

By authentication, we mean the purported sender of a message is in fact the sender.

   Hashing techniques such as MD5 or SHA-1 are employed.

By privacy, we mean the message is understood only by the sender and the recipient.

   Encryption algorithms supported are DES, 3DES and AES.

By administration, we mean network administrators have the potential for transaction by transaction protection. Network reconfiguration can be accomplished in real time without redeployment.

In short, with SNMPv3 protocol, network communications occur between recognized entities, the messages are understood only by the proper entities and network administrators have real time control of network operations.
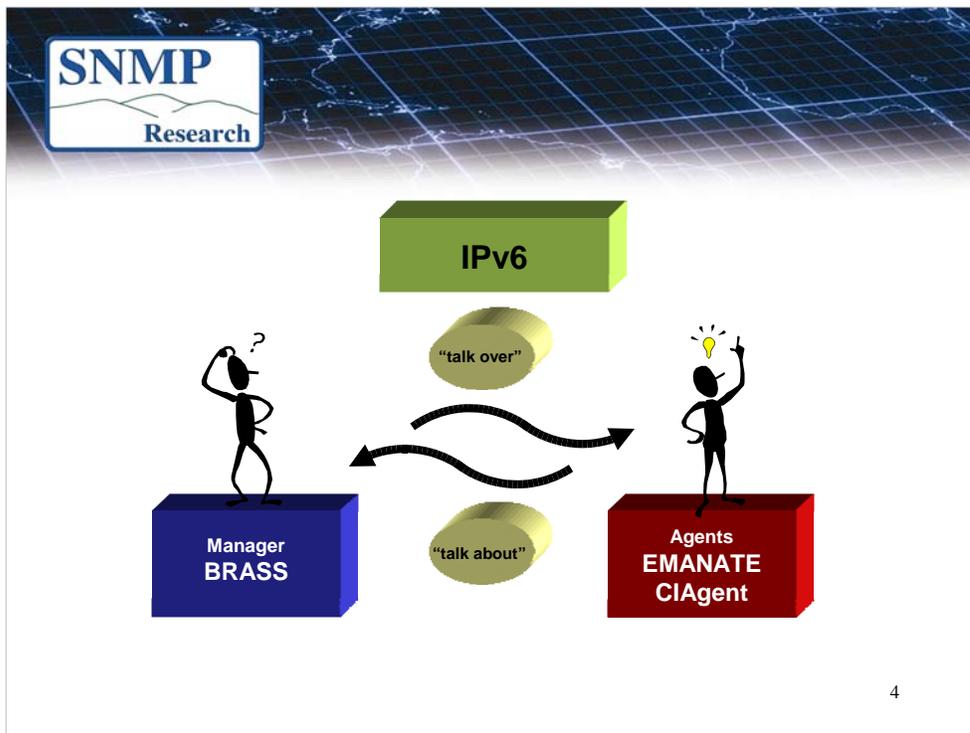
Let's focus for a moment on the IPv6 Internet Protocol.

The icon on your left, marked BRASS, represents a network manager application installed on a server.

The icon on your right, marked EMANATE®, represents the multiple devices in your network with a SNMP agent installed.

The communication link between the network manager application and network devices is the Internet Protocol IPv6.

We recognize two forms of communication: talk over and talk about.

Talk over means the SNMP agent can receive and respond to SNMP messages that are sent to it on an IPv6 transport. Talk over also means that the SNMP agent can transmit notifications to IPv6 addresses.

Talk about means that information about IPv6 interfaces and network activity is exposed by the agent in SNMP MIB objects. More on MIB objects in a moment.
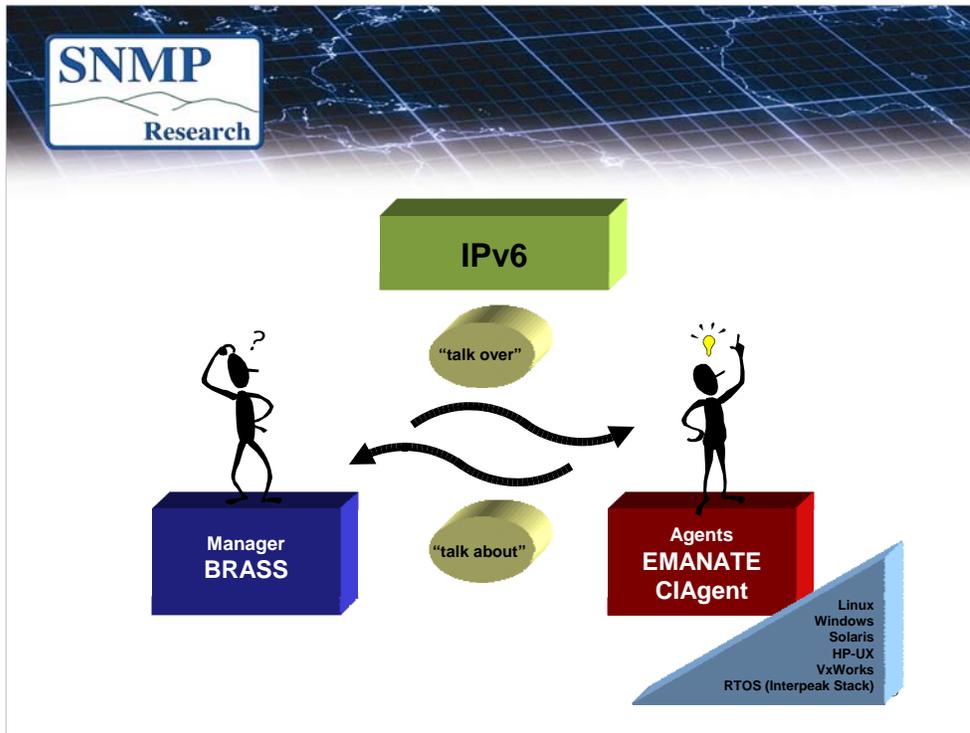
BRASS™ is our Management Application Toolkit that provides the facilities to create SNMP management applications. BRASS has been used to create our Distributed SNMP Security Pack™, an application that incorporates the SNMP v3 protocol for industry applications such as HP OpenView™, IBM NetView® and Concord eHealth™.

EMANATE® is our SNMP agent development product. EMANATE is a recognized industry standard that has been licensed by companies such as CISCO, Lucent® Technologies, and Siemens.

BRASS and EMANATE are available on the major open operating systems (Windows, Solaris, LINUX, HP/UX, AIX).

EMANATE in source form has been deployed on over 30 major embedded systems, including VxWorks®, MontaVista®, embedded Linux®.

"Talk Over" IPv4 vs. IPv6

32-bit IPv4 address

xxx xxx xxx xxx

xxx = 8 bits (Resulting in 4,294,967,296 unique IP addresses)

128-bit IPv6 address

← Network prefix → ← Interface ID →
(Describes network location) (Provides unique identifying number)

xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx

xxxx = 16 bits (Resulting in 340,282,366,920,938,463,374,607,432,768,211,458 unique IP addresses)

6

The Internet Engineering Task Force (IETF) became aware of the shortage of IPv4 addresses over a decade ago. IPv6 addresses this shortage.

With current IPv4 deployment, the address space is limited to around 4 billion unique IP addresses. IPv6 exponentially increases the address space by employing a 128-bit address.

Remember, talk over means the IPv6 network addresses are recognized by SNMP agents and managers.

IPv6 "Talk About"

- **Managed Objects (MIB) supported by SNMP Research**

    * IF-MIB (RFC 2863)
    * INET-ADDRESS-MIB (RFC 4001)
    * IP-MIB (RFC 4293)
    * TCP-MIB (RFC 4022)
    * UDP-MIB (RFC 4113)
    * IP-FORWARD-MIB (RFC 4292)

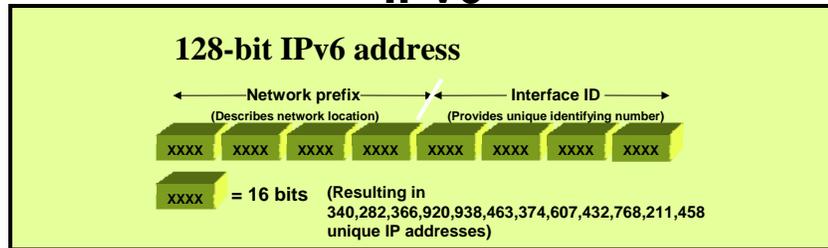- **Request For Comments (RFC) documents available at www.ietf.org**

7

Remember, from our earlier comments, that talk about means the SNMP agent exposes the IPv6 interfaces and network activity (termed managed objects) supported by the installed operating system. The definitions of these "managed objects" are found in Management Information Base documents (termed RFCs) published by the IETF.

Operating systems that support IPv6 managed objects at some level are Linux, Windows, HP-UX 11i, and Solaris. Consult your vendor for specific information.

For complete details about SNMP Research's "talk about" IPv6 extensions for a specific platform, contact SNMP Research and request the AGENT-CAPABILITIES statement for that particular operating system.

IPv6

128-bit IPv6 address

Network prefix
(Describes network location)

Interface ID
(Provides unique identifying number)

xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx

xxxx = 16 bits (Resulting in
340,282,366,920,938,463,374,607,432,768,211,458
unique IP addresses)

Talk About: EMANATE agent receives/sends SNMP messages in IPv6 packets

Talk Over: EMANATE agent supports IPv6 managed objects (MIBs) implemented by operating system

8

To review briefly,

- IPv6 extends the available address space for networks exponentially by using the 128- bit address space,

- Talk over means the SNMP agent can receive and send SNMP messages in an IPv6 packet, and

- Talk about means the SNMP agent supports IPv6 managed objects (called MIBs) implemented by the resident operating system

- **Supports SNMPv1, SNMPv2c, and SNMPv3**

- **Supports IPv6**

  talk over is platform independent
  talk about is platform dependent

Linux	Solaris
Windows	VxWorks
HP-UX	Real Time OS

- **Provides Master Agent/Subagent Development Architecture**

- **EMANATE Options:**

  CLI   Web Interface   XML
  Java

9

A key component in implementing Secure Internet Management is a robust SNMP agent development toolkit. As emphasized earlier, the SNMP Research EMANATE product is a recognized industry standard for agent development.

Specifically, EMANATE supports the SNMP version 1 and version 2c protocols for legacy applications and SNMP v3 protocol for advanced security features including authentication, privacy and network administration with dynamic deployment.

IPv6 support is available with our current EMANATE release and active development continues to keep pace with Ipv6 releases by the industry operating systems for both talk over and talk about features.

EMANATE produces the effect of multiple SNMP agents on a single platform through a modular and extensible master agent/subagent architecture. This architecture permits dynamic loading and unloading of subagents during run time.

Need a Command Line Interface or a web-based management interface for access to the MIB object data? How about support for XML or Java. These features are available with EMANATE.

DSSP Internet Management Appliance-RF is available for AIX, HP-UX, Linux, Solaris, and Windows.

10
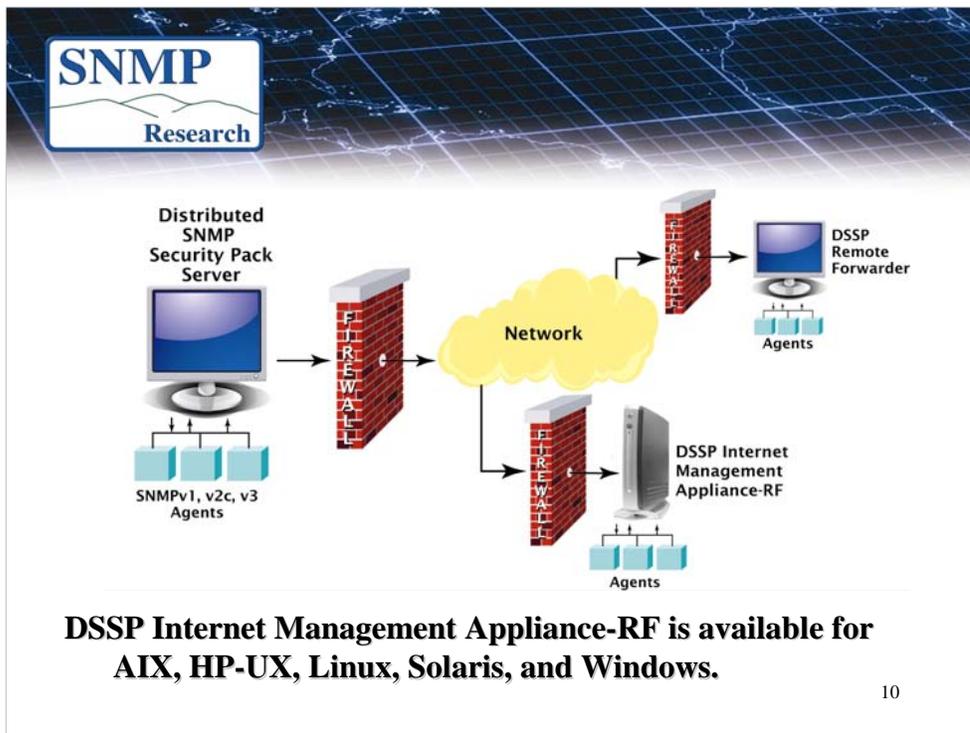
Let's now turn to our final topic, SNMP Research's BRASS management application represented here by our Distributed SNMP Security Pack.

There are three products in the DSSP family:

To your left, behind the red firewall, the DSSP Server provides support for SNMPv3 protocol to applications that do not natively support the SNMPv3 protocol. Industry applications such as IBM Netview, HP OpenView and Concord eHealth are integrated with the DSSP Server to add SNMPv3 protocol support.

The DSSP Remote Forwarder (upper right on your screen) will establish secure connections for SNMP managers through firewalls to all SNMP agents. The DSSP Remote Forwarder working with the DSSP Server enables network administrators to use the SNMP protocols for monitoring and control throughout their networks.

The DSSP Internet Management Appliance-RF (lower right) provides the DSSP Remote Forwarder application pre-installed on an embedded Linux platform. This newest member of the DSSP product family provides network administrators with the option of installing the DSSP Remote Forwarder application on an existing platform or on the stand alone embedded Linux appliance.

Our DSSP Remote Forwarder and DSSP Internet Management Appliance-RF offer these benefits for network management:

- Secure communication for multi-site networks

- SNMPv1 and v2c support for legacy systems and SNMPv3 protocol for advanced security

- These products are available on industry standard operating systems

- And offer deployment on existing servers or on a stand alone embedded Linux appliance.

Thank you for visiting with SNMP Research today.