Protocol for Carrying Authentication for Network Access (PANA) Requirements

Michael Schneider

Protocol for Carrying Authentication for Network Access (PANA) Requirements

Michael Schneider

Published 2004

Table of Contents

List of Figures

List of Tables

Foreword

The history of PANA, the temporary process of goals and milestones of PANA working group was just the other way round, than their order in this document will be. PANA working group submitted its first draft of requirements and terminology for PANA in February 2002. This was followed by further drafts of PANA interactions with PPP and 802.1x in May 2002 and finally the first draft of protocol specification in June 2002. In this document, first of all I will write about PANA and its working group's intention in general, followed by terminology and the PANA usage model. After this extended introduction to PANA in the first two chapters the third chapter will be about the actual topic of this document, the requirements of PANA. These requirements are fixed in an IETF internet-draft called "Protocol for Carrying Authentication for Network Access (PANA) Requirements". Its recent version number seven is from June 2003. I chose this order of topics, because it will be much easier for the reader to understand the requirements of PANA if he knows about PANA protocol, how it works and which were the intentions of PANA working group to come up with the idea of developing PANA.

Chapter 1. Introduction to PANA

1.1. Nowadays situation

Modern devices for IP technology do not have only a single way of gaining network connectivity. Instead, they achieve network access by a variety of technologies. Authentication methods exist for each kind of access, which deliver information between client and network in order to authenticate each other. Those technologies are not only restricted to certain access media, such as 802.1x for IEEE802 links, but also to specific network topologies, such as PPP for point-to-point links. Components of connectivity depend on link-layer connectivity, IP address configuration, on-link forwarding like ARP and neighbourhood discovery, in addition to off-link forwarding. The technologies currently used are inadequate and have a lack of security issues:

Technology	Issues
Door locks	Wireless network leaks No doors on street!
HTTP-based schemes	Requires user intervention
PPP	Only for point-to-point links
802.1x	Only for 802-family links

Table 1.1. Currently used technologies

1.2. Motivation for a new protocol

Nowadays networking world requires IP-devices to authenticate themselves before getting permission to access a network, means to get authorization to use it. To achieve this authentication a protocol is needed, which provides several authentication methods and furthermore special features that link-layer is not able to satisfy. Because of the absence of such mechanism, like a protocol for authorization in link-layer, non-standard and proprietary methods where used to get the needed functionality. Both, application-layer authentication methods (e.g. web-based registration) and additional layers between link-layer and network-layer where used, in addition to overloading existing network-layer's protocols to achieve the functionality of a missing authentication protocol. Instead of those non-standard inventions a network-layer protocol for authentication would be a much cleaner solution. An authentication protocol for a higher layer than link-layer is necessary, when functionality of link-layer authentication is not satisfying and does not meet the expected authentication and security requirements. Access control with authentication and authorization of the clients and the access networks is needed to provide secure network access, therefore a protocol is required which works as a transport for the authentication parameters between the client and the access network.

1.3. The goal and solutions of PANA working group

PANA working group's goal was to define or identify a carrier respectively a transport for a certain payload. This payload should ideally be an existing authentication protocol which meets the current requirements of network access authentication. The working group took care of the described problem and defined a protocol for clients using IP protocols to authenticate themselves to an access network in order to be granted network access, called PANA. Now a client can get access to a network's backend Authentication, Authorization and Accounting (AAA) infrastructure without knowing details about the used protocols and without having to use link-layer specific mechanisms. PANA also supports both multi-access and point-to-point links, as much as methods for authentication, dynamic service provider selection and roaming clients. Being a network-layer protocol, PANA does not depend on the kind of access and network topology, though it is a protocol between a terminal and a network node, a so called access point. This node can be part of an AAA infrastructure. As a conclusion, PANA provides a protocol that allows a host and a network to authenticate each other for network access.

1.4. What is NOT in the scope of PANA

After the facts about the reasons for the development of PANA, the goals and solutions PANA working group is working for, one has to delimit clearly which issues are not in the scope of PANA and will not be treated by PANA working group. So it was not the intention of PANA to develop a new security protocol and technologies belonging to such a protocol, like authentication and authorization mechanisms. Existing methods should be reused, such as the Extensible Authentication Protocol (EAP), and its features like key distribution and derivation methods. Note, that EAP may need to be extended to fulfil the requirements for PANA. But this extension is outside the scope of PANA. The protocol to be invented, PANA, can be considered as a front-end of the AAA protocol or any other protocol the network uses for authentication of its clients. PANA will be a carrier for an already existing security protocol or mechanism.

Chapter 2. Terminology and how PANA works

2.1. Terminology and short cuts

To understand the further discussion about the requirements of PANA and before that, the description of PANA usage model, here some short explanations to the components involved and required in PANA. There are five such components, PaC, PaCI, DI, PAA and EP, at which one will have a closer look at.

- PaC - PANA client;

  Provides the credentials to prove its identity for network access authorization. The PaC resides in a device which wants to get access to a network over the PAA and therefore has to identify itself.

- PaCI - PANA client identifier;

  This identifier is created by the PaC and sent to the PAA to identify and authenticate the PaC for network access.

- DI - Device identifier;

  A pointer to the client, used by the network to control and police network access. Dependent of the kind of access technology, the DI contains, for example, an IP address, a link-layer address or a switch port number.

- PAA - PANA authentication agent;

  The PAA verifies the credentials provided by a PaC and grants or denies access to the device, which is host of the PaC and identified by the DI. This is the counterpart to the PaC on the access network.

- EP - Enforcement point;

  A node on the access network where decisions on per-packet filtering rules for network traffic of the client device are implemented by using information of the DI, which is presented by the client (PaC) itself.

2.2. The PANA usage model

After this brief introduction to the components necessary for PANA, I will now show how those work together to achieve the needed functionality of authenticating a client to a network. PANA makes it possible for a terminal, the client, to log in to a network. This is controlled by the PAA. The terminal (PaC) must be able to find out the IP address of the PAA in order to connect it. Afterwards it starts authentication and transmits its data before a DI can be assigned. The PAA authenticates the PaC and provides network services. Like in the existing RADIUS system, the PAA has to provide control mechanisms for making filtering possible. For PANA, no new security mechanisms are developed, but existing ones are used. PANA is regarded as a front-end to an AAA-infrastructure or other protocols and acts like a carrier for current authentication methods. For example, Mobil IP Working group has already defined such a transport for Mobil IPv4. Mobil IPv4 can even be regarded as starting point for PANA, because therefore a carrier for transmission of data was developed, too. For PANA four different usage models can be defined in different network architectures according to the physical placement of PANA components.

- PAA co-located with EP but separated from AR

  The shape below shows the topology, where the Enforcement Point (EP), which controls access, and the PANA Authentication Agent (PAA) are located together. The PaCs, residing on different devices, communicate to the PAA to be authenticated. The job of PANA in this logical topology is to carry the authentication data from PaC to PAA, which is responsible for checking this data, granting or denying network access to the PaC and sending a positive or negative message back to the client (PaC) after verification of the credentials (authentication data). PANA however is only responsible for a secure transport of those credentials and the methods to verify them, but not at all for the verification itself.

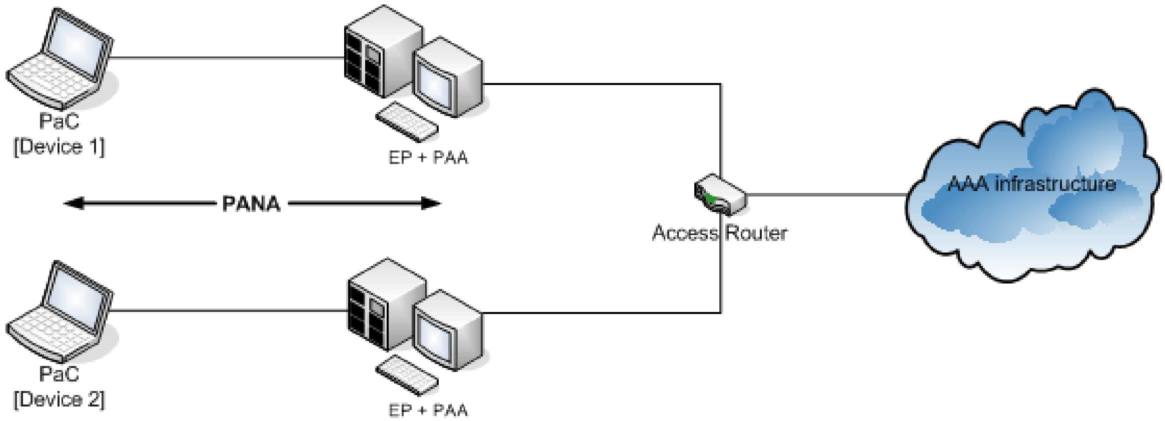

Figure 2.1. PAA co-located with EP but separated from AR

- PAA co-located with AR but separated from EP

The second scenario, described by the figure below, shows that PAA and the first-hop access router are located together. Both are separated from the EP, which is located between themselves and a PaC on a certain device. Here, the same authentication data, like in scenario 1, is sent from PaCs to PAA. But, if the first attempt of authentication was successful, parameters for access control, according to the PaC, have to be distributed to the corresponding EPs, in order to grant network access to the device, on which the PaC is authenticated. In this case, PANA is only carrier of authentication data and methods, too. Additionally a further protocol is needed to transport those parameters for access control between PAA and EP.

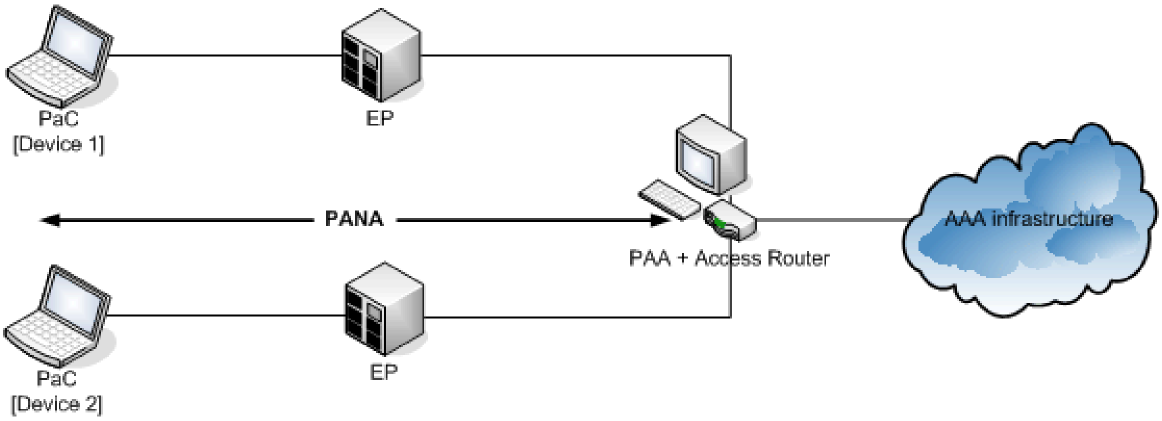

Figure 2.2. PAA co-located with AR but separated from EP

- PAA co-located with EP and AR

The figure below shows that EP, PAA and the access router, which provides routing and access control in this case, are united in one single location. The messages between PaC and PAA are still the same und have to be verified by the PAA. Like in the other scenarios, PANA is only carrier.

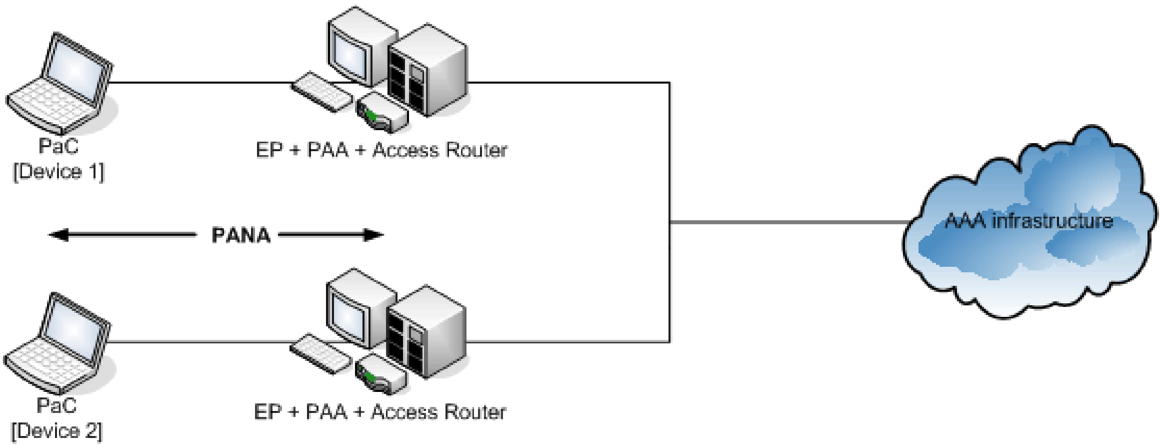

Figure 2.3. PAA co-located with EP and AR

- PAA separated from EP and AR

EP, PAA and AR each are standalone instances. The separate PAA, however, has to be on the same IP range. Similar to the scenarios before, the PaC exchanges messages with the PAA. After successful authentication of the PaC by the PAA, the access control parameters have to be distributed, over a separate protocol, to the corresponding EPs, similar to scenario two. As usual, this is not the job of PANA.

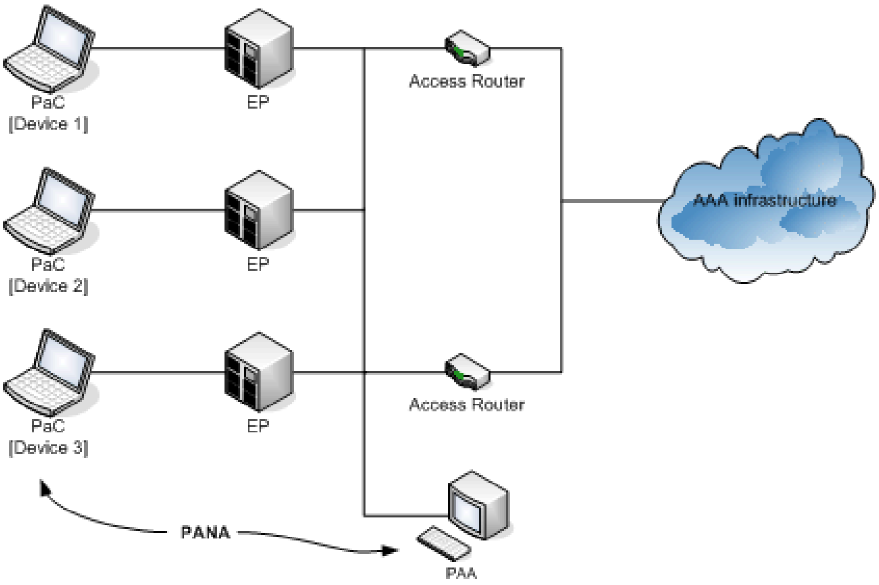

Figure 2.4. PAA separated from EP and AR

Chapter 3. Requirements of PANA

After this extended introduction to PANA itself and the corresponding usage models, the third chapter of this document is about the requirements of PANA and what is expected from PANA.

3.1. Authentication

Authentication of the PaC through authentication data, provided by the device, which wants to access the network, must be offered by PANA. Network access may only be granted to a device, which was identified by a DI, like IP address, link-layer address or even the port number of a switch. Like the DI as an identifier for the device accessing the network, the PaCI is the identifier for the PaC residing on this device. Those two identifiers, the DI and the PaCI, must be recognized as corresponding by the PAA, for example by communication them to the PAA during protocol exchange, and they are used for access control. The job of PANA must not be the definition of new security protocols, but PANA has to be a means of transport for a protocol like the Extensible Authentication Protocol (EAP). EAP would be a good choice for enabling authentication, however, the requirements EAP imposes to its carriers, must be satisfied to grant correct operation. Key derivation and distribution, which is actually not the job of PANA, but necessary for link-layer or network-layer security, must be provided by the protocol carried by PANA, e.g. EAP. The mechanism or protocol, used for authentication on the backend, like an AAA infrastructure, does not touch PANA and PANA must be independent from the technology used there. With PANA, the client (PaC) and the PAA must be able to authenticate and re-authenticate each other. Re-authentication can be periodic or initiated by PaC or PAA. One way authentication of the PaC by the PAA might be sufficient, if there is physical security provided by the network. The DI must be exchanged in a secure way between the PaC and the PAA in order to minimize the risk of man-in-the-middle attacks.

After successful authentication of a client, its device must be authorized for accessing the network to be able to sent and receive IP packets. This, confirming the authorization of a PaC, is the most important intention of PANA. Hiding privacy of PaC from visited networks is not the job of PANA, even if this could erroneously be expected from PANA.

3.2. IP address assignment

A PANA client (PaC) is not required to be configured with an IP address before using PANA, instead any other identifier should be used. This increases complexity of using PANA, but simply assigning an IP address to a not yet authenticated PaC would be a risk. Attacks like IP address depletion, especially on the minor address space of IPv4, in comparison to IPv6, could be launched when communicating an address to the PaC.

3.3. PAA-to-EP Protocol

As we have seen in chapter two, it is not obligatory, that PAA and Enforcement Point (EP) are tied together in one location, but are separated. In this situation a secure means of transportation between PAA and EP is needed for the creation of control lists, which make it possible to authorized and before authenticated clients to sent and receive packets on the network. Therefore, PANA working group has to specify an existing protocol solution to carry authorization data from the PAA to one or more separated EPs, in order to set up filtering policies controlling network access of the PaCs. Both, the so called pull model and push model, describing the initiator of communication between PAA and EP, may be essential. The pull model regards EP as initiator of PAA-to-EP communication; push model communication is initiated by PAA. As a consumption, the PAA has to tell the EP, which traffic may be generated by a authorized PaC, the so called filtering rules, and this communication has to be secure. Afterwards the EP has to control this rules for each PaC.

3.4. Network

According to network issues, the requirements of PANA belong to the location of the PAA, in addition to the indication of a disconnected PaC and to the kind of channel between PaC and PAA, which has to be secure. A further requirement belongs to the number of network interfaces of the PaCs, which must be able to have more than one of those. PANA even has to come up with functionality for more than one router in a network and multi-access links instead of point-to-point links.

Furthermore, it would be desirable if PANA provides a mechanism, which indicates the PAA that a PaC is disconnected and has left the network, in order to free resources and tell the enforcement point(s), that a certain PaC is no longer online. This indication could be initiated by the PaC informing the PAA, or, if the PaC is not able to send such a disconnect message, the PAA can be informed about the departure of a PaC by regularly sending authentication requests. To avoid denial-of-service attacks, sending disconnect indication messages must be secure, because this information could be used to launch an attack. The other way round, the PaC should be able to be told that network service is no longer available. The danger of possible denial-of-service attacks just imposes one more requirement. PANA consequently has to be resistant against such assault attempts.

A further requirement for PANA is that PAA and PaC may not be divided by an IP router. This means that they are one IP hop away from each other, and no router may be located between both. This one hop distance offers many possibilities to the PaC of finding out the IP address of the PAA, if it doesn't know it, like multicast or anycast.

As we have seen above, the communication between PaC and PAA has to be secure to avoid certain kinds of attacks like eavesdropping and spoofing. This security has to be provided by

PANA and may not be considered as already existing. In order to achieve a secure channel, applying EAP can be very useful. Satisfying methods for mutual authentication, key derivation and distribution are features of EAP, in addition to many further authentication methods.

3.5. Interaction with Other Protocols

Another clear but important requirement of PANA is co-existence next to other protocols like Mobile IPv4 and Mobile IPv6. These and other mobility management protocols may not be obstructed or influenced by PANA. Moreover, PANA has to work and operate independently with both, IPv4 and IPv6.

3.6. Congestion Control and Performance

In order to keep PaCs in a network from all together starting authentication at the same time, e.g. if they are all just starting up after a power blackout, PANA has to offer a mechanism to regulate the amount of verification traffic. This same-time-start-up problem can be solved by delayed initialization, forcing the clients (PaCs) to wait a random time delay before trying to send an authentication request to the PAA. Nevertheless, PANA has to stay efficient without performance decrease to realize short responding times when authenticating PaCs.

Chapter 4. Conclusion

As one could see in this document, it is really necessary to achieve a clean and secure solution for getting network access. Therefore, the possibilities, offered by link layer, are not at all satisfying, and so a higher layer protocol is needed to realize this. Instead of already used ad-hoc and inadequate non-standard solutions, PANA now provides a clean and secure mechanism, based on the network layer for secure network access.

Bibliography

IETF internet drafts

[1] Yoshihiro Ohba, Reinaldo Penno, George Tsirtsis, and Cliff Wang. Copyright © 2003 The Internet Society. Alper E. Yegin. *Protocol for Carrying Authentication for Network Access (PANA) Requirements*.

[2] L. Blunk, Merit Network, Inc, J. Vollbrecht, Vollbrecht Consulting LLC, B. Aboba, Microsoft, J. Carlson, and Sun. Copyright © 2004 The Internet Society. H. Levkowetz. *Extensible Authentication Protocol (EAP)*.

Internet Documents

[3] Yacine Rebahi and Dorgham Sisalem. *EVOLUTE's AAA Infrastructure*. Comparison between Radius and Diameter.

[4] IETF Secretariat. *Authentication, Authorization and Accounting (aaa)*.

[5] N. Asokan, Kaisa Nyberg, Valtteri Niemi, and Nokia Research Center. Copyright © 2003 Cambridge Security Protocols Workshop. *Man-in-the-middle in Tunnelled Authentication*.

[6] Alper E. Yegin. Copyright © 2002 DoCoMo USA Labs. *Secure Network Access*.

[7] Yacine El Mghazli. *PAA-2-EP Protocol*. PANA wg - IETF 58 Minneapolis.

[8] Yacine El Mghazli. *PAA-EP protocol considerations*. PANA wg - IETF 57 Vienna.

[9] Yoshihiro Ohba, Reinaldo Penno, George Tsirtsis, Cliff Wang, and Alper E. Yegin. *PANA Requirements and Terminology*. IETF53.

Glossary

A

Authentication, Authorization and Accounting

These are the three basic issues that are encountered frequently in many network services. Examples of these services are dial in access to Internet, electronic commerce, Internet printing, and Mobile IP.

Anycast

Anycast is a kind of addressing, where exactly one address out of a group of computers is reached.Es antwortet der Rechner, der am besten (schnellsten) erreichbar ist. Anycasts sind eine Neuerung bei IPv6 und ansonsten noch wenig verbreitet. Anycast sind sehr praktisch, da man eine ganze Gruppe von Geräten (z.B. DNS-Server oder Router) zusammenfassen kann. Eine Anfrage beantwortet dann immer der Rechner, der am schnellsten erreichbar ist.

Address Resolution Protocol

In computer networking using the internet protocol suite, the Address Resolution Protocol is a method for finding a host's Ethernet (MAC) address from its IP address. The sender broadcasts an ARP packet containing the Internet address of another host and waits for it (or some other host) to send back its Ethernet address. Each host maintains a cache of address translations to reduce delay and loading. ARP allows the Internet address to be independent of the Ethernet address but it only works if all hosts support it. ARP is defined in RFC 826 .

Authentication

The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization , which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

Authorization

The process of granting or denying access to a network resource. Most computer security systems are based on a two-step process. The first stage is authentication, which ensures that a user is who he or she claims to be. The second stage is authorization, which allows the user access to various resources based on the user's identity.

D

Device Identifier

A pointer to the client, used by the network to control and police network access.

E

Enforcement Point

A node on the access network where decisions on per-packet filtering rules for network traffic of the client device are implemented.

Eavesdropping

Eavesdropping is the secret listening of others conversations without their consent.

I

Internet Engineering Task Force

Internet Engineering Task Force, the main standards organization for the Internet. The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual.

IEEE802

The IEEE 802 LAN/MAN Standards Committee (LMSC) is a committee within the IEEE that develops local area network standards and metropolitan area network standards. The most widely used standards are for the Ethernet family, Token Ring, Wireless LAN, Bridging and Virtual Bridged LANs. An individual Working Group provides the focus for each area.

IPv4

IPv4 is version 4 of the Internet Protocol (IP). It was the first version of the Internet Protocol to be widely deployed, and forms the basis for the current (as of 2004) Internet. IPv4 addresses are written in Dot-decimal notation. Here's an example: 127.0.0.1. IPv4 uses 32-bit addresses, limiting it to 4,294,967,296 unique addresses, many of which are dedicated to local networks. This limitation has helped stimulate the push towards IPv6, which is currently in the early stages of deployment, and is expected to eventually replace IPv4.

IPv6

IPv6 is version 6 of the Internet Protocol. IPv6 is intended to replace the previous standard, IPv4, which only supports up to about 4 billion (4 × 109) addresses, whereas IPv6 supports up to about 3.4 × 1038 addresses. IPv6 is the second version of the Internet Protocol to be widely deployed, and is expected (as of 2001) to form the basis for future expansion of the Internet. In 2003, Nihon Keizai Shimbun (as cited in CNET Asia Staff, 2003) reported that Japan, China, and South Korea claimed to have made themselves determined to become the leading nations in internet technology, which would partially take the form of jointly developing IPv6, and completely adopting IPv6 starting in 2005.

M

Multicast

To transmit a single message to a select group of recipients. A simple example of multicasting is sending an e-mail message to a mailing list. Teleconferencing and videoconferencing also use multicasting, but require more robust protocols and networks. Standards are being developed to support multicasting over a TCP/IP network such as the Internet. These standards, IP Multicast and Mbone, will allow users to easily join multicast groups.

P

PANA

Protocol for Carrying Authentication for Network Access

PANA Authentication Agent

The PAA verifies the credentials provided by a PaC and grants or denies network access to a device.

PANA Client

Provides the credentials to prove its identity for network access authorization.

PANA Client Identifier

This identifier is created by the PaC and sent to the PAA to identify and authenticate the PaC for network access.

Point to Point Protocol

Point-to-Point Protocol, a method of connecting a computer to the Internet. PPP is more stable than the older SLIP protocol and provides error checking features. Working in the data link layer of the OSI model, PPP sends the computer's TCP/IP packets to a server that puts them onto the Internet.

R

RADIUS

Radius (Remote Authentication Dial In User Service) is an authentication, authorization and accounting client-server protocol between a NAS (Network Access Server) and a centralized Radius server. Radius is an open protocol and is distributed as source code.This protocol is based on the UDP transport protocol.

S

IP Spoofing

A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host.