**TCP/IP Tutorial and**

**Technical Overview.**

* [**https://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf**](https://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf) (Cap. 1, 3, 4, 5, 12, 17, 22 y 24)

### 1.1 TCP/IP architectural model

The TCP/IP protocol suite is so named for two of its most important protocols:

Transmission Control Protocol (TCP) and Internet Protocol (IP). A less used

name for it is the Internet Protocol Suite, which is the phrase used in official Internet standards documents. In this book, we use the more common, shorter term, TCP/IP, to refer to the entire protocol suite.

#### 1.1.1 Internetworking

The main design goal of TCP/IP was to build an interconnection of networks, referred to as an *internetwork*, or *internet*, that provided universal communication services over heterogeneous physical networks. The clear benefit of such an internetwork is the enabling of communication between hosts on different networks, perhaps separated by a large geographical area.

The words internetwork and internet are simply a contraction of the phrase interconnected network. However, when written with a capital “I”, the Internet refers to the worldwide set of interconnected networks. Therefore, the Internet is an internet, but the reverse does not apply. The Internet is sometimes called the *connected Internet*.

The Internet consists of the following groups of networks:

Backbones: Large networks that exist primarily to interconnect other networks. Also known as network access points (NAPs) or Internet Exchange Points (IXPs). Currently, the backbones consist of commercial entities.

Regional networks connecting, for example, universities and colleges.

Commercial networks providing access to the backbones to subscribers, and networks owned by commercial organizations for internal use that also have connections to the Internet.

Local networks, such as campus-wide university networks.

In most cases, networks are limited in size by the number of users that can belong to the network, by the maximum geographical distance that the network can span, or by the applicability of the network to certain environments. For example, an Ethernet network is inherently limited in terms of geographical size. Therefore, the ability to interconnect a large number of networks in some

hierarchical and organized fashion enables the communication of any two hosts belonging to this internetwork.

Figure 1-1 shows two examples of internets. Each consists of two or more physical networks.

rconnected by a

Two networks inte

rou

ter

equals

Internet A

Router

R

One

Virtual

Network

Netw

ork 1

Network 2

Router

R

Net

work 3

Netw

ork 1

Network 2

Router

R

Multiple network

s interconnected by routers

(

also seen as 1 virtual network, an Internet

)

*Figure 1-1 Internet examples: Two interconnected sets of networks, each seen as one logical network*

Another important aspect of TCP/IP internetworking is the creation of a standardized abstraction of the communication mechanisms provided by each type of network. Each physical network has its own technology-dependent communication interface, in the form of a programming interface that provides basic communication functions (primitives). TCP/IP provides communication services that run between the programming interface of a physical network and user applications. It enables a common interface for these applications, independent of the underlying physical network. The architecture of the physical network is therefore hidden from the user and from the developer of the application. The application need only code to the standardized communication abstraction to be able to function under any type of physical network and operating platform.

As is evident in Figure 1-1, to be able to interconnect two networks, we need a computer that is attached to both networks and can forward data packets from one network to the other; such a machine is called a router. The term IP router is also used because the routing function is part of the Internet Protocol portion of the TCP/IP protocol suite (see 1.1.2, “The TCP/IP protocol layers” on page 6).

To be able to identify a host within the internetwork, each host is assigned an address, called the IP address. When a host has multiple network adapters (interfaces), such as with a router, each interface has a unique IP address. The IP address consists of two parts:

IP address = <network number><host number>

The network number part of the IP address identifies the network within the internet and is assigned by a central authority and is unique throughout the internet. The authority for assigning the host number part of the IP address resides with the organization that controls the network identified by the network number. We describe the addressing scheme in detail in 3.1.1, “IP addressing” on page 68.

#### 1.1.2 The TCP/IP protocol layers

Like most networking software, TCP/IP is modeled in layers. This layered representation leads to the term protocol stack, which refers to the stack of layers in the protocol suite. It can be used for positioning (but not for functionally comparing) the TCP/IP protocol suite against others, such as Systems Network Architecture (SNA) and the Open System Interconnection (OSI) model. Functional comparisons cannot easily be extracted from this, because there are basic differences in the layered models used by the different protocol suites.

By dividing the communication software into layers, the protocol stack allows for division of labor, ease of implementation and code testing, and the ability to develop alternative layer implementations. Layers communicate with those above and below via concise interfaces. In this regard, a layer provides a service for the layer directly above it and makes use of services provided by the layer directly below it. For example, the IP layer provides the ability to transfer data from one host to another without any guarantee to reliable delivery or duplicate suppression. Transport protocols such as TCP make use of this service to provide applications with reliable, in-order, data stream delivery.

Figure 1-2 shows how the TCP/IP protocols are modeled in four layers.

Applications

Transport

Internetwork

Network Interface

and

Hardware

Applications

TCP/UDP

ICMP

IP

ARP/RARP

Network Interface

and Hardware

.......

.......

.......

.......

*Figure 1-2 The TCP/IP protocol stack: Each layer represents a package of functions* These layers include:

|  |  |
| --- | --- |
| **Application layer** | The application layer is provided by the program that uses TCP/IP for communication. An application is a user process cooperating with another process usually on a different host (there is also a benefit to application communication within a single host). Examples of applications include Telnet and the File Transfer Protocol (FTP). The interface between the application and transport layers is defined by port numbers and sockets, which we describe in more detail in 4.1, “Ports and sockets” on page 144. |
| **Transport layer** | The transport layer provides the end-to-end data transfer by delivering data from an application to its remote peer. Multiple applications can be supported simultaneously. The most-used transport layer protocol is the Transmission Control Protocol (TCP), which provides connection-oriented reliable data delivery, duplicate data suppression, congestion control, and flow control. We discuss this in more detail in 4.3, “Transmission Control Protocol (TCP)” on    page 149. |

Another transport layer protocol is the User Datagram Protocol (see 4.2, “User Datagram Protocol (UDP)” on page 146). It provides connectionless, unreliable, best-effort service. As a result, applications using UDP as the transport protocol have to provide their own end-to-end integrity, flow control, and congestion control, if desired. Usually, UDP is used by applications that need a fast transport mechanism and can tolerate the loss of some data.

|  |  |
| --- | --- |
| **Internetwork layer** | The internetwork layer, also called the *internet layer* or the *network layer*, provides the “virtual network” image of an internet (this layer shields the higher levels from the physical network architecture below it). Internet Protocol (IP) is the most important protocol in this layer. It is a connectionless protocol that does not assume reliability from lower layers. IP does *not* provide reliability, flow control, or error recovery. These functions must be provided at a higher level.  IP provides a routing function that attempts to deliver transmitted messages to their destination. We discuss IP in detail in Chapter 3, “Internetworking protocols” on page 67. A message unit in an IP network is called an *IP datagram*. This is the basic unit of information transmitted across TCP/IP networks. Other internetwork-layer protocols are IP, ICMP, IGMP, ARP, and RARP. |
| **Network interface layer** The network interface layer, also called the *link layer* or the *data-link layer*, is the interface to the actual network hardware. This interface may or may not provide reliable delivery, and may be packet or stream oriented. In fact, TCP/IP does not specify any protocol here, but can use almost any network interface available, which illustrates the flexibility of the IP layer. Examples are IEEE 802.2, X.25 (which is reliable in itself), ATM, FDDI, and even SNA. We discuss some physical networks and interfaces in Chapter 2, “Network interfaces” on page 29. | |

TCP/IP specifications do not describe or standardize any network-layer protocols per se; they only standardize ways of accessing those protocols from the internetwork layer.

A more detailed layering model is included in Figure 1-3.

Applications

Transport

Internetwork

Network Interface

and Hardware

SMTP, Telnet, FTP, Gopher...

UDP

TCP

IP

ICMP

ARPRARP

Ethernet, Token-Ring, FDDI, X.25, Wireless, Async, ATM,

SNA...

*Figure 1-3 Detailed architectural model*

#### 1.1.3 TCP/IP applications

The highest-level protocols within the TCP/IP protocol stack are application protocols. They communicate with applications on other internet hosts and are the user-visible interface to the TCP/IP protocol suite.

All application protocols have some characteristics in common:

They can be user-written applications or applications standardized and shipped with the TCP/IP product. Indeed, the TCP/IP protocol suite includes application protocols such as:

* Telnet for interactive terminal access to remote internet hosts
* File Transfer Protocol (FTP) for high-speed disk-to-disk file transfers
* Simple Mail Transfer Protocol (SMTP) as an internet mailing system

These are some of the most widely implemented application protocols, but many others exist. Each particular TCP/IP implementation will include a lesser or greater set of application protocols.

They use either UDP or TCP as a transport mechanism. Remember that UDP is unreliable and offers no flow-control, so in this case, the application has to provide its own error recovery, flow control, and congestion control functionality. It is often easier to build applications on top of TCP because it is a reliable stream, connection-oriented, congestion-friendly, flow control-enabled protocol. As a result, most application protocols will use TCP, but there are applications built on UDP to achieve better performance through increased protocol efficiencies.

Most applications use the client/server model of interaction.

##### The client/server model

TCP is a peer-to-peer, connection-oriented protocol. There are no master/subordinate relationships. The applications, however, typically use a client/server model for communications, as demonstrated in Figure 1-4.

A *server* is an application that offers a service to internet users. A *client* is a requester of a service. An application consists of both a server and a client part, which can run on the same or on different systems. Users usually invoke the client part of the application, which builds a *request* for a particular service and sends it to the server part of the application using TCP/IP as a transport vehicle.

The server is a program that receives a request, performs the required service, and sends back the results in a *reply*. A server can usually deal with multiple requests and multiple requesting clients at the same time.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | |  | |  | | |  | |  | | |  | |
|  | Cli  A | ent |  |  |  | Client  B | |  | ..... |  | Server | |  |  |
|  | TC | P/IP |  | TCP/IP | |  | TCP/IP | |
|  |  |  |  |  |  |  |  |  |
|  |  | |  |  | |  |  | |
|  | | Internet Network | | | | | | | |  | | | |

*Figure 1-4 The client/server model of applications*

Most servers wait for requests at a *well-known port* so that their clients know to which port (and in turn, which application) they must direct their requests. The client typically uses an arbitrary port called an *ephemeral port* for its communication. Clients that want to communicate with a server that does not use a well-known port must have another mechanism for learning to which port they must address their requests. This mechanism might employ a registration service such as portmap, which does use a well-known port. For detailed information about TCP/IP application protocols, refer to Part 2,

“TCP/IP application protocols” on page 405.

##### Bridges, routers, and gateways

There are many ways to provide access to other networks. In an internetwork, this done with *routers*. In this section, we distinguish between a router, a bridge, and a gateway for allowing remote network access:

|  |  |
| --- | --- |
| **Bridge** | Interconnects LAN segments at the network interface layer level and forwards frames between them. A bridge performs the function of a MAC relay, and is independent of any higher layer protocol (including the logical link protocol). It provides MAC layer protocol conversion, if required.  A bridge is said to be *transparent* to IP. That is, when an IP host sends an IP datagram to another host on a network connected by a bridge, it sends the datagram directly to the host and the datagram “crosses” the bridge without the sending IP host being aware of it. |
| **Router** | Interconnects networks at the internetwork layer level and  routes packets between them. The router must understand the addressing structure associated with the networking protocols it supports and take decisions on whether, or how, to forward packets. Routers are able to select the best transmission paths and optimal packet sizes. The basic routing function is implemented in the IP layer of the TCP/IP protocol stack, so any host or workstation running TCP/IP over more than one interface could, in theory and also with most of today's TCP/IP implementations, forward IP datagrams. However, dedicated routers provide much more sophisticated routing than the minimum functions implemented by IP. |

Because IP provides this basic routing function, the term

“IP router,” is often used. Other, older terms for router are “IP gateway,” “Internet gateway,” and “gateway.” The term *gateway* is now normally used for connections at a higher layer than the internetwork layer.

A router is said to be *visible* to IP. That is, when a host sends an IP datagram to another host on a network connected by a router, it sends the datagram to the router so that it can forward it to the target host.

**Gateway** Interconnects networks at higher layers than bridges and routers. A gateway usually supports address mapping from one network to another, and might also provide transformation of the data between the environments to support end-to-end application connectivity. Gateways typically limit the interconnectivity of two networks to a subset of the application protocols supported on either one. For example, a VM host running TCP/IP can be used as an SMTP/RSCS mail gateway.

**Note:** The term “gateway,” when used in this sense, is *not* synonymous with “IP gateway.”

A gateway is said to be *opaque* to IP. That is, a host cannot send an IP datagram through a gateway; it can only send it *to* a gateway. The higher-level protocol information carried by the datagrams is then passed on by the gateway using whatever networking architecture is used on the other side of the gateway.

Closely related to routers and gateways is the concept of a *firewall*, or *firewall gateway*, which is used to restrict access from the Internet or some untrusted network to a network or group of networks controlled by an organization for security reasons. See 22.3, “Firewalls” on page 794 for more information about firewalls.

### 1.2 The roots of the Internet

Networks have become a fundamental, if not the most important, part of today's information systems. They form the backbone for information sharing in enterprises, governmental groups, and scientific groups. That information can take several forms. It can be notes and documents, data to be processed by another computer, files sent to colleagues, and multimedia data streams.

A number of networks were installed in the late 1960s and 1970s, when network design was the “state of the art” topic of computer research and sophisticated implementers. It resulted in multiple networking models such as packet-switching

technology, collision-detection local area networks, hierarchical networks, and many other excellent communications technologies.

The result of all this great know-how was that any group of users could find a physical network and an architectural model suitable for their specific needs. This ranges from inexpensive asynchronous lines with no other error recovery than a bit-per-bit parity function, through full-function wide area networks (public or private) with reliable protocols such as public packet-switching networks or private SNA networks, to high-speed but limited-distance local area networks.

The down side of the development of such heterogeneous protocol suites is the rather painful situation where one group of users wants to extend its information system to another group of users who have implemented a different network technology and different networking protocols. As a result, even if they could agree on some network technology to physically interconnect the two environments, their applications (such as mailing systems) would still not be able to communicate with each other because of different application protocols and interfaces.

This situation was recognized in the early 1970s by a group of U.S. researchers funded by the *Defense Advanced Research Projects Agency* (DARPA). Their work addressed *internetworking,* or the interconnection of networks. Other official organizations became involved in this area, such as ITU-T (formerly CCITT) and ISO. The main goal was to define a set of protocols, detailed in a well-defined suite, so that applications would be able to communicate with other applications, regardless of the underlying network technology or the operating systems where those applications run.

The official organization of these researchers was the ARPANET Network Working Group, which had its last general meeting in October 1971. DARPA continued its research for an internetworking protocol suite, from the early *Network Control Program* (NCP) host-to-host protocol to the TCP/IP protocol suite, which took its current form around 1978. At that time, DARPA was well known for its pioneering of packet-switching over radio networks and satellite channels. The first real implementations of the *Internet* were found around 1980 when DARPA started converting the machines of its research network (ARPANET) to use the new TCP/IP protocols. In 1983, the transition was completed and DARPA demanded that *all* computers willing to connect to its ARPANET use TCP/IP.

DARPA also contracted Bolt, Beranek, and Newman (BBN) to develop an implementation of the TCP/IP protocols for Berkeley UNIX® on the VAX and funded the University of California at Berkeley to distribute the code free of charge with their UNIX operating system. The first release of the *Berkeley Software Distribution* (BSD) to include the TCP/IP protocol set was made available in 1983 (4.2BSD). From that point on, TCP/IP spread rapidly among universities and research centers and has become the standard communications subsystem for all UNIX connectivity. The second release (4.3BSD) was distributed in 1986, with updates in 1988 (4.3BSD Tahoe) and 1990 (4.3BSD Reno). 4.4BSD was released in 1993. Due to funding constraints, 4.4BSD was the last release of the BSD by the Computer Systems Research Group of the University of California at Berkeley.

As TCP/IP internetworking spread rapidly, new wide area networks were created in the U.S. and connected to ARPANET. In turn, other networks in the rest of the world, not necessarily based on the TCP/IP protocols, were added to the set of interconnected networks. The result is what is described as *the Internet*. We describe some examples of the different networks that have played key roles in this development in the next sections.

#### 1.2.1 ARPANET

Sometimes referred to as the “grand-daddy of packet networks,” the ARPANET was built by DARPA (which was called ARPA at that time) in the late 1960s to accommodate research equipment on packet-switching technology and to allow resource sharing for the Department of Defense's contractors. The network interconnected research centers, some military bases, and government locations. It soon became popular with researchers for collaboration through electronic mail and other services. It was developed into a research utility run by the Defense Communications Agency (DCA) by the end of 1975 and split in 1983 into MILNET for interconnection of military sites and ARPANET for interconnection of research sites. This formed the beginning of the “capital I” Internet.

In 1974, the ARPANET was based on 56 Kbps leased lines that interconnected *packet-switching nodes* (PSN) scattered across the continental U.S. and western Europe. These were minicomputers running a protocol known as *1822* (after the number of a report describing it) and dedicated to the packet-switching task. Each PSN had at least two connections to other PSNs (to allow alternate routing in case of circuit failure) and up to 22 ports for user computer (*host*) connections. These 1822 systems offered reliable, flow-controlled delivery of a packet to a destination node. This is the reason why the original NCP protocol was a rather simple protocol. It was replaced by the TCP/IP protocols, which do not assume the reliability of the underlying network hardware and can be used on other-than-1822 networks. This 1822 protocol did not become an industry standard, so DARPA decided later to replace the 1822 packet switching technology with the *CCITT X.25* standard.

Data traffic rapidly exceeded the capacity of the 56 Kbps lines that made up the network, which were no longer able to support the necessary throughput. Today the ARPANET has been replaced by new technologies in its role of backbone on the research side of the connected Internet (see NSFNET later in this chapter), while MILNET continues to form the backbone of the military side.

#### 1.2.2 NSFNET

NSFNET, the National Science Foundation (NSF) Network, is a three-level internetwork in the United States consisting of:

The backbone: A network that connects separately administered and operated mid-level networks and NSF-funded supercomputer centers. The backbone also has transcontinental links to other networks such as EBONE, the European IP backbone network.

Mid-level networks: Three kinds of networks (regional, discipline-based, and supercomputer consortium networks).

Campus networks: Whether academic or commercial, connected to the mid-level networks.

Over the years, the NSF upgraded its backbone to meet the increasing demands of its clients:

First backbone: Originally established by the NSF as a communications network for researchers and scientists to access the NSF supercomputers, the first NSFNET backbone used six DEC LSI/11 microcomputers as packet switches, interconnected by 56 Kbps leased lines. A primary interconnection between the NSFNET backbone and the ARPANET existed at Carnegie Mellon, which allowed routing of datagrams between users connected to each of those networks.

Second backbone: The need for a new backbone appeared in 1987, when the first one became overloaded within a few months (estimated growth at that time was 100% per year). The NSF and MERIT, Inc., a computer network consortium of eight state-supported universities in Michigan, agreed to develop and manage a new, higher-speed backbone with greater transmission and switching capacities. To manage it, they defined the *Information Services* (IS), which is comprised of an Information Center and a Technical Support Group. The Information Center is responsible for information dissemination, information resource management, and electronic communication. The Technical Support Group provides support directly to the field. The purpose of this is to provide an integrated information system with easy-to-use-and-manage interfaces accessible from any point in the network supported by a full set of training services.

Merit and NSF conducted this project in partnership with IBM and MCI. IBM provided the software, packet-switching, and network-management equipment, while MCI provided the long-distance transport facilities. Installed in 1988, the new network initially used 448 Kbps leased circuits to interconnect 13 *nodal switching systems* (NSSs), supplied by IBM. Each NSS was composed of nine IBM RISC systems (running an IBM version of 4.3BSD

UNIX) loosely coupled by two IBM token-ring networks (for redundancy). One

Integrated Digital Network Exchange (IDNX) supplied by IBM was installed at each of the 13 locations, to provide:

* Dynamic alternate routing
* Dynamic bandwidth allocation

Third backbone: In 1989, the NSFNET backbone circuits topology was reconfigured after traffic measurements and the speed of the leased lines increased to T1 (1.544 Mbps) using primarily fiber optics.

Due to the constantly increasing need for improved packet switching and transmission capacities, three NSSs were added to the backbone and the link speed was upgraded. The migration of the NSFNET backbone from T1 to T3 (45 Mbps) was completed in late 1992. The subsequent migration to gigabit levels has already started and is continuing today.

In April 1995, the U.S. government discontinued its funding of NSFNET. This was, in part, a reaction to growing commercial use of the network. About the same time, NSFNET gradually migrated the main backbone traffic in the U.S. to commercial network service providers, and NSFNET reverted to being a network for the research community. The main backbone network is now run in cooperation with MCI and is known as the vBNS (very high speed Backbone Network Service).

NSFNET has played a key role in the development of the Internet. However, many other networks have also played their part and also make up a part of the Internet today.

#### 1.2.3 Commercial use of the Internet

In recent years the Internet has grown in size and range at a greater rate than anyone could have predicted. A number of key factors have influenced this growth. Some of the most significant milestones have been the free distribution of Gopher in 1991, the first posting, also in 1991, of the specification for hypertext and, in 1993, the release of Mosaic, the first graphics-based browser. Today the vast majority of the hosts now connected to the Internet are of a commercial nature. This is an area of potential and actual conflict with the initial aims of the Internet, which were to foster open communications between academic and research institutions. However, the continued growth in commercial use of the Internet is inevitable, so it will be helpful to explain how this evolution is taking place.

One important initiative to consider is that of the *Acceptable Use Policy* (AUP). The first of these policies was introduced in 1992 and applies to the use of NSFNET. At the heart of this AUP is a commitment “to support open research and education.” Under “Unacceptable Uses” is a prohibition of “use for for-profit activities,” unless covered by the General Principle or as a specifically acceptable use. However, in spite of this apparently restrictive stance, the NSFNET was increasingly used for a broad range of activities, including many of a commercial nature, before reverting to its original objectives in 1995.

The provision of an AUP is now commonplace among Internet service providers, although the AUP has generally evolved to be more suitable for commercial use. Some networks still provide services free of any AUP.

Let us now focus on the Internet service providers who have been most active in introducing commercial uses to the Internet. Two worth mentioning are PSINet and UUNET, which began in the late 1980s to offer Internet access to both businesses and individuals. The California-based CERFnet provided services free of any AUP. An organization to interconnect PSINet, UUNET, and CERFnet was formed soon after, called the Commercial Internet Exchange (CIX), based on the understanding that the traffic of any member of one network may flow without restriction over the networks of the other members. As of July 1997, CIX had grown to more than 146 members from all over the world, connecting member internets. At about the same time that CIX was formed, a non-profit company, Advance Network and Services (ANS), was formed by IBM, MCI, and Merit, Inc. to operate T1 (subsequently T3) backbone connections for NSFNET. This group was active in increasing the commercial presence on the Internet.

ANS formed a commercially oriented subsidiary called ANS CO+RE to provide linkage between commercial customers and the research and education domains. ANS CO+RE provides access to NSFNET as well as being linked to CIX. In 1995 ANS was acquired by America Online.

In 1995, as the NSFNET was reverting to its previous academic role, the architecture of the Internet changed from having a single dominant backbone in the U.S. to having a number of commercially operated backbones. In order for the different backbones to be able to exchange data, the NSF set up four Network Access Points (NAPs) to serve as data interchange points between the backbone service providers.

Another type of interchange is the Metropolitan Area Ethernet (MAE). Several MAEs have been set up by Metropolitan Fiber Systems (MFS), who also have their own backbone network. NAPs and MAEs are also referred to as public exchange points (IXPs). Internet service providers (ISPs) typically will have connections to a number of IXPs for performance and backup. For a current listing of IXPs, consult the Exchange Point at:

[http://www.ep.net](http://www.ep.net/)

Similar to CIX in the United States, European Internet providers formed the RIPE

(Réseaux IP Européens) organization to ensure technical and administrative coordination. RIPE was formed in 1989 to provide a uniform IP service to users throughout Europe. Today, the largest Internet backbones run at OC48 (2.4 Gbps) or OC192 (9.6 Gbps).

#### 1.2.4 Internet2

The success of the Internet and the subsequent frequent congestion of the NSFNET and its commercial replacement led to some frustration among the research community who had previously enjoyed exclusive use of the Internet. The university community, therefore, together with government and industry partners, and encouraged by the funding component of the Next Generation Internet (NGI) initiative, have formed the *Internet2* project.

The NGI initiative is a federal research program that is developing advanced networking technologies, introducing revolutionary applications that require advanced networking technologies and demonstrating these technological capabilities on high-speed testbeds.

##### Mission

The Internet2 mission is to facilitate and coordinate the development, operation, and technology transfer of advanced, network-based applications and network services to further U.S. leadership in research and higher education and accelerate the availability of new services and applications on the Internet.

Internet2 has the following goals:

Demonstrate new applications that can dramatically enhance researchers’ ability to collaborate and conduct experiments.

Demonstrate enhanced delivery of education and other services (for instance, health care, environmental monitoring, and so on) by taking advantage of *virtual proximity* created by an advanced communications infrastructure.

Support development and adoption of advanced applications by providing middleware and development tools.

Facilitate development, deployment, and operation of an affordable communications infrastructure, capable of supporting differentiated quality of service (QoS) based on application requirements of the research and education community.

Promote experimentation with the next generation of communications technologies.

Coordinate adoption of agreed working standards and common practices among participating institutions to ensure end-to-end quality of service and interoperability.

Catalyze partnerships with governmental and private sector organizations.

Encourage transfer of technology from Internet2 to the rest of the Internet.

Study the impact of new infrastructure, services, and applications on higher education and the Internet community in general.

##### Internet2 participants

Internet2 has 180 participating universities across the United States. Affiliate organizations provide the project with valuable input. All participants in the Internet2 project are members of the University Corporation for Advanced Internet Development (UCAID).

In most respects, the partnership and funding arrangements for Internet2 will parallel those of previous joint networking efforts of academia and government, of which the NSFnet project is a very successful example. The United States government will participate in Internet2 through the NGI initiative and related programs.

Internet2 also joins with corporate leaders to create the advanced network services necessary to meet the requirements of broadband, networked applications. Industry partners work primarily with campus-based and regional university teams to provide the services and products needed to implement the applications developed by the project. Major corporations currently participating in Internet2 include Alcatel, Cisco Systems, IBM, Nortel Networks, Sprint, and Sun Microsystems™. Additional support for Internet2 comes from collaboration with non-profit organizations working in research and educational networking. Affiliate organizations committed to the project include MCNC, Merit, National Institutes of Health (NIH), and the State University System of Florida.

For more information about Internet2, see their Web page at: [http://www.internet2.edu](http://www.internet2.edu/)

#### 1.2.5 The Open Systems Interconnection (OSI) Reference Model

The OSI (Open Systems Interconnect) Reference Model (ISO 7498) defines a seven-layer model of data communication with physical transport at the lower layer and application protocols at the upper layers. This model, shown in Figure 1-5, is widely accepted as a basis for the understanding of how a network protocol stack should operate and as a reference tool for comparing network stack implementation.

Application

Presentation

Session

Transport

Network

Data Link

Physical

Application

Presentation

Session

Transport

Network

Data Link

Physical

*Figure 1-5 The OSI Reference Model*

Each layer provides a set of functions to the layer above and, in turn, relies on the functions provided by the layer below. Although messages can only pass vertically through the stack from layer to layer, from a logical point of view, each layer communicates directly with its peer layer on other nodes.

The seven layers are:

|  |  |
| --- | --- |
| **Application** | Network applications such as terminal emulation and file transfer |
| **Presentation** | Formatting of data and encryption |
| **Session** | Establishment and maintenance of sessions |
| **Transport** | Provision of reliable and unreliable end-to-end delivery |
| **Network** | Packet delivery, including routing |
| **Data Link**  **Physical** | Framing of units of information and error checking  Transmission of bits on the physical hardware |

In contrast to TCP/IP, the OSI approach started from a clean slate and defined standards, adhering tightly to their own model, using a formal committee process without requiring implementations. Internet protocols use a less formal engineering approach, where anybody can propose and comment on Request for Comments, known as RFC, and implementations are required to verify feasibility. The OSI protocols developed slowly, and because running the full protocol stack is resource intensive, they have not been widely deployed, especially in the desktop and small computer market. In the meantime, TCP/IP and the Internet were developing rapidly, with deployment occurring at a very high rate.

### 1.3 TCP/IP standards

TCP/IP has been popular with developers and users alike because of its inherent openness and perpetual renewal. The same holds true for the Internet as an open communications network. However, this openness could easily turn into something that can help you and hurt you if it were not controlled in some way. Although there is no overall governing body to issue directives and regulations for the Internet—control is mostly based on mutual cooperation—the Internet Society (ISOC) serves as the standardizing body for the Internet community. It is organized and managed by the Internet Architecture Board (IAB).

The IAB itself relies on the Internet Engineering Task Force (IETF) for issuing new standards, and on the Internet Assigned Numbers Authority (IANA) for coordinating values shared among multiple protocols. The RFC Editor is responsible for reviewing and publishing new standards documents.

The IETF itself is governed by the Internet Engineering Steering Group (IESG) and is further organized in the form of Areas and Working Groups where new specifications are discussed and new standards are propsoed.

The Internet Standards Process, described in RFC 2026, The Internet Standards Process, Revision 3, is concerned with all protocols, procedures, and conventions that are used in or by the Internet, whether or not they are part of the TCP/IP protocol suite.

The overall goals of the Internet Standards Process are:

Technical excellence

Prior implementation and testing Clear, concise, and easily understood documentation

Openness and fairness

Timeliness

The process of standardization is summarized as follows:

In order to have a new specification approved as a standard, applicants have to submit that specification to the IESG where it will be discussed and reviewed for technical merit and feasibility and also published as an Internet draft document. This should take no shorter than two weeks and no longer than six months.

After the IESG reaches a positive conclusion, it issues a last-call notification to allow the specification to be reviewed by the whole Internet community.

After the final approval by the IESG, an Internet draft is recommended to the Internet Engineering Taskforce (IETF), another subsidiary of the IAB, for inclusion into the Standards Track and for publication as a Request for Comments (see 1.3.1, “Request for Comments (RFC)” on page 22).

Once published as an RFC, a contribution may advance in status as described in 1.3.2, “Internet standards” on page 24. It may also be revised over time or phased out when better solutions are found.

If the IESG does not approve of a new specification after, or if a document has remained unchanged within, six months of submission, it will be removed from the Internet drafts directory.

#### 1.3.1 Request for Comments (RFC)

The Internet protocol suite is still evolving through the mechanism of *Request for Comments* (RFC). New protocols (mostly application protocols) are being designed and implemented by researchers, and are brought to the attention of the Internet community in the form of an Internet draft (ID).[[1]](#footnote-1) The largest source of IDs is the Internet Engineering Task Force (IETF), which is a subsidiary of the IAB. However, anyone can submit a memo proposed as an ID to the RFC Editor. There are a set of rules which RFC/ID authors must follow in order for an RFC to be accepted. These rules are themselves described in an RFC (RFC 2223), which also indicates how to submit a proposal for an RFC.

After an RFC has been published, all revisions and replacements are published as new RFCs. A new RFC that revises or replaces an existing RFC is said to

“update” or to “obsolete” that RFC. The existing RFC is said to be “updated by” or

“obsoleted by” the new one. For example RFC 1542, which describes the BOOTP protocol, is a “second edition,” being a revision of RFC 1532 and an amendment to RFC 951. RFC 1542 is therefore labelled like this: “Obsoletes RFC 1532; Updates RFC 951." Consequently, there is never any confusion over whether two people are referring to different versions of an RFC, because there is never more than one current version.

Some RFCs are described as *information documents*, while others describe

Internet protocols. The Internet Architecture Board (IAB) maintains a list of the RFCs that describe the protocol suite. Each of these is assigned a *state* and a *status*.

An Internet protocol can have one of the following states:

|  |  |
| --- | --- |
| **Standard** | The IAB has established this as an official protocol for the Internet. These are separated into two groups:  IP protocol and above, protocols that apply to the whole Internet  Network-specific protocols, generally specifications of how to do IP on particular types of networks |
| **Draft standard** | The IAB is actively considering this protocol as a possible standard protocol. Substantial and widespread testing and comments are desired. Submit comments and test results to the IAB. There is a possibility that changes will be made in a draft protocol before it becomes a standard. |
| **Proposed standard** | These are protocol proposals that might be considered by the IAB for standardization in the future. Implementations and testing by several groups are desirable. Revision of the protocol is likely. |
| **Experimental** | A system should not implement an experimental protocol unless it is participating in the experiment and has coordinated its use of the protocol with the developer of the protocol. |
| **Informational** | Protocols developed by other standard organizations, or vendors, or that are for other reasons outside the purview of the IAB may be published as RFCs for the convenience of the Internet community as informational protocols. Such protocols might, in some cases, also be recommended for use on the Internet by the IAB. |
| **Historic** | These are protocols that are unlikely to ever become standards in the Internet either because they have been  superseded by later developments or due to lack of interest. |

Protocol status can be any of the following:

|  |  |
| --- | --- |
| **Required** | A system must implement the required protocols. |
| **Recommended** | A system should implement the recommended protocol. |
| **Elective** | A system may or may not implement an elective protocol. The general notion is that if you are going to do something like this, you must do exactly this. |
| **Limited use** | These protocols are for use in limited circumstances. This may be because of their experimental state, specialized nature, limited functionality, or historic state. |
| **Not recommended** | These protocols are not recommended for general use. This may be because of their limited functionality, specialized nature, or experimental or historic state. |

#### 1.3.2 Internet standards

Proposed standard, draft standard, and standard protocols are described as being on the *Internet Standards Track*. When a protocol reaches the standard state, it is assigned a standard (STD) number. The purpose of STD numbers is to clearly indicate which RFCs describe Internet standards. STD numbers reference multiple RFCs when the specification of a standard is spread across multiple documents. Unlike RFCs, where the number refers to a specific document, STD numbers do not change when a standard is updated. STD numbers do not, however, have version numbers because all updates are made through RFCs and the RFC numbers are unique. Therefore, to clearly specify which version of a standard one is referring to, the standard number and all of the RFCs that it includes should be stated. For instance, the Domain Name System (DNS) is STD 13 and is described in RFCs 1034 and 1035. To reference the standard, a form such as “STD-13/RFC1034/RFC1035” should be used.

For some Standards Track RFCs, the status category does not always contain enough information to be useful. It is therefore supplemented, notably for routing protocols, by an *applicability statement*, which is given either in STD 1 or in a separate RFC.

References to the RFCs and to STD numbers will be made throughout this book, because they form the basis of all TCP/IP protocol implementations.

The following Internet standards are of particular importance:

STD 1 – Internet Official Protocol Standards

This standard gives the state and status of each Internet protocol or standard and defines the meanings attributed to each state or status. It is issued by the IAB approximately quarterly. At the time of writing, this standard is in RFC 3700.

STD 2 – Assigned Internet Numbers

This standard lists currently assigned numbers and other protocol parameters in the Internet protocol suite. It is issued by the Internet Assigned Numbers Authority (IANA). The current edition at the time of writing is RFC 3232.

STD 3 – Host Requirements

This standard defines the requirements for Internet host software (often by reference to the relevant RFCs). The standard comes in three parts:

* RFC 1122 – Requirements for Internet hosts – communications layer
* RFC 1123 – Requirements for Internet hosts – application and support
* RFC 2181 – Clarifications to the DNS Specification

STD 4 – Router Requirements

This standard defines the requirements for IPv4 Internet gateway (router) software. It is defined in RFC 1812 – Requirements for IPv4 Routers.

##### For Your Information (FYI)

A number of RFCs that are intended to be of wide interest to Internet users are classified as *For Your Information* (FYI) documents. They frequently contain introductory or other helpful information. Like STD numbers, an FYI number is not changed when a revised RFC is issued. Unlike STDs, FYIs correspond to a single RFC document. For example, FYI 4 - FYI on Questions and Answers - Answers to Commonly asked “New Internet User” Questions, is currently in its fifth edition. The RFC numbers are 1177, 1206, 1325 and 1594, and 2664.

##### Obtaining RFCs

RFC and ID documents are available publicly and online and best obtained from the IETF Web site: [http://www.ietf.org](http://www.ietf.org/)

A complete list of current Internet Standards can be found in RFC 3700 – Internet Official Protocol Standards.

### 1.4 Future of the Internet

Trying to predict the future of the Internet is not an easy task. Few would have imagined, even five years ago, the extent to which the Internet has now become a part of everyday life in business, homes, and schools. There are a number of things, however, about which we can be fairly certain.

#### 1.4.1 Multimedia applications

Bandwidth requirements will continue to increase at massive rates; not only is the number of Internet users growing rapidly, but the applications being used are becoming more advanced and therefore consume more bandwidth. New technologies such as dense wave division multiplexing (DWDM) are emerging to meet these high bandwidth demands being placed on the Internet.

Much of this increasing demand is attributable to the increased use of multimedia applications. One example is that of Voice over IP technology. As this technology matures, we are almost certain to see a sharing of bandwidth between voice and data across the Internet. This raises some interesting questions for phone companies. The cost to a user of an Internet connection between Raleigh, NC and Santiago, Chile is the same as a connection within Raleigh, not so for a traditional phone connection. Inevitably, voice conversations will become video conversations as phone calls become video conferences.

Today, it is possible to hear radio stations from almost any part of the globe through the Internet with FM quality. We can watch television channels from all around the world, leading to the clear potential of using the Internet as the vehicle for delivering movies and all sorts of video signals to consumers everywhere. It all comes at a price, however, as the infrastructure of the Internet must adapt to such high bandwidth demands.

#### 1.4.2 Commercial use

The Internet has been through an explosion in terms of commercial use. Today, almost all large business depend on the Internet, whether for marketing, sales, customer service, or employee access. These trends are expected to continue. Electronic stores will continue to flourish by providing convenience to customers that do not have time to make their way to traditional stores.

Businesses will rely more and more on the Internet as a means for communicating branches across the globe. With the popularity of virtual private networks (VPNs), businesses can securely conduct their internal business over a wide area using the Internet; employees can work from home offices yielding a *virtual office* environment. Virtual meetings probably will be common occurrences.

#### 1.4.3 The wireless Internet

Perhaps the most widespread growth in the use of the Internet, however, is that of wireless applications. Recently, there has been an incredible focus on the enablement of wireless and pervasive computing. This focus has been largely motivated by the convenience of wireless connectivity. For example, it is impractical to physically connect a mobile workstation, which by definition, is free to roam. Constraining such a workstation to some physical geography simply defeats the purpose. In other cases, wired connectivity simply is not feasible. Examples include the ruins of Macchu Picchu or offices in the Sistine Chapel. In these circumstances, fixed workstations also benefit from otherwise unavailable network access.

Protocols such as Bluetooth, IEEE 802.11, and Wireless Application Protocol (WAP) are paving the way toward a wireless Internet. While the personal benefits of such access are quite advantageous, even more appealing are the business applications that are facilitated by such technology. Every business, from factories to hospitals, could enhance their respective services. Wireless devices will become standard equipment in vehicles, not only for the personal enjoyment of the driver, but also for the flow of maintenance information to your favorite automobile mechanic. The applications are limitless.

### 1.5 RFCs relevant to this chapter

The following RFCs provide detailed information about the connection protocols and architectures presented throughout this chapter:

[RFC 2026 – The Internet Standards Process -- Revision 3 (October 1996)](ftp://ftp.rfc-editor.org/in-notes/rfc2026.txt)

[RFC 2223 – Instructions to RFC (October 1997)](ftp://ftp.rfc-editor.org/in-notes/rfc2223.txt)

[RFC 2900 – Internet Official Protocol Standards (August 2001)](ftp://ftp.rfc-editor.org/in-notes/rfc2900.txt)

[RFC 3232 – Assigned Numbers: RFC 1700 is Replaced by an On-line](ftp://ftp.rfc-editor.org/in-notes/rfc3232.txt)

[Database (January 2002)](ftp://ftp.rfc-editor.org/in-notes/rfc3232.txt)

|  |  |  |
| --- | --- | --- |
|  | |  | | --- | | **3** | |

## Chapter 3. Internetworking protocols

This chapter provides an overview of the most important and common protocols associated with the TCP/IP internetwork layer. These include:

Internet Protocol (IP)

Internet Control Message Protocol (ICMP)

Address Resolution Protocol (ARP)

Dynamic Host Configuration Protocol (DHCP)

These protocols perform datagram addressing, routing and delivery, dynamic address configuration, and resolve between the internetwork layer addresses and the network interface layer addresses.

© Copyright IBM Corp. 1989-2006. All rights reserved.

### 3.1 Internet Protocol (IP)

IP is a standard protocol with STD number 5. The standard also includes ICMP

(see 3.2, “Internet Control Message Protocol (ICMP)” on page 109) and IGMP (see 3.3, “Internet Group Management Protocol (IGMP)” on page 119). IP has a status of required.

The current IP specification is in RFC 950, RFC 919, RFC 922, RFC 3260 and RFC 3168, which updates RFC 2474, and RFC 1349, which updates RFC 791. Refer to 3.8, “RFCs relevant to this chapter” on page 140 for further details regarding the RFCs.

IP is the protocol that hides the underlying physical network by creating a *virtual network* view. It is an unreliable, best-effort, and connectionless packet delivery protocol. Note that best-effort means that the packets sent by IP might be lost, arrive out of order, or even be duplicated. IP assumes higher layer protocols will address these anomalies.

One of the reasons for using a connectionless network protocol was to minimize the dependency on specific computing centers that used hierarchical connection-oriented networks. The United States Department of Defense intended to deploy a network that would still be operational if parts of the country were destroyed. This has been proven to be true for the Internet.

#### 3.1.1 IP addressing

IP addresses are represented by a 32-bit unsigned binary value. It is usually expressed in a dotted decimal format. For example, 9.167.5.8 is a valid IP address. The numeric form is used by IP software. The mapping between the IP address and an easier-to-read symbolic name, for example, myhost.ibm.com, is done by the *Domain Name System (DNS)*, discussed in 12.1, “Domain Name System (DNS)” on page 426.

##### The IP address

IP addressing standards are described in RFC 1166. To identify a host on the

Internet, each host is assigned an address, the *IP address*, or in some cases, the *Internet address*. When the host is attached to more than one network, it is called *multihomed* and has one IP address for each network interface. The IP address consists of a pair of numbers:

IP address = <network number><host number>

The *network number* portion of the IP address is administered by one of three Regional Internet Registries (RIR):

American Registry for Internet Numbers (ARIN): This registry is responsible for the administration and registration of Internet Protocol (IP) numbers for North America, South America, the Caribbean, and sub-Saharan Africa.

Reseaux IP Europeans (RIPE): This registry is responsible for the administration and registration of Internet Protocol (IP) numbers for Europe, Middle East, and parts of Africa.

Asia Pacific Network Information Centre (APNIC): This registry is responsible for the administration and registration of Internet Protocol (IP) numbers within the Asia Pacific region.

IP addresses are 32-bit numbers represented in a *dotted decimal* form (as the decimal representation of four 8-bit values concatenated with dots). For example, 128.2.7.9 is an IP address with 128.2 being the network number and 7.9 being the host number. Next, we explain the rules used to divide an IP address into its network and host parts.

The binary format of the IP address 128.2.7.9 is:

10000000 00000010 00000111 00001001

IP addresses are used by the IP protocol to uniquely identify a host on the Internet (or more generally, any internet). Strictly speaking, an IP address identifies an interface that is capable of sending and receiving IP datagrams. One system can have multiple such interfaces. However, both hosts and routers must have at least one IP address, so this simplified definition is acceptable. IP datagrams (the basic data packets exchanged between hosts) are transmitted by a physical network attached to the host. Each IP datagram contains a *source IP address* and a *destination IP address*. To send a datagram to a certain IP destination, the target IP address must be translated or mapped to a physical address. This might require transmissions in the network to obtain the destination's physical network address. (For example, on LANs, the Address Resolution Protocol, discussed in 3.4, “Address Resolution Protocol (ARP)” on page 119, is used to translate IP addresses to physical MAC addresses.)

##### Class-based IP addresses

The first bits of the IP address specify how the rest of the address should be separated into its network and host part. The terms *network address* and *netID* are sometimes used instead of network number, but the formal term, used in RFC 1166, is network number. Similarly, the terms *host address* and *hostID* are sometimes used instead of host number.

There are five classes of IP addresses. They are shown in Figure 3-1.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Class A  Class B  Class C  Class D  Class E | 1 2 3  01 8 6 4 1 | | | | | | | | | | |
|  | |  | | | | |  | | |  |
| 0 |  | netID | | | | | hostID | | |  |
|  |  | | | | | | | | |
|  | | | | | | | | | |
|  | | |  | | | | |  | |  |
|  | 10 | | netID | | | | | hostID | |  |
|  |  | | | | | | | | |
|  | | | | | | | | | |
|  | | | |  | | | | |  |  |
|  | 110 | | | netID | | | | | hostID |  |
|  |  | | | | | | | | |
|  | | | | | | | | | |
|  | | | | |  | | | | |  |
|  | 1110 | | | | multicast | | | | |  |
|  |  | | | | | | | | |
|  | | | | | | | | | |
|  | | | | | |  | | | |  |
|  | 11110 | | | | | future/experimental use | | | |  |
|  |  | | | | | | | | |

*Figure 3-1 IP: Assigned classes of IP addresses*

Where:

|  |  |
| --- | --- |
| **Class A addresses** | These addresses use 7 bits for the <network> and 24 bits for the <host> portion of the IP address. This allows for 27-2 (126) networks each with 224-2 (16777214) hosts—a total of more than 2 billion addresses. |
| **Class B addresses** | These addresses use 14 bits for the <network> and 16 bits for the <host> portion of the IP address. This allows for 214-2 (16382) networks each with 216-2 (65534) hosts—a total of more than 1 billion addresses. |
| **Class C addresses** | These addresses use 21 bits for the <network> and 8 bits for the <host> portion of the IP address. That allows for 221-2 (2097150) networks each with 28-2 (254) hosts—a total of more than half a billion addresses. |
| **Class D addresses** | These addresses are reserved for multicasting (a sort of |
| **Class E addresses** | broadcasting, but in a limited area, and only to hosts using the same Class D address).  These addresses are reserved for future or experimental use. |

A Class A address is suitable for networks with an extremely large number of hosts. Class C addresses are suitable for networks with a small number of hosts. This means that medium-sized networks (those with more than 254 hosts or where there is an expectation of more than 254 hosts) must use Class B addresses. However, the number of small- to medium-sized networks has been growing very rapidly. It was feared that if this growth had been allowed to continue unabated, all of the available Class B network addresses would have been used by the mid-1990s. This was termed the IP address exhaustion problem (refer to 3.1.5, “The IP address exhaustion problem” on page 86).

The division of an IP address into two parts also separates the responsibility for selecting the complete IP address. The network number portion of the address is assigned by the RIRs. The host number portion is assigned by the authority controlling the network. As shown in the next section, the host number can be further subdivided: This division is controlled by the authority that manages the network. It is not controlled by the RIRs.

##### Reserved IP addresses

A component of an IP address with a value *all bits 0* or *all bits 1* has a special meaning:

All bits 0: An address with all bits zero in the host number portion is interpreted as *this* host (IP address with <host address>=0). All bits zero in the network number portion is *this* network (IP address with <network address>=0). When a host wants to communicate over a network, but does not yet know the network IP address, it can send packets with <network address>=0. Other hosts in the network interpret the address as meaning *this* network. Their replies contain the fully qualified network address, which the sender records for future use.

All bits 1: An address with all bits one is interpreted as *all* networks or *all* hosts. For example, the following means all hosts on network 128.2 (Class B address):

128.2.255.255

This is called a directed broadcast address because it contains both a valid <network address> and a broadcast <host address>.

Loopback: The Class A network 127.0.0.0 is defined as the loopback network. Addresses from that network are assigned to interfaces that process data within the local system. These loopback interfaces do not access a physical network.

##### Special use IP addresses

RFC 3330 discusses special use IP addresses. We provide a brief description of these IP addresses in Table 3-1.

*Table 3-1 Special use IP addresses*

|  |  |
| --- | --- |
| **Address block** | **Present use** |
| 0.0.0.0/8 | “This” network |
| 14.0.0.0/8 | Public-data networks |
| 24.0.0.0/8 | Cable television networks |
| 39.0.0.0/8 | Reserved but subject to allocation |
| 128.0.0.0/16 | Reserved but subject to allocation |
| 169.254.0.0/16 | Link local |
| 191.255.0.0/16 | Reserved but subject to allocation |
| 192.0.0.0/24 | Reserved but subject to allocation |
| 192.0.2.0/24 | Test-Net 192.88.99.0/24 6to4 relay anycast |
| 198.18.0.0/15 | Network interconnect device benchmark testing |
| 223.255.255.0/24 | Reserved but subject to allocation |
| 224.0.0.0/4 | Multicast |
| 240.0.0.0/4 | Reserved for future use |

#### 3.1.2 IP subnets

Due to the explosive growth of the Internet, the principle of assigned IP addresses became too inflexible to allow easy changes to local network configurations. Those changes might occur when:

A new type of physical network is installed at a location.

Growth of the number of hosts requires splitting the local network into two or more separate networks.

Growing distances require splitting a network into smaller networks, with gateways between them.

To avoid having to request additional IP network addresses, the concept of IP subnetting was introduced. The assignment of subnets is done locally. The entire network still appears as one IP network to the outside world.

The host number part of the IP address is subdivided into a second network number and a host number. This second network is termed a *subnetwork* or *subnet*. The main network now consists of a number of subnets. The IP address is interpreted as:

<network number><subnet number><host number>

The combination of subnet number and host number is often termed the *local address* or the *local portion* of the IP address. *Subnetting* is implemented in a way that is transparent to remote networks. A host within a network that has subnets is aware of the subnetting structure. A host in a different network is not. This remote host still regards the local part of the IP address as a host number.

The division of the local part of the IP address into a subnet number and host number is chosen by the local administrator. Any bits in the local portion can be used to form the subnet. The division is done using a 32-bit *subnet mask*. Bits with a value of zero bits in the subnet mask indicate positions ascribed to the host number. Bits with a value of one indicate positions ascribed to the subnet number. The bit positions in the subnet mask belonging to the original network number are set to ones but are not used (in some platform configurations, this value was specified with zeros instead of ones, but either way it is not used). Like IP addresses, subnet masks are usually written in dotted decimal form.

The special treatment of all bits zero and all bits one applies to each of the three parts of a subnetted IP address just as it does to both parts of an IP address that has not been subnetted (see “Reserved IP addresses” on page 71). For example, subnetting a Class B network can use one of the following schemes:

The first octet is the subnet number; the second octet is the host number. This gives 28-2 (254) possible subnets, each having up to 28-2 (254) hosts. Recall that we subtract two from the possibilities to account for the all ones and all zeros cases. The subnet mask is 255.255.255.0.

The first 12 bits are used for the subnet number and the last four for the host number. This gives 212-2 (4094) possible subnets but only 24-2 (14) hosts per subnet. The subnet mask is 255.255.255.240.

In this example, there are several other possibilities for assigning the subnet and host portions of the address. The number of subnets and hosts and any future requirements need to be considered before defining this structure. In the last example, the subnetted Class B network has 16 bits to be divided between the subnet number and the host number fields. The network administrator defines either a larger number of subnets each with a small number of hosts, or a smaller number of subnets each with many hosts.

When assigning the subnet part of the local address, the objective is to assign a *number* of bits to the subnet number and the remainder to the local address.

Therefore, it is normal to use a contiguous block of bits at the beginning of the local address part for the subnet number. This makes the addresses more readable. (This is particularly true when the subnet occupies 8 or 16 bits.) With this approach, either of the previous subnet masks are “acceptable” masks. Masks such as 255.255.252.252 and 255.255.255.15 are “unacceptable.” In fact, most TCP/IP implementations do not support non-contiguous subnet masks. Their use is universally discouraged.

##### Types of subnetting

There are two types of subnetting: static and variable length. Variable length subnetting is more flexible than static. Native IP routing and RIP Version 1 support only static subnetting. However, RIP Version 2 supports variable length subnetting (refer to Chapter 5, “Routing protocols” on page 171).

###### Static subnetting

Static subnetting implies that all subnets obtained from the same network use the same subnet mask. Although this is simple to implement and easy to maintain, it might waste address space in small networks. Consider a network of four hosts using a subnet mask of 255.255.255.0. This allocation wastes 250 IP addresses. All hosts and routers are required to support static subnetting.

###### Variable length subnetting

When variable length subnetting or variable length subnet masks (VLSM) are used, allocated subnets within the same network can use different subnet masks. A small subnet with only a few hosts can use a mask that accommodates this need. A subnet with many hosts requires a different subnet mask. The ability to assign subnet masks according to the needs of the individual subnets helps conserve network addresses. Variable length subnetting divides the network so that each subnet contains sufficient addresses to support the required number of hosts.

An existing subnet can be split into two parts by adding another bit to the subnet portion of the subnet mask. Other subnets in the network are unaffected by the change.

###### Mixing static and variable length subnetting

Not every IP device includes support for variable length subnetting. Initially, it appears that the presence of a host that only supports static subnetting prevents the use of variable length subnetting. This is not the case. Routers interconnecting the subnets are used to hide the different masks from hosts. Hosts continue to use basic IP routing. This offloads subnetting complexities to dedicated routers.

##### Static subnetting example

Consider the Class A network shown in Figure 3-2.

0

Class A

netID

hostID

1 2 3

01

8 6 4

1

*Figure 3-2 IP: Class A address without subnets* Use the IP address shown in Figure 3-3.

|  |
| --- |
| 00001001 01000011 00100110 00000001 a 32-bit address  9 67 38 1 decimal notation (9.67.38.1) |

*Figure 3-3 IP address*

The IP address is 9.67.38.1 (Class A) with 9 as the <network address> and 67.38.1 as the <host address>.

The network administrator might want to choose the bits from 8 to 25 to indicate the subnet address. In that case, the bits from 26 to 31 indicate the host addresses. Figure 3-4 shows the subnetted address derived from the original Class A address.

1 2 3

01

8 6 4

1

Class A

Subnet

subnet number

0

host

ID

netID

*Figure 3-4 IP: Class A address with subnet mask and subnet address*

A bit mask, known as the subnet mask, is used to identify which bits of the original host address field indicate the subnet number. In the previous example, the subnet mask is 255.255.255.192 (or 11111111 11111111 11111111

11000000 in bit notation). Note that, by convention, the <network address> is included in the mask as well.

Because of the all bits 0 and all bits 1 restrictions, this defines 218-2 (from 1 to 262143) valid subnets. This split provides 262142 subnets each with a maximum of 26-2 (62) hosts.

The value applied to the subnet number takes the value of the full octet with non-significant bits set to zero. For example, the hexadecimal value 01 in this subnet mask assumes an 8-bit value 01000000. This provides a subnet value of 64.

Applying the 255.255.255.192 to the sample Class A address of 9.67.38.1 provides the following information:

00001001 01000011 00100110 00000001 = 9.67.38.1 (Class A address)

11111111 11111111 11111111 11------ 255.255.255.192 (subnet mask)

===================================== logical\_AND 00001001 01000011 00100110 00------ = 9.67.38.0 (subnet base address)

This leaves a host address of:

-------- -------- -------- --000001 = 1 (host address)

IP will recognize all host addresses as being on the local network for which the logical\_AND operation described earlier produces the same result. This is important for routing IP datagrams in subnet environments (refer to 3.1.3, “IP routing” on page 77).

The subnet number is:

-------- 01000011 00100110 00------ = 68760 (subnet number)

This subnet number is a relative number. That is, it is the 68760th subnet of network 9 with the given subnet mask. This number bears no resemblance to the actual IP address that this host has been assigned (9.67.38.1). It has no meaning in terms of IP routing.

The division of the original <host address> into <subnet><host> is chosen by the network administrator. The values of all zeroes and all ones in the <subnet> field are reserved.

##### Variable length subnetting example

Consider a corporation that has been assigned the Class C network

165.214.32.0. The corporation has the requirement to split this address range into five separate networks each with the following number of hosts:

Subnet 1: 50 hosts

Subnet 2: 50 hosts

Subnet 3: 50 hosts

Subnet 4: 30 hosts

Subnet 5: 30 hosts

This cannot be achieved with static subnetting. For this example, static subnetting divides the network into four subnets each with 64 hosts or eight subnets each with 32 hosts. This subnet allocation does not meet the stated requirements.

To divide the network into five subnets, multiple masks need to be defined. Using a mask of 255.255.255.192, the network can be divided into four subnets each with 64 hosts. The fourth subnet can be further divided into two subnets each with 32 hosts by using a mask of 255.255.255.224. There will be three subnets each with 64 hosts and two subnets each with 32 hosts. This satisfies the stated requirements and eliminates the possibility of a high number of wasted host addresses.

##### Determining the subnet mask

Usually, hosts will store the subnet mask in a configuration file. However, sometimes this cannot be done, for example, as in the case of a diskless workstation. The ICMP protocol includes two messages: address mask request and address mask reply. These allow hosts to obtain the correct subnet mask from a server (refer to “Address Mask Request (17) and Address Mask Reply (18)” on page 116).

##### Addressing routers and multihomed hosts

Whenever a host has a physical connection to multiple networks or subnets, it is described as being *multihomed*. By default, all routers are multihomed because their purpose is to join networks or subnets. A multihomed host has different IP addresses associated with each network adapter. Each adapter connects to a different subnet or network.

#### 3.1.3 IP routing

An important function of the IP layer is *IP routing*. This provides the basic mechanism for routers to interconnect different physical networks. A device can simultaneously function as both a normal host and a router.

A router of this type is referred to as a router with partial routing information. The router only has information about four kinds of destinations:

Hosts that are directly attached to one of the physical networks to which the router is attached.

Hosts or networks for which the router has been given explicit definitions.

Hosts or networks for which the router has received an ICMP redirect message.

A default for all other destinations.

Additional protocols are needed to implement a full-function router. These types of routers are essential in most networks, because they can exchange information with other routers in the environment. We review the protocols used by these routers in Chapter 5, “Routing protocols” on page 171.

There are two types of IP routing: direct and indirect.

##### Direct routing

If the destination host is attached to the same physical network as the source host, IP datagrams can be directly exchanged. This is done by encapsulating the IP datagram in the physical network frame. This is called direct delivery and is referred to as direct routing.

##### Indirect routing

Indirect routing occurs when the destination host is not connected to a network directly attached to the source host. The only way to reach the destination is through one or more IP gateways. (Note that in TCP/IP terminology, the terms gateway and router are used interchangeably. This describes a system that performs the duties of a router.) The address of the first gateway (the first hop) is called an indirect route in the IP routing algorithm. The address of the first gateway is the only information needed by the source host to send a packet to the destination host.

In some cases, there may be multiple subnets defined on the same physical network. If the source and destination hosts connect to the same physical network but are defined in different subnets, indirect routing is used to communicate between the pair of devices. A router is needed to forward traffic between subnets.

Figure 3-5 shows an example of direct and indirect routes. Here, host C has a direct route to hosts B and D, and an indirect route to host A via gateway B.

Host D

Host C

Host B

Host A

*Figure 3-5 IP: Direct and indirect routes*

##### IP routing table

The determination of direct routes is derived from the list of local interfaces. It is automatically composed by the IP routing process at initialization. In addition, a list of networks and associated gateways (indirect routes) can be configured. This list is used to facilitate IP routing. Each host keeps the set of mappings between the following:

Destination IP network addresses

Routes to next gateways

This information is stored in a table called the IP routing table. Three types of mappings are in this table:

The direct routes describing locally attached networks

The indirect routes describing networks reachable through one or more gateways

The default route that contains the (direct or indirect) route used when the destination IP network is not found in the mappings of the previous types of type 1 and 2

Figure3-6 presents a sample network.

*Figure 3-6 IP: Routing table scenario*

Host D

Host C

Host E

Host F

Host B

Host A

128.15

129.7

128.10

The routing table of host D might contain the following (symbolic) entries (Table 3-2).

*Table 3-2 Host D sample entries*

|  |  |  |
| --- | --- | --- |
| **Destination** | **Router** | **Interface** |
| 129.7.0.0 | E | lan0 |
| 128.15.0.0 | D | lan0 |
| 128.10.0.0 | B | lan0 |
| default | B | lan0 |
| 127.0.0.1 | loopback | loo |

Because D is directly attached to network 128.15.0.0, it maintains a direct route for this network. To reach networks 129.7.0.0 and 128.10.0.0, however, it must have an indirect route through E and B, respectively, because these networks are not directly attached to it.

The routing table of host F might contain the following (symbolic) entries (Table 3-3).

*Table 3-3 Host F sample entries*

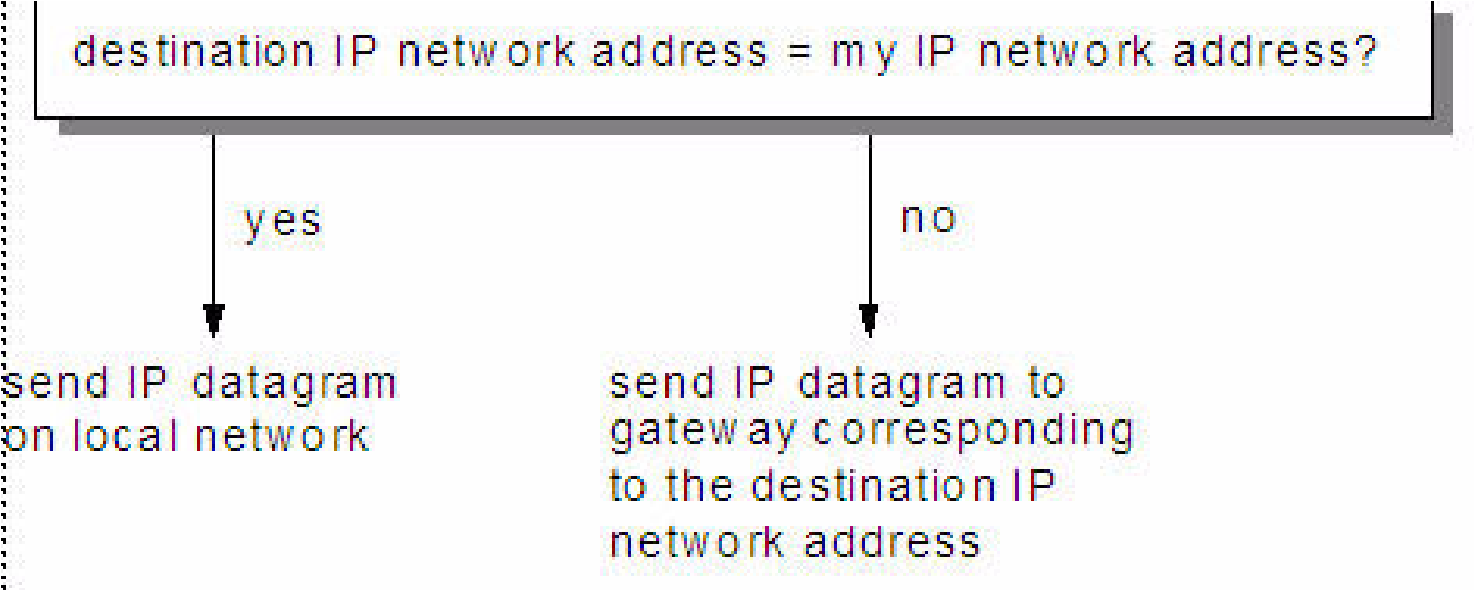
|  |  |  |
| --- | --- | --- |
| **Destination** | **Router** | **Interface** |
| 129.7.0.0 | F | wan0 |
| default | E | wan0 |
| 127.0.0.1 | loopback | lo |

Because every host not on the 129.7.0.0 network must be reached through host E, host F simply maintains a default route through E.

##### IP routing algorithm

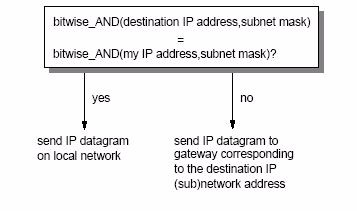
IP uses a unique algorithm to route datagrams, as illustrated in Figure 3-7.

*Figure 3-7 IP: Routing without subnets*



To differentiate between subnets, the IP routing algorithm is updated, as shown in Figure 3-8.

*Figure 3-8 IP: Routing with subnets*



Some implications of this change include:

This algorithm represents a change to the general IP algorithm. Therefore, to be able to operate this way, the particular gateway must contain the new algorithm. Some implementations might still use the general algorithm, and will not function within a subnetted network, although they can still communicate with hosts in other networks that are subnetted.

As IP routing is used in all of the hosts (and not just the routers), all of the hosts in the subnet must have:

* An IP routing algorithm that supports subnetting
* The same subnet mask (unless subnets are formed within the subnet)

If the IP implementation on any of the hosts does not support subnetting, that host will be able to communicate with any host in its own subnet but not with any machine on another subnet within the same network. This is because the host sees only one IP network and its routing cannot differentiate between an IP datagram directed to a host on the local subnet and a datagram that should be sent through a router to a different subnet.

In case one or more hosts do not support subnetting, an alternative way to achieve the same goal exists in the form of *proxy-ARP*. This does not require any changes to the IP routing algorithm for single-homed hosts. It does require changes on routers between subnets in the network (refer to 3.4.4, “Proxy-ARP or transparent subnetting” on page 123).

Figure 3-9 illustrates the entire IP routing algorithm.

Bitwise AND local interface(s)

with local\_subnet\_mask(s)

Yes

Yes

Yes

Take destination IP

address

No

No

No

Send ICMP error message

"network unreachable"

Bitwise AND dest\_IP\_addr

with local\_subnet\_mask(s)

Is there a match?

Is there an indirect route

entry?

Is a default route

specified?

Deliver indirectly to the

default router's IP address

Deliver directly using the

corresponding local

interface

Deliver indirectly to the

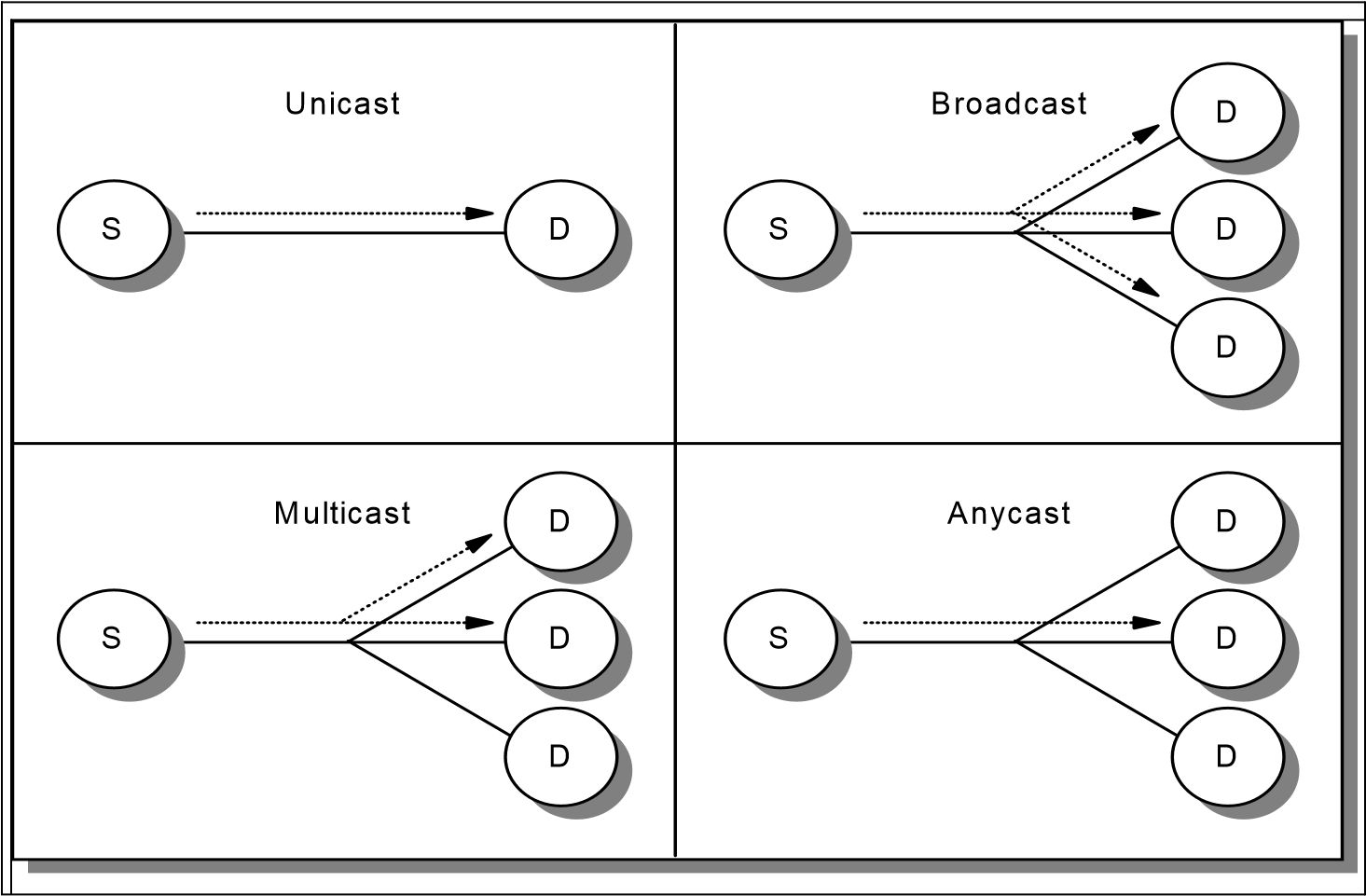
corresponding router's IP

address

*Figure 3-9 IP: Routing algorithm (with subnets)*

#### 3.1.4 Methods of delivery: Unicast, broadcast, multicast, and anycast

The majority of IP addresses refer to a single recipient, this is called a *unicast* address. Unicast connections specify a one-to-one relationship between a single source and a single destination. Additionally, there are three special types of IP addresses used for addressing multiple recipients: broadcast addresses, multicast addresses, and anycast addresses. Figure 3-10 shows their operation.



*Figure 3-10 IP: Packet delivery modes*

A *connectionless* protocol can send unicast, broadcast, multicast, or anycast messages. A *connection-oriented* protocol can only use unicast addresses (a connection must exist between a specific pair of hosts).

##### Broadcasting

Broadcast addresses are never valid as a source address. They must specify the destination address. The different types of broadcast addresses include:

Limited broadcast address: This uses the address 255.255.255.255 (all bits 1 in all parts of the IP address). It refers to all hosts on the local subnet. This is recognized by every host. The hosts do not need any IP configuration

information. Routers do not forward this packet.

One exception to this rule is called *BOOTP forwarding*. The BOOTP protocol uses the limited broadcast address to allow a diskless workstation to contact a boot server. BOOTP forwarding is a configuration option available on some routers. Without this facility, a separate BOOTP server is required on each subnet (refer to 3.6, “Bootstrap Protocol (BOOTP)” on page 125).

Network-directed broadcast address: This is used in an unsubnetted environment. The network number is a valid network number and the host number is all ones (for example, 128.2.255.255). This address refers to all hosts on the specified network. Routers should forward these broadcast messages. This is used in ARP requests (refer to 3.4, “Address Resolution Protocol (ARP)” on page 119) on unsubnetted networks.

Subnet-directed broadcast address: If the network number is a valid network number, the subnet number is a valid subnet number, and the host number is all ones, the address refers to all hosts on the specified subnet. Because the sender's subnet and the target subnet might have a different subnet mask, the sender must somehow determine the subnet mask in use at the target. The broadcast is performed by the router that receives the datagram into the subnet.

All-subnets-directed broadcast address: If the network number is a valid network number, the network is subnetted, and the local part is all ones (for example, 128.2.255.255), the address refers to all hosts on all subnets in the specified network. In principle, routers can propagate broadcasts for all subnets but are not required to do so. In practice, they do not. There are very few circumstances where such a broadcast is desirable. If misconfigured, it can lead to problems. Consider the misconfigured host 9.180.214.114 in a subnetted Class A network. If the device was configured with the address 9.255.255.255 as a local broadcast address instead of 9.180.214.255, all of the routers in the network will forward the request to all clients.

If routers do respect all-subnets-directed broadcast address, they use an algorithm called *reverse path forwarding* to prevent the broadcast messages from multiplying out of control. See RFC 922 for more details about this algorithm.

##### Multicasting

If an IP datagram is broadcast to a subnet, it is received by every host on the subnet. Each host processes the packet to determine if the target protocol is active. If it is not active, the IP datagram is discarded. Multicasting avoids this by selecting destination groups.

Each group is represented by a Class D IP address. For each multicast address, a set of zero or more hosts are listening for packets addressed to the address. This set of hosts is called the *host group*. Packets sent to a multicast address are forwarded only to the members of the corresponding host group. Multicast enables one-to-many connections (refer to Chapter 6, “IP multicast” on page 237).

##### Anycasting

Sometimes, the same IP services are provided by different hosts. For example, a user wants to download a file using FTP and the file is available on multiple FTP servers. Hosts that implement the same service provide an anycast address to other hosts that require the service. Connections are made to the first host in the anycast address group to respond. This process is used to guarantee the service is provided by the host with the best connection to the receiver.

The anycast service is included in IPV6 (refer to 9.2.2, “IPv6 addressing” on page 339).

#### 3.1.5 The IP address exhaustion problem

The number of networks on the Internet has been approximately doubling annually for a number of years. However, the usage of the Class A, B, and C networks differs greatly. Nearly all of the new networks assigned in the late 1980s were Class B, and in 1990 it became apparent that if this trend continued, the last Class B network number would be assigned during 1994. However, Class C networks were hardly being used.

The reason for this trend was that most potential users found a Class B network to be large enough for their anticipated needs, because it accommodates up to 65534 hosts, while a Class C network, with a maximum of 254 hosts, severely restricts the potential growth of even a small initial network. Furthermore, most of the Class B networks being assigned were small ones. There are relatively few networks that would need as many as 65,534 host addresses, but very few for which 254 hosts would be an adequate limit. In summary, although the Class A, Class B, and Class C divisions of the IP address are logical and easy-to-use (because they occur on byte boundaries), with hindsight, they are not the most practical because Class C networks are too small to be useful for most organizations, while Class B networks are too large to be densely populated by any but the largest organizations.

In May 1996, all Class A addresses were either allocated or assigned, as well as 61.95 percent of Class B and 36.44 percent of Class C IP network addresses.

The terms assigned and allocated in this context have the following meanings:

Assigned: The number of network numbers in use. The Class C figures are somewhat inaccurate, because the figures do not include many Class C

networks in Europe, which were allocated to RIPE and subsequently assigned but which are still recorded as allocated.

Allocated: This includes all of the assigned networks and additionally, those networks that have either been reserved by IANA (for example, the 63 Class A networks are all reserved by IANA) or have been allocated to regional registries by IANA and will subsequently be assigned by those registries.

Another way to look at these numbers is to examine the proportion of the address space that has been used. For example, the Class A address space is as big as the rest combined, and a single Class A network can theoretically have as many hosts as 66,000 Class C networks.

Since 1990, the number of assigned Class B networks has been increasing at a much lower rate than the total number of assigned networks and the anticipated exhaustion of the Class B network numbers has not yet occurred. The reason for this is that the policies on network number allocation were changed in late 1990 to preserve the existing address space, in particular to avert the exhaustion of the Class B address space. The new policies can be summarized as follows:

The upper half of the Class A address space (network numbers 64 to 127) is reserved indefinitely to allow for the possibility of using it for transition to a new numbering scheme.

Class B networks are only assigned to organizations that can clearly demonstrate a need for them. The same is, of course, true for Class A networks. The requirements for Class B networks are that the requesting organization:

* Has a subnetting plan that documents more than 32 subnets within its organizational network
* Has more than 4096 hosts

Any requirements for a Class A network are handled on an individual case basis.

Organizations that do not fulfill the requirements for a Class B network are assigned a consecutively numbered block of Class C network numbers.

The lower half of the Class C address space (network numbers 192.0.0 through 207.255.255) is divided into eight blocks, which are allocated to regional authorities as follows:

|  |  |  |
| --- | --- | --- |
| **192.0.0 - 193.255.255** | Multi-regional | |
| **194.0.0 - 195.255.255** | Europe | |
| **196.0.0 - 197.255.255** | Others | |
| **198.0.0 - 199.255.255** | North America | |
| **200.0.0 - 201.255.255** | Central and South America | |
| **202.0.0 - 203.255.255** | Pacific Rim | |
| **204.0.0 - 205.255.255 206.0.0 - 207.255.255 208.0.0 - 209.255.255**  **210.0.0 - 211.255.255** | Others  Others  ARIN1  APNIC | |
| **212.0.0 - 213.255.255** | RIPE NCC |
| **214.0.0 - 215.255.255** | US Department of Defense |
| **216.0.0 - 216.255.255** | ARIN |
| **217.0.0 - 217.255.255** | RIPE NCC |
| **218.0.0 - 218.255.255** | APNIC |
| **219.0.0 - 222.255.255** | APNIC |

The ranges defined as Others are to be where flexibility outside the constraints of regional boundaries is required. The range defined as multi-regional includes the Class C networks that were assigned before this new scheme was adopted. The 192 networks were assigned by the InterNIC and the 193 networks were previously allocated to RIPE in Europe.

Where an organization has a range of Class C network numbers, the range provided is assigned as a *bit-wise contiguous* range of network numbers, and the number of networks in the range is a power of 2. That is, all IP addresses in the range have a common prefix, and every address with that prefix is within the range. For example, a European organization requiring 1500 IP addresses would be assigned eight Class C network numbers (2048 IP addresses) from the number space reserved for European networks (194.0.0 through 195.255.255) and the first of these network numbers would be divisible by eight. A range of addresses satisfying these rules is 194.32.136 through 194.32.143, in which case the range consists of all of the IP addresses with the 21-bit prefix 194.32.136, or B '110000100010000010001'.

The maximum number of network numbers assigned contiguously is 64, corresponding to a prefix of 18 bits. An organization requiring more than 4096 addresses but less than 16,384 addresses can request either a Class B or a range of Class C addresses. In general, the number of Class C networks assigned is the minimum required to provide the necessary number of IP addresses for the organization on the basis of a two-year outlook. However, in some cases, an organization can request multiple networks to be treated separately. For example, an organization with 600 hosts is normally assigned four Class C networks. However, if those hosts were distributed across 10 LANs with between 50 and 70 hosts per LAN, such an allocation can cause serious problems, because the organization would have to find 10 subnets within a 10-bit local address range. This means at least some of the LANs have a subnet mask of 255.255.255.192, which allows only 62 hosts per LAN. The intent of the rules is not to force the organization into complex subnetting

of small networks, and the organization should request 10 different Class C numbers, one for each LAN.

1 Information for this and the following numbers in this list are from:

<http://www.iana.org/assignments/ipv4-address-space>

The current rules are in RFC 2050, which updates RFC 1466. The reasons for the rules for the allocation of Class C network numbers will become apparent in the following sections. The use of Class C network numbers in this way has averted the exhaustion of the Class B address space, but it is not a permanent solution to the overall address space constraints that are fundamental to IP. We discuss a long-term solution in Chapter 9, “IP version 6” on page 327.

#### 3.1.6 Intranets: Private IP addresses

Another approach to conserve the IP address space is described in RFC 1918. This RFC relaxes the rule that IP addresses must be globally unique. It reserves part of the global address space for use in networks that do not require connectivity to the Internet. Typically these networks are administered by a single organization. Three ranges of addresses have been reserved for this purpose:

10.0.0.0: A single Class A network

172.16.0.0 through 172.31.0.0: 16 contiguous Class B networks

192.168.0.0 through 192.168.255.0: 256 contiguous Class C networks

Any organization can use any address in these ranges. However, because these addresses are not globally unique, they are not defined to any external routers. Routers in networks not using private addresses, particularly those operated by Internet service providers, are expected to quietly discard all routing information regarding these addresses. Routers in an organization using private addresses are expected to limit all references to private addresses to internal links. They should neither externally advertise routes to private addresses nor forward IP datagrams containing private addresses to external routers.

Hosts having only a private IP address do not have direct IP layer connectivity to the Internet. All connectivity to external Internet hosts must be provided with application gateways (refer to “Application-level gateway (proxy)” on page 798), SOCKS (refer to 22.5, “SOCKS” on page 846), or Network Address Translation (NAT), which is discussed in the next section.

#### 3.1.7 Network Address Translation (NAT)

This section explains Traditional Network Address Translation (NAT), Basic NAT, and Network Address Port Translation (NAPT). NAT is also known as IP masquerading. It provides a mapping between internal IP addresses and officially assigned external addresses.

Originally, NAT was suggested as a short-term solution to the IP address exhaustion problem. Also, many organizations have, in the past, used locally assigned IP addresses, not expecting to require Internet connectivity.

There are two variations of traditional NAT, Basic NAT and NAPT. Traditional NAT is defined in RFC 3022 and discussed in RFC 2663. The following sections provide a brief discussion of Traditional NAT, Basic NAT, and NAPT based on RFC 3022.

##### Traditional NAT

The idea of Traditional NAT (hereafter referred to as NAT) is based on the fact that only a small number of the hosts in a private network are communicating outside of that network. If each host is assigned an IP address from the official IP address pool only when they need to communicate, only a small number of official addresses are required.

NAT might be a solution for networks that have private address ranges or unofficial addresses and want to communicate with hosts on the Internet. When a proxy server, SOCKS server, or firewall are not available, or do not meet specific requirements, NAT might be used to manage the traffic between the internal and external network without advertising the internal host addresses.

##### Basic NAT

Consider an internal network that is based on the private IP address space, and the users want to use an application protocol for which there is no application gateway; the only option is to establish IP-level connectivity between hosts in the internal network and hosts on the Internet. Because the routers in the Internet would not know how to route IP packets back to a private IP address, there is no point in sending IP packets with private IP addresses as source IP addresses through a router into the Internet.

As shown in Figure 3-11, Basic NAT takes the IP address of an outgoing packet and dynamically translates it to an officially assigned global address. For incoming packets, it translates the assigned address to an internal address.



Non-Secure

a.b.1.0/24

a.b.1.1

10.0.1.1

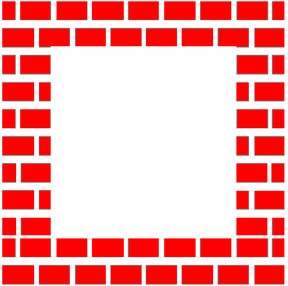
Secure

src=a.b.1.1 dest=a.b.2.1

src=a.b.1.1 dest=10.0.1.1



10.0.0.0/8



NAT

Filtering

TCP/UDP

IP/ICMP



NAT Configuration

**RESERVE a.b.2.0 255.255.255.0**

**TRANSLATE 10.0.0.0 255.0.0.0**



Filtering Rules

Based on non-translated

IP addresses (10.x.x.x)

*Figure 3-11 Basic Network Address Translation (NAT)*

From the point of two hosts that exchange IP packets with each other, one in the internal network and one in the external network, the NAT itself is transparent (see Figure 3-12).



Non-Secure

a.b.1.0/24

a.b.1.1

Looks like a

normal router

src=a.b.1.1 dest=a.b.2.1

a.b.2.0/24

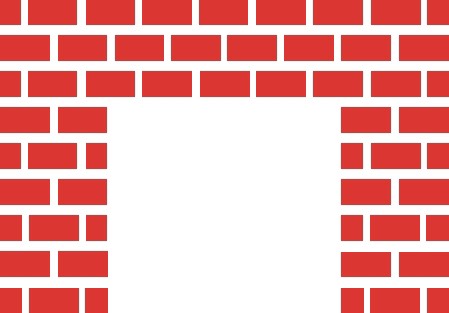
a.b.2.1

Secure

*Figure 3-12 NAT seen from the external network*

##### Basic NAT translation mechanism

For each outgoing IP packet, the source address is checked by the NAT configuration rules. If a rule matches the source address, the address is translated to a global address from the address pool. The predefined address pool contains the addresses that NAT can use for translation. For each incoming packet, the destination address is checked if it is used by NAT. When this is true, the address is translated to the original internal address. Figure 3-13 shows the Basic NAT configuration.



To be translated

Exclude

Secure network

Non-secure network

Reserve

N

A

T

Exclude

Firewall

Map

Pool

*Figure 3-13 Basic NAT configuration*

When Basic NAT translates an address for an IP packet, the checksum is also adjusted. For FTP packets, the task is even more difficult, because the packets can contain addresses in the data of the packet. For example, the FTP PORT command contains an IP address in ASCII. These addresses should also be translated correctly; checksum updates and TCP sequence and acknowledgement updates should also be made accordingly.

In order to make the routing tables work, the IP network design needs to choose addresses as though connecting two or more IP networks or subnets through a router. The NAT IP addresses need to come from separate networks or subnets, and the addresses need to be unambiguous with respect to other networks or subnets in the non-secure network. If the external network is the Internet, the NAT addresses need to come from a public network or subnet; in other words, the NAT addresses need to be assigned by IANA.

The assigned addresses need to be reserved in a pool in order to use them when needed. If connections are established from the internal network, NAT can just pick the next free public address in the NAT pool and assign that to the requesting internal host. The NAT service keeps track of which internal IP addresses are mapped to which external IP addresses at any given point in time, so it will be able to map a response it receives from the external network into the corresponding secure IP address.

When the NAT service assigns IP addresses on a demand basis, it needs to know when to return the external IP address to the pool of available IP addresses. There is no connection setup or tear-down at the IP level, so there is nothing in the IP protocol itself that the NAT service can use to determine when an association between a internal IP address and a NAT external IP address is no longer needed. Because TCP is a connection-oriented protocol, it is possible to obtain the connection status information from TCP header (whether connection is ended or not), while UDP does not include such information. Therefore, configure a timeout value that instructs NAT how long to keep an association in an idle state before returning the external IP address to the free NAT pool. Generally, the default value for this parameter is 15 minutes.

Network administrators also need to instruct NAT whether all the internal hosts are allowed to use NAT or not. This can be done by using corresponding configuration commands. If hosts in the external network need to initiate connections to hosts in the internal network, NAT needs to be configured in advance as to which external NAT address matches which internal IP address. Thus, a static mapping should be defined to allow connections from outside networks to a specific host in the internal network. Note that the external NAT addresses as statically mapped to internal IP addresses should not overlap with the addresses specified as belonging to the pool of external addresses that the NAT service can use on a demand basis.

The external name server can, for example, have an entry for a mail gateway that runs on a computer in the internal network. The external name server resolves the public host name of the internal mail gateway to the statically mapped IP address (the external address), and the remote mail server sends a connection request to this IP address. When that request comes to the NAT service on the external interface, the NAT service looks into its mapping rules to see if it has a static mapping between the specified external public IP address and a internal IP address. If so, it translates the IP address and forwards the IP packet into the internal network to the mail gateway.

##### Network Address Port Translation (NAPT)

The difference between Basic NAT and NAPT is that Basic NAT is limited to only translating IP addresses, while NAPT is extended to include IP address and transport identifier (such as TCP/UDP port or ICMP query ID).

As shown in Figure 3-14, Network Address Port Translation is able to translate many network addresses and their transport identifiers into a single network address with many transport identifiers, or more specifically, ports.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Transition Table  10.10.10.11:80 = a.b.65.1:8000  10.10.10.12:80 = a.b.65.1:8001 |  |  |
| External  a.b.65.0 /30  a.b.65.3 /30 |  | Internal  10.10.10.0 /24 | 10.10.10.11 /24  10.10.10.12 /24 |
| NAPT |

*Figure 3-14 Network Address Port Translation*

NAPT maps private addresses to a single globally unique address. Therefore, the binding is from the private address and private port to the assigned address and assigned port. NAPT permits multiple nodes in a local network to simultaneously access remote networks using the single IP address assigned to their router.

In NAPT, modifications to the IP header are similar to that of Basic NAT. However for TCP/UDP sessions, modifications must be extended to include translation of the source port for outbound packets and destination port for inbound packets in the TCP/UDP header. In addition to TCP/UDP sessions, ICMP messages, with the exception of the REDIRECT message type, can also be monitored by the NAPT service running on the router. ICMP query type packets are translated similar to that of TCP/UDP packets in that the identifier field in ICMP message header will be uniquely mapped to a query identifier of the registered IP address.

##### NAT limitations

The NAT limitations are mentioned in RFC 3022 and RFC2663. We discuss some of the limitations here.

NAT works fine for IP addresses in the IP header. Some application protocols exchange IP address information in the application data part of an IP packet, and NAT will generally not be able to handle translation of IP addresses in the application protocol. Currently, most of the implementations handle the FTP protocol. It should be noted that implementation of NAT for specific applications that have IP information in the application data is more sophisticated than the standard NAT implementations.

NAT is compute intensive even with the assistance of a sophisticated checksum adjustment algorithm, because each data packet is subject to NAT lookup and modifications.

It is mandatory that all requests and responses pertaining to a session be routed through the same router that is running the NAT service.

Translation of outbound TCP/UDP fragments (that is, those originating from private hosts) in a NAPT setup will not work (refer to “Fragmentation” on page 104). This is because only the first fragment contains the TCP/UDP header that is necessary to associate the packet to a session for translation purposes. Subsequent fragments do not contain TCP/UDP port information, but simply carry the same fragmentation identifier specified in the first fragment. When the target host receives the two unrelated datagrams, carrying the same fragmentation ID and from the same assigned host address, it is unable to determine to which of the two sessions the datagrams belong. Consequently, both sessions will be corrupted.

NAT changes some of the address information in an IP packet. This becomes an issue when IPSec is used. Refer to 22.4, “IP Security Architecture (IPSec)” on page 809 and 22.10, “Virtual private networks (VPNs) overview” on page 861. When end-to-end IPSec authentication is used, a packet whose address has been changed will always fail its integrity check under the Authentication Header protocol, because any change to any bit in the datagram will invalidate the integrity check value that was generated by the source. Because IPSec protocols offer some solutions to the addressing issues that were previously handled by NAT, there is no need for NAT when all hosts that compose a given virtual private network use globally unique (public) IP addresses. Address hiding can be achieved by the IPSec tunnel mode. If a company uses private addresses within its intranet, the IPSec tunnel mode can keep them from ever appearing in cleartext from in the public Internet, which eliminates the need for NAT.

#### 3.1.8 Classless Inter-Domain Routing (CIDR)

Standard IP routing understands only Class A, B, and C network addresses. Within each of these networks, subnetting can be used to provide better granularity. However, there is no way to specify that multiple Class C networks are related. The result of this is termed the *routing table explosion* problem: A Class B network of 3000 hosts requires one routing table entry at each backbone

router. The same environment, if addressed as a range of Class C networks, requires 16 entries.

The solution to this problem is called Classless Inter-Domain Routing (CIDR).

CIDR is described in RFCs 1518 to 1520. CIDR does not route according to the

class of the network number (thus the term classless). It is based solely on the high order bits of the IP address. These bits are called the IP prefix.

Each CIDR routing table entry contains a 32-bit IP address and a 32-bit network mask, which together give the length and value of the IP prefix. This is represented as the tuple <IP\_address network\_mask>. For example, to address a block of eight Class C addresses with one single routing table entry, the following representation suffices: <192.32.136.0 255.255.248.0>. This refers, from a backbone point of view, to the Class C network range from 192.32.136.0 to 192.32.143.0 as one single network. This is illustrated in Figure 3-15.

11000000 00100000 10001000 00000000 = 192.32.136.0 (Class C address)

11111111 11111111 11111--- -------- 255.255.248.0 (network mask)

===================================== logical\_AND

11000000 00100000 10001--- -------- = 192.32.136 (IP prefix)

11000000 00100000 10001111 00000000 = 192.32.143.0 (Class C address)

11111111 11111111 11111--- -------- 255.255.248.0 (network mask)

===================================== logical\_AND

11000000 00100000 10001--- -------- = 192.32.136 (same IP prefix)

*Figure 3-15 Classless Inter-Domain Routing: IP supernetting example*

This process of combining multiple networks into a single entry is referred to as *supernetting*. Routing is based on network masks that are shorter than the natural network mask of an IP address. This contrasts with subnetting (see 3.1.2, “IP subnets” on page 72) where the subnet masks are longer than the natural network mask.

The current Internet address allocation policies and the assumptions on which those policies were based are described in RFC 1518. They can be summarized as follows:

IP address assignment reflects the physical topology of the network and not the organizational topology. Wherever organizational and administrative boundaries do not match the network topology, they should *not* be used for the assignment of IP addresses.

In general, network topology will closely follow continental and national boundaries. Therefore, IP addresses should be assigned on this basis.

There will be a relatively small set of networks that carry a large amount of traffic between routing domains. These networks will be interconnected in a non-hierarchical way that crosses national boundaries. These networks are referred to as *transit routing domains (TRDs)* Each TRD will have a unique IP prefix. TRDs will not be organized in a hierarchical way when there is no appropriate hierarchy. However, whenever a TRD is wholly within a continental boundary, its IP prefix should be an extension of the continental IP prefix.

There will be many organizations that have attachments to other organizations that are for the private use of those two organizations. The attachments do not carry traffic intended for other domains (transit traffic). Such private connections do not have a significant effect on the routing topology and can be ignored.

The great majority of routing domains will be single-homed. That is, they will be attached to a single TRD. They should be assigned addresses that begin with that TRD's IP prefix. All of the addresses for all single-homed domains attached to a TRD can therefore be aggregated into a single routing table entry for all domains outside that TRD.

There are a number of address assignment schemes that can be used for multihomed domains. These include:

* The use of a single IP prefix for the domain. External routers must have an entry for the organization that lies partly or wholly outside the normal hierarchy. Where a domain is multihomed, but all of the attached TRDs themselves are topologically nearby, it is appropriate for the domain's IP prefix to include those bits common to all of the attached TRDs. For example, if all of the TRDs were wholly within the United States, an IP prefix implying an exclusively North American domain is appropriate.
* The use of one IP prefix for each attached TRD with hosts in the domain having IP addresses containing the IP prefix of the most appropriate TRD. The organization appears to be a set of routing domains.
* Assigning an IP prefix from one of the attached TRDs. This TRD becomes a default TRD for the domain but other domains can explicitly route by one of the alternative TRDs.
* The use of IP prefixes to refer to sets of multihomed domains having the TRD attachments. For example, there can be an IP prefix to refer to single-homed domains attached to network A, one to refer to

single-homed domains attached to network B, and one to refer to dual-homed domains attached to networks A and B.

Each of these has various advantages, disadvantages, and side effects. For example, the first approach tends to result in inbound traffic entering the target domain closer to the sending host than the second approach.

Therefore, a larger proportion of the network costs are incurred by the receiving organization.

Because multihomed domains vary greatly in character, none of the these schemes is suitable for every domain. There is no single policy that is best. RFC 1518 does not specify any rules for choosing between them.

##### CIDR implementation

The implementation of CIDR in the Internet is primarily based on Border Gateway Protocol Version 4 (see 5.9, “Border Gateway Protocol (BGP)” on page 215). The implementation strategy, described in RFC 1520, involves a staged process through the routing hierarchy beginning with backbone routers. Network service providers are divided into four types:

Type 1: Those providers that cannot employ any default inter-domain routing.

Type 2: Those providers that use default inter-domain routing but require explicit routes for a substantial proportion of the assigned IP network numbers.

Type 3: Those providers that use default inter-domain routing and supplement it with a small number of explicit routes.

Type 4: Those providers that perform inter-domain routing using only default routes.

The CIDR implementation began with the Type 1 network providers, then the Type 2, and finally the Type 3 providers. CIDR has already been widely deployed in the backbone and more than 190,000 class-based routes have been replaced by approximately 92,000 CIDR-based routes (through unique announced aggregates).

#### 3.1.9 IP datagram

The unit of transfer in an IP network is called an IP datagram. It consists of an IP header and data relevant to higher-level protocols. See Figure 3-16 for details.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | header | data |   base IP datagram...   |  |  | | --- | --- | | physical network header | IP datagram as data |   encapsulated within the physical network's frame |

*Figure 3-16 IP: Format of a base IP datagram*

IP can provide fragmentation and reassembly of datagrams. The maximum length of an IP datagram is 65,535 octets. All IP hosts must support 576 octets datagrams without fragmentation.

Fragments of a datagram each have a header. The header is copied from the original datagram. A fragment is treated as a normal IP datagrams while being transported to their destination. However, if one of the fragments gets lost, the complete datagram is considered lost. Because IP does not provide any acknowledgment mechanism, the remaining fragments are discarded by the destination host.

##### IP datagram format

The IP datagram header has a minimum length of 20 octets, as illustrated in Figure 3-17.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 1 2 3  0 4 8 6 9 4 1   |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | VERS |  | HLEN | | Service Type | Total | | Length | |  |  | ID | | | FLG | | Fragment Offset | |  | TTL |  | Protocol | |  | | Header Checksum | |  |  | Source IP Ad | | | | | dress | |  |  | Destination IP | | | | | Address | |  |  | IP Options | | | |  | Padding | |  |  | Data …  …  … | | | | |  | |

*Figure 3-17 IP: Format of an IP datagram header*

Where:

VERS: The field contains the IP protocol version. The current version is 4. Version 5 is an experimental version. Version 6 is the version for IPv6 (see 9.2, “The IPv6 header format” on page 330).

HLEN: The length of the IP header counted in 32-bit quantities. This does not include the data field.

Service Type: The service type is an indication of the quality of service requested for this IP datagram. This field contains the information illustrated in Figure 3-18.

|  |  |  |  |
| --- | --- | --- | --- |
| 0 1 2 3 4 5 6 7   |  |  |  | | --- | --- | --- | | precedence | TOS | MBZ | |

*Figure 3-18 IP: Service type*

Where:

* Precedence: This field specifies the nature and priority of the datagram:
  + 000: Routine
  + 001: Priority
  + 010: Immediate
  + 011: Flash
  + 100: Flash override
  + 101: Critical
  + 110: Internetwork control
  + 111: Network control
* TOS: Specifies the type of service value:
  + 1000: Minimize delay
  + 0100: Maximize throughput
  + 0010: Maximize reliability
  + 0001: Minimize monetary cost
  + 0000: Normal service

A detailed description of the type of service is in the RFC 1349 (refer to 8.1, “Why QoS?” on page 288).

* MBZ:Reserved for future use.

Total Length: The total length of the datagram, header and data.

Identification: A unique number assigned by the sender to aid in reassembling a fragmented datagram. Each fragment of a datagram has the same identification number.

Flags: This field contains control flags illustrated in Figure 3-19.

0

0

1

2

D

F

M

F

*Figure 3-19 IP: Flags*

Where:

* 0: Reserved, must be zero.
* DF (Do not Fragment): 0 means allow fragmentation; 1 means do not allow fragmentation.
* MF (More Fragments): 0 means that this is the last fragment of the datagram; 1 means that additional fragments will follow.

Fragment Offset: This is used to aid the reassembly of the full datagram. The value in this field contains the number of 64-bit segments (header bytes are not counted) contained in earlier fragments. If this is the first (or only) fragment, this field contains a value of zero.

Time to Live: This field specifies the time (in seconds) the datagram is allowed to travel. Theoretically, each router processing this datagram is supposed to subtract its processing time from this field. In practise, a router processes the datagram in less than 1 second. Therefore, the router subtracts one from the value in this field. The TTL becomes a hop-count metric rather than a time metric. When the value reaches zero, it is assumed that this datagram has been traveling in a closed loop and is discarded. The initial value should be set by the higher-level protocol that creates the datagram.

Protocol Number: This field indicates the higher-level protocol to which IP should deliver the data in this datagram. These include:

* 0: Reserved
* 1: Internet Control Message Protocol (ICMP)
* 2: Internet Group Management Protocol (IGMP)
* 3: Gateway-to-Gateway Protocol (GGP)
* 4: IP (IP encapsulation)
* 5: Stream
* 6: Transmission Control Protocol (TCP)
* 8: Exterior Gateway Protocol (EGP)
* 9: Interior Gateway Protocol (IGP)
* 17: User Datagram Protocol (UDP)
* 41:Simple Internet Protocol (SIP)
* 50: SIPP Encap Security Payload (ESP)
* 51: SIPP Authentication Header (AH)
* 89: Open Shortest Path First (OSPF) IGP

The complete list is in STD 2 – Assigned Internet Numbers.

Header Checksum: This field is a checksum for the information contained in the header. If the header checksum does not match the contents, the datagram is discarded.

Source IP Address: The 32-bit IP address of the host sending this datagram. Destination IP Address: The 32-bit IP address of the destination host for this datagram.

Options: An IP implementation is not required to be capable of generating options in a datagram. However, all IP implementations are required to be able to process datagrams containing options. The Options field is variable in length (there can be zero or more options). There are two option formats. The format for each is dependent on the value of the option number found in the first octet:

* A type octet alone is illustrated in Figure 3-20.

|  |  |
| --- | --- |
| |  | | --- | | type |   1 byte |

*Figure 3-20 IP: A type byte*

* A type octet, a length octet, and one or more option data octets, as illustrated in Figure 3-21.

type

length

option data...

/ /

/ /

1

byte

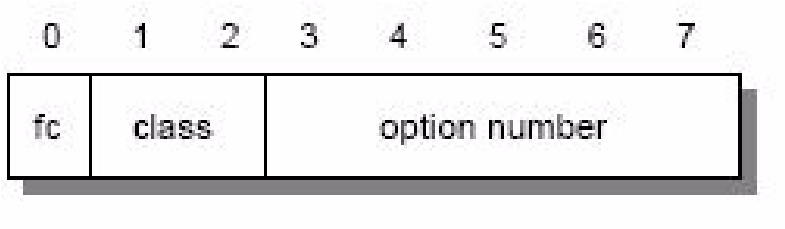
length - 2 bytes

1

byte

*Figure 3-21 IP: A type byte, a length byte, and one or more option data bytes*

The type byte has the same structure in both cases, as illustrated in Figure 3-22.



*Figure 3-22 IP: The type byte structure*

Where:

* fc (Flag copy): This field indicates whether (1) or not (0) the option field is copied when the datagram is fragmented.
* class: The option class is a 2-bit unsigned integer:
  + 0: Control
  + 1: Reserved
  + 2: Debugging and measurement
  + 3: Reserved
* option number: The option number is a 5-bit unsigned integer:
  + 0: End of option list. It has a class of 0, the fc bit is set to zero, and it has no length byte or data. That is, the option list is terminated by a X'00' byte. It is only required if the IP header length (which is a multiple of 4 bytes) does not match the actual length of the options.
  + 1: No operation. It has a class of 0, the fc bit is not set, and there is no length byte or data. That is, a X'01' byte is a NOP. It can be used to align fields in the datagram.
  + 2: Security. It has a class of 0, the fc bit is set, and there is a length byte with a value of 11 and 8 bytes of data). It is used for security information needed by U.S. Department of Defense requirements.
  + 3: Loose source routing. It has a class of 0, the fc bit is set, and there is a variable length data field. We discuss this option in more detail later.
  + 4: Internet time stamp. It has a class of 2, the fc bit is not set, and there is a variable length data field. The total length can be up to 40 bytes. We discuss this option in more detail later.
  + 7: Record route. It has a class of 0, the fc bit is not set, and there is a variable length data field. We discuss this option in more detail later.
  + 8: Stream ID. It has a class of 0, the fc bit is set, and there is a length byte with a value of 4 and one data byte. It is used with the SATNET system.
  + 9: Strict source routing. It has a class of 0, the fc bit is set, and there is a variable length data field. We discuss this option in more detail later.
* length: This field counts the length (in octets) of the option, including the type and length fields.
* option data: This field contains data relevant to the specific option.

Padding: If an option is used, the datagram is padded with all-zero octets up to the next 32-bit boundary.

Data: The data contained in the datagram. It is passed to the higher-level protocol specified in the protocol field.

##### Fragmentation

When an IP datagram travels from one host to another, it can pass through different physical networks. Each physical network has a maximum frame size. This is called the *maximum transmission unit* (MTU). It limits the length of a datagram that can be placed in one physical frame.

IP implements a process to fragment datagrams exceeding the MTU. The process creates a set of datagrams within the maximum size. The receiving host reassembles the original datagram. IP requires that each link support a minimum MTU of 68 octets. This is the sum of the maximum IP header length (60 octets) and the minimum possible length of data in a non-final fragment (8 octets). If any network provides a lower value than this, fragmentation and reassembly must be implemented in the network interface layer. This must be transparent to IP. IP implementations are not required to handle unfragmented datagrams larger than 576 bytes. In practice, most implementations will accommodate larger values.

An unfragmented datagram has an all-zero fragmentation information field. That is, the more fragments flag bit is zero and the fragment offset is zero. The following steps fragment the datagram:

1. The DF flag bit is checked to see if fragmentation is allowed. If the bit is set, the datagram will be discarded and an ICMP error returned to the originator.
2. Based on the MTU value, the data field is split into two or more parts. All newly created data portions must have a length that is a multiple of 8 octets, with the exception of the last data portion.
3. Each data portion is placed in an IP datagram. The headers of these datagrams are minor modifications of the original:
   * The more fragments flag bit is set in all fragments except the last.
   * The fragment offset field in each is set to the location this data portion occupied in the original datagram, relative to the beginning of the original unfragmented datagram. The offset is measured in 8-octet units.
   * If options were included in the original datagram, the high order bit of the option type byte determines if this information is copied to all fragment datagrams or only the first datagram. For example, source route options are copied in all fragments.
   * The header length field of the new datagram is set.
   * The total length field of the new datagram is set.
   * The header checksum field is re-calculated.
4. Each of these fragmented datagrams is now forwarded as a normal IP datagram. IP handles each fragment independently. The fragments can traverse different routers to the intended destination. They can be subject to further fragmentation if they pass through networks specifying a smaller MTU.

At the destination host, the data is reassembled into the original datagram. The identification field set by the sending host is used together with the source and destination IP addresses in the datagram. Fragmentation does not alter this field.

In order to reassemble the fragments, the receiving host allocates a storage buffer when the first fragment arrives. The host also starts a timer. When subsequent fragments of the datagram arrive, the data is copied into the buffer storage at the location indicated by the fragment offset field. When all fragments have arrived, the complete original unfragmented datagram is restored. Processing continues as for unfragmented datagrams.

If the timer is exceeded and fragments remain outstanding, the datagram is discarded. The initial value of this timer is called the IP datagram time to live (TTL) value. It is implementation-dependent. Some implementations allow it to be configured.

The **netstat** command can be used on some IP hosts to list the details of fragmentation.

##### IP datagram routing options

The IP datagram Options field provides two methods for the originator of an IP datagram to explicitly provide routing information. It also provides a method for an IP datagram to determine the route that it travels.

###### Loose source routing

The loose source routing option, also called the loose source and record route (LSRR) option, provides a means for the source of an IP datagram to supply explicit routing information. This information is used by the routers when forwarding the datagram to the destination. It is also used to record the route, as illustrated in Figure 3-23.

10000011

length

pointer

route data

//

/

/

*Figure 3-23 IP: Loose source routing option*

The fields of this header include:

**1000011(decimal 131)** This is the value of the option type octet for loose source routing.

**Length** This field contains the length of this option field,

including the type and length fields.

|  |  |
| --- | --- |
| **Pointer** | This field points to the option data at the next IP address to be processed. It is counted relative to the beginning of the option, so its minimum value is four. If the pointer is greater than the length of the option, the end of the source route is reached and further routing is to be based on the destination IP address (as for datagrams without this option). |
| **Route data** | This field contains a series of 32-bit IP addresses. |

When a datagram arrives at its destination and the source route is not empty (pointer < length) the receiving host:

1. Takes the next IP address in the route data field (the one indicated by the pointer field) and puts it in the destination IP address field of the datagram.
2. Puts the local IP address in the source list at the location pointed to by the pointer field. The IP address for this is the local IP address corresponding to the network on which the datagram will be forwarded. (Routers are attached to multiple physical networks and thus have multiple IP addresses.)
3. Increments the pointer by 4.
4. Transmits the datagram to the new destination IP address.

This procedure ensures that the return route is recorded in the route data (in reverse order) so that the final recipient uses this data to construct a loose source route in the reverse direction. This is a *loose* source route because the forwarding router is allowed to use any route and any number of intermediate routers to reach the next address in the route.

###### Strict source routing

The strict source routing option, also called the strict source and record route (SSRR) option, uses the same principle as loose source routing except the intermediate router *must* send the datagram to the next IP address in the source route through a directly connected network. It cannot use an intermediate router. If this cannot be done, an ICMP Destination Unreachable error message is issued. Figure 3-24 gives an overview of the SSRR option.

*Figure 3-24 IP: Strict source routing option*

100001001

length

pointer

route data

//

/

/

Where:

**1001001 (Decimal 137)** The value of the option type byte for strict source routing.

**Length** This information is described in “Loose source routing” on page 105.

**Pointer** This information is described in “Loose source routing” on page 105.

**Route data** A series of 32-bit IP addresses.

###### Record route

This option provides a means to record the route traversed by an IP datagram. It functions similarly to the source routing option. However, this option provides an empty routing data field. This field is filled in as the datagram traverses the network. Sufficient space for this routing information must be provided by the source host. If the data field is filled before the datagram reaches its destination, the datagram is forwarded with no further recording of the route. Figure 3-25 gives an overview of the record route option.

00000111

length

pointer

route data

//

/

/

*Figure 3-25 IP: Record route option*

Where:

|  |  |
| --- | --- |
| **0000111 (Decimal 7)** | The value of the option type byte for record route |
| **Length** | This information is described in “Loose source routing” on page 105. |
| **Pointer** | This information is described in “Loose source routing” on page 105. |
| **Route data** | A series of 32-bit IP addresses. |

##### Internet time stamp

A time stamp is an option forcing some (or all) of the routers along the route to the destination to put a time stamp in the option data. The time stamps are

measured in seconds and can be used for debugging purposes. They cannot be used for performance measurement for two reasons:

Because most IP datagrams are forwarded in less than one second, the time stamps are not precise.

Because IP routers are not required to have synchronized clocks, they may not be accurate.

Figure 3-26 gives an overview of the Internet time stamp option.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 8 16 24 28   |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | 01000100 | length |  | pointer | oflw | flag | |  | IP address | |  |  | | |  | time st | amp |  |  | | |  | ... |  |  |  | | |

*Figure 3-26 IP: Internet time stamp option*

Where:

|  |  |  |
| --- | --- | --- |
| **01000100 (Decimal 68)** | | This field is the value of the option type for the internet time stamp option. |
| **Length** |  | This field contains the total length of this option, including the type and length fields. |
| **Pointer** |  | This field points to the next time stamp to be processed (first free time stamp). |
| **Oflw (overflow)** |  | This field contains the number of devices that cannot register time stamps due to a lack of space in the data field. |
| **Flag** |  | This field is a 4-bit value that indicates how time stamps are to be registered:   1. Time stamps only, stored in consecutive 32-bit words. 2. Each time stamp is preceded by the IP address of the registering device. 3. The IP address fields are prespecified; an IP device only registers when it finds its own address in the list. |
| **Time stamp** | A 32-bit time stamp recorded in milliseconds since midnight UT (GMT). | |

The originating host must compose this option with a sufficient data area to hold all the time stamps. If the time stamp area becomes full, no further time stamps are added.

### 3.2 Internet Control Message Protocol (ICMP)

ICMP is a standard protocol with STD number 5. That standard also includes IP

(see 3.1, “Internet Protocol (IP)” on page 68) and IGMP (see 6.2, “Internet Group

Management Protocol (IGMP)” on page 241). Its status is required. It is described in RFC 792 with updates in RFC 950. ICMPv6 used for IPv6 is discussed in 9.3, “Internet Control Message Protocol Version 6 (ICMPv6)” on page 352.

Path MTU Discovery is a draft standard protocol with a status of elective. It is described in RFC 1191.

ICMP Router Discovery is a proposed standard protocol with a status of elective. It is described in RFC 1256.

When a router or a destination host must inform the source host about errors in datagram processing, it uses the Internet Control Message Protocol (ICMP). ICMP can be characterized as follows:

ICMP uses IP as though ICMP were a higher-level protocol (that is, ICMP messages are encapsulated in IP datagrams). However, ICMP is an integral part of IP and must be implemented by every IP module.

ICMP is used to report errors, *not* to make IP reliable. Datagrams can still be undelivered without any report on their loss. Reliability must be implemented by the higher-level protocols using IP services.

ICMP cannot be used to report errors with ICMP messages. This avoids infinite repetitions. ICMP responses are sent in response to ICMP query messages (ICMP types 0, 8, 9, 10, and 13 through 18).

For fragmented datagrams, ICMP messages are only sent about errors with the first fragment. That is, ICMP messages never refer to an IP datagram with a non-zero fragment offset field.

ICMP messages are never sent in response to datagrams with a broadcast or a multicast destination address.

ICMP messages are never sent in response to a datagram that does not have a source IP address representing a unique host. That is, the source address cannot be zero, a loopback address, a broadcast address, or a multicast address.

RFC 792 states that ICMP messages *can* be generated to report IP datagram processing errors. However, this is not required. In practice, routers will almost always generate ICMP messages for errors. For destination hosts, ICMP message generation is implementation dependent.

#### 3.2.1 ICMP messages

ICMP messages are described in RFC 792 and RFC 950, belong to STD 5, and are mandatory.

ICMP messages are sent in IP datagrams. The IP header has a protocol number of 1 (ICMP) and a type of service of zero (routine). The IP data field contains the ICMP message shown in Figure 3-27.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 8 16 31   |  |  |  |  | | --- | --- | --- | --- | | identifier | sequence number |  | checksum | | ICMP data (depending on the type of mes | | sage) |  | |

*Figure 3-27 ICMP: Message format*

The message contains the following components:

**Type** Specifies the type of the message:

**0** Echo reply

1. Destination unreachable
2. Source quench
3. Redirect
4. Echo
5. Router advertisement
6. Router solicitation
7. Time exceeded
8. Parameter problem
9. Time stamp request
10. Time stamp reply
11. Address mask request
12. Address mask reply

**30** Traceroute

1. Domain name request)
2. Domain name reply)

The following RFCs are required to be mentioned for some of the ICMP message types: RFC 1256, RFC 1393, and RFC 1788.

|  |  |
| --- | --- |
| **Code** | Contains the error code for the datagram reported by this  ICMP message. The interpretation is dependent on the |
| **Checksum** | message type.    Contains the checksum for the ICMP message starting with the ICMP Type field. If the checksum does not match the contents, the datagram is discarded. |

**Data** Contains information for this ICMP message. Typically, it

will contain the portion of the original IP message for which this ICMP message was generated.

Each of the ICMP messages is described individually.

##### Echo (8) and Echo Reply (0)

Echo is used to detect if another host is active in the network. It is used by the Ping command (refer to “Ping” on page 117). The sender initializes the identifier, sequence number, and data field. The datagram is then sent to the destination host. The recipient changes the type to Echo Reply and returns the datagram to the sender. See Figure 3-28 for more details.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 0 8 16 31   |  |  | | --- | --- | | identifier | sequence number | |  | data ... | |

*Figure 3-28 Echo and Echo Reply*

##### Destination Unreachable (3)

If this message is received from an intermediate router, it means that the router regards the destination IP address as unreachable.

If this message is received from the destination host, it means that either the protocol specified in the protocol number field of the original datagram is not active or the specified port is inactive. (Refer to 4.2, “User Datagram Protocol (UDP)” on page 146 for additional information regarding ports.) See Figure 3-29 for more details.

|  |  |  |
| --- | --- | --- |
| 0 8 16 31   |  | | --- | | unused (zero) | | IP header - 64 bits of original data of the datagram | |

*Figure 3-29 ICMP: Destination Unreachable*

The ICMP header code field contains one of the following values:

1. Network unreachable
2. Host unreachable
3. Protocol unreachable
4. Port unreachable
5. Fragmentation needed but the Do Not Fragment bit was set
6. Source route failed
7. Destination network unknown
8. Destination host unknown
9. Source host isolated (obsolete)
10. Destination network administratively prohibited
11. Destination host administratively prohibited
12. Network unreachable for this type of service
13. Host unreachable for this type of service
14. Communication administratively prohibited by filtering
15. Host precedence violation
16. Precedence cutoff in effect

These are detailed in RFC 792, RFC 1812 updated by RFC 2644, RFC 1122, updated by RFC 4379, and forms part of STD 3 – Host Requirements.

If a router implements the Path MTU Discovery protocol, the format of the destination unreachable message is changed for code 4. This includes the MTU of the link that did not accept the datagram. See Figure 3-30 for more information.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 0 8 16 31   |  |  | | --- | --- | | unused (zero) | link MTU | | IP header - 64 bits of original data of the datagram | | |

*Figure 3-30 ICMP: Fragmentation required with link MTU*

##### Source Quench (4)

If this message is received from an intermediate router, it means that the router did not have the buffer space needed to queue the datagram.

If this message is received from the destination host, it means that the incoming datagrams are arriving too quickly to be processed.

The ICMP header code field is always zero.

See Figure 3-31 for more details.

|  |  |  |
| --- | --- | --- |
| 0 8 16 31   |  | | --- | | unused (zero) | | IP header - 64 bits of original data of the datagram | |

*Figure 3-31 ICMP: Source Quench*

##### Redirect (5)

If this message is received from an intermediate router, it means that the host should send future datagrams for the network to the router whose IP address is specified in the ICMP message. This preferred router will always be on the same subnet as the host that sent the datagram and the router that returned the IP datagram. The router forwards the datagram to its next hop destination. This message will not be sent if the IP datagram contains a source route.

The ICMP header code field will have one of the following values:

1. Network redirect
2. Host redirect
3. Network redirect for this type of service **3** Host redirect for this type of service See Figure 3-32 for more details.

|  |  |  |
| --- | --- | --- |
| 0 8 16 31   |  | | --- | | router IP address | | IP header - 64 bits of original data of the datagram | |

*Figure 3-32 ICMP: Redirect*

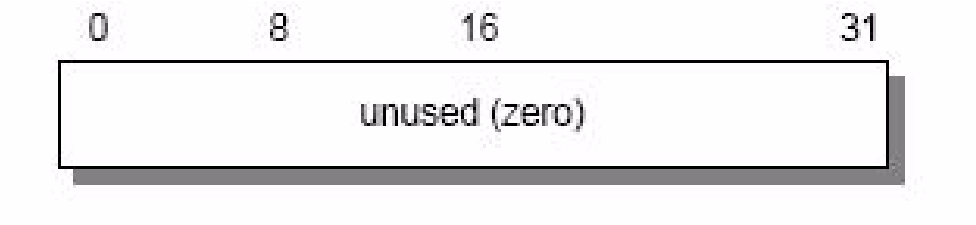
##### Router Advertisement (9) and Router Solicitation (10)

ICMP messages 9 and 10 are optional. They are described in RFC 1256, which is elective. See Figure 3-33 and Figure 3-34 on page 114 for details.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 0 8 16 31 | | | | | | | |
|  |  | |  |  | |  | |
|  | number | entry length | TTL | |  |  |
|  |  | | | |
| router address 1 | | | |  |
|  |  | | | |
| preference level 1 | | | |  |
|  |  | | | |
|  | | | |  |
| / | / |  | | | / | / |
|  |  |  |  |
|  | | | | |
|  | router address n | | | |  |
|  | preference level n | | | |
|  |  | | | |
|  | | | | |

*Figure 3-33 ICMP: Router Advertisement*

*Figure 3-34 ICMP: Router Solicitation*



Where:

|  |  |
| --- | --- |
| **Number** | The number of entries in the message. |
| **Entry length** | The length of an entry in 32-bit units. This is 2 (32 bits for the IP address and 32 bits for the preference value). |
| **TTL** | The number of seconds that an entry will be considered valid. |
| **Router address** | One of the sender's IP addresses. |
| **Preference level** | A signed 32-bit level indicating the preference to be assigned to this address when selecting a default router. Each router on a subnet is responsible for advertising its own preference level. Larger values imply higher preference; smaller values imply lower. The default is zero, which is in the middle of the possible range. A value of X'80000000' (-231) indicates the router should never be used as a default router. |

The ICMP header code field is zero for both of these messages.

These two messages are used if a host or a router supports the router discovery protocol. Routers periodically advertise their IP addresses on those subnets where they are configured to do so. Advertisements are made on the all-systems multicast address (224.0.0.1) or the limited broadcast address

(255.255.255.255). The default behavior is to send advertisements every 10 minutes with a TTL value of 1800 (30 minutes). Routers also reply to solicitation messages they receive. They might reply directly to the soliciting host, or they might wait a short random interval and reply with a multicast.

Hosts can send solicitation messages. Solicitation messages are sent to the all-routers multicast address (224.0.0.2) or the limited broadcast address (255.255.255.255). Typically, three solicitation messages are sent at 3-second intervals. Alternatively, a host can wait for periodic advertisements. Each time a host receives an advertisement with a higher preference value, it updates its default router. The host also sets the TTL timer for the new entry to match the value in the advertisement. When the host receives a new advertisement for its current default router, it resets the TTL value to that in the new advertisement.

This process also provides a mechanism for routers to declare themselves unavailable. They send an advertisement with a TTL value of zero.

##### Time Exceeded (11)

If this message is received from an intermediate router, it means that the time to live field of an IP datagram has expired.

If this message is received from the destination host, it means that the IP fragment reassembly time to live timer has expired while the host is waiting for a fragment of the datagram. The ICMP header code field can have the one of the following values:

1. Transit TTL exceeded
2. Reassembly TTL exceeded

See Figure 3-35 for more details.

|  |  |  |
| --- | --- | --- |
| 0 8 16 31   |  | | --- | | unused (zero) | | IP header - 64 bits of original data of the datagram | |

*Figure 3-35 ICMP: Time Exceeded*

##### Parameter Problem (12)

This message indicates that a problem was encountered during processing of the IP header parameters. The pointer field indicates the octet in the original IP datagram where the problem was encountered. The ICMP header code field can have the one of the following values:

1. Unspecified error
2. Required option missing

See Figure 3-36 for more details.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 0 8 16 31   |  |  | | --- | --- | | pointer | unused (zero) | | IP header - 64 bits of original data of the datagram | | |

*Figure 3-36 ICMP: Parameter Problem*

##### Timestamp Request (13) and Timestamp Reply (14)

These two messages are for debugging and performance measurements. They are not used for clock synchronization.

The sender initializes the identifier and sequence number (which is used if multiple time stamp requests are sent), sets the originate time stamp, and sends the datagram to the recipient. The receiving host fills in the receive and transmit time stamps, changes the type to time stamp reply, and returns it to the original sender. The datagram has two time stamps if there is a perceptible time difference between the receipt and transmit times. In practice, most implementations perform the two (receipt and reply) in one operation. This sets the two time stamps to the same value. Time stamps are the number of milliseconds elapsed since midnight UT (GMT).

See Figure 3-37 for details.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 8 16 31   |  |  | | --- | --- | | identifier | sequence number | | originate timestamp | | | receive timestamp | | | transmit timestamp | | |

*Figure 3-37 ICMP: Timestamp Request and Timestamp Reply*

##### Address Mask Request (17) and Address Mask Reply (18)

An address mask request is used by a host to determine the subnet mask used on an attached network. Most hosts are configured with their subnet mask or masks. However some, such as diskless workstations, must obtain this information from a server. A host uses RARP (see 3.5, “Reverse Address Resolution Protocol (RARP)” on page 124) to obtain its IP address. To obtain a subnet mask, the host broadcasts an address mask request. Any host in the network that has been configured to send address mask replies will fill in the subnet mask, convert the packet to an address mask reply, and return it to the sender. The ICMP header code field is zero.

See Figure 3-38 on page 117 for more details.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 0 8 16 31   |  |  | | --- | --- | | identifier | sequence number | | subnet address mask | | |

*Figure 3-38 ICMP: Address Mask Request and Reply*

#### 3.2.2 ICMP applications

There are two simple and widely used applications based on ICMP: Ping and Traceroute. Ping uses the ICMP Echo and Echo Reply messages to determine whether a host is reachable. Traceroute sends IP datagrams with low TTL values so that they expire en route to a destination. It uses the resulting ICMP Time Exceeded messages to determine where in the internet the datagrams expired and pieces together a view of the route to a host. We discuss these applications in the following sections.

##### Ping

Ping is the simplest of all TCP/IP applications. It sends IP datagrams to a specified destination host and measures the round trip time to receive a response. The word *ping*, which is used as a noun and a verb, is taken from the sonar operation to locate an underwater object. It is also an abbreviation for *Packet InterNet Groper*.

Generally, the first test of reachability for a host is to attempt to ping it. If you can successfully ping a host, other applications such as Telnet or FTP should be able to reach that host. However with the advent of security measures on the Internet, particularly firewalls (see 22.3, “Firewalls” on page 794), which control access to networks by application protocol or port number, or both, this is no longer necessarily true. The ICMP protocol can be restricted on the firewall and therefore the host is unable to be successfully pinged.

The syntax that is used in different implementations of ping varies from platform to platform. A common format for using the ping command is: ping host

Where host is the destination, either a symbolic name or an IP address.

Most platforms allow you to specify the following values:

|  |  |
| --- | --- |
| **Size** | The size of the data portion of the packet. |
| **Packets** | The number of packets to send. |
| **Count** | The number of echo requests to send. |
| **Record routes** | Record the route per count hop. | |
| **Time stamp** | Time stamp each count hop. | |
| **Endless ping** | Ping until manually stopped. | |
| **Resolve address** | Resolve the host address to the host name. | |
| **Time to Live (TTL)** | The time (in seconds) the datagram is allowed to travel. | |

**Type of Service (TOS)** The type of internet service quality.

**Host-list** Loose source route or strict source route of host lists.

**Timeout** The timeout to wait for each reply. **No fragmentation** The fragment flag is not set.

Ping uses the ICMP Echo and Echo Reply messages (refer to “Echo (8) and Echo Reply (0)” on page 111). Because ICMP is required in every TCP/IP implementation, hosts do not require a separate server to respond to ping requests.

Ping is useful for verifying an IP installation. The following variations of the command each require the operation of an different portion of an IP installation:

ping loopback: Verifies the operation of the base TCP/IP software.

ping my-IP-address: Verifies whether the physical network device can be addressed.

ping a-remote-IP-address: Verifies whether the network can be accessed.

ping a-remote-host-name: Verifies the operation of the name server (or the flat namespace resolver, depending on the installation).

##### Traceroute

The Traceroute program is used to determine the route IP datagrams follow through the network.

Traceroute is based on ICMP and UDP. It sends an IP datagram with a TTL of 1 to the destination host. The first router decrements the TTL to 0, discards the datagram, and returns an ICMP Time Exceeded message to the source. In this way, the first router in the path is identified. This process is repeated with successively larger TTL values to identify the exact series of routers in the path to the destination host.

Traceroute sends UDP datagrams to the destination host. These datagrams reference a port number outside the standard range. When an ICMP Port Unreachable message is received, the source determines the destination host has been reached.

### 3.3 Internet Group Management Protocol (IGMP)

IGMP is a standard protocol with STD number 5. That standard also includes IP (see 3.1, “Internet Protocol (IP)” on page 68) and ICMP (see 3.2, “Internet

Control Message Protocol (ICMP)” on page 109). Its status is recommended. It is described in RFC 1112 with updates in RFC 2236.

Similar to ICMP, the Internet Group Management Protocol (IGMP) is also an integral part of IP. It allows hosts to participate in IP multicasts. IGMP further provides routers with the capability to check if any hosts on a local subnet are interested in a particular multicast.

Refer to 6.2, “Internet Group Management Protocol (IGMP)” on page 241 for a detailed review of IGMP.

### 3.4 Address Resolution Protocol (ARP)

Address Resolution Protocol (ARP) is a network-specific standard protocol. The address resolution protocol is responsible for converting the higher-level protocol addresses (IP addresses) to physical network addresses. It is described in

RFC 826.

#### 3.4.1 ARP overview

On a single physical network, individual hosts are known in the network by their physical hardware address. Higher-level protocols address destination hosts in the form of a symbolic address (IP address in this case). When such a protocol wants to send a datagram to destination IP address w.x.y.z, the device driver does not understand this address.

Therefore, a module (ARP) is provided that will translate the IP address to the physical address of the destination host. It uses a lookup table (sometimes referred to as the *ARP cache*) to perform this translation.

When the address is not found in the ARP cache, a broadcast is sent out in the network with a special format called the *ARP request*. If one of the machines in the network recognizes its own IP address in the request, it will send an *ARP reply* back to the requesting host. The reply will contain the physical hardware address of the host and source route information (if the packet has crossed bridges on its path). Both this address and the source route information are stored in the ARP cache of the requesting host. All subsequent datagrams to this destination IP address can now be translated to a physical address, which is used by the device driver to send out the datagram in the network.

An exception to the rule is the asynchronous transfer mode (ATM) technology, where ARP cannot be implemented in the physical layer as described previously. Therefore, every host, upon initialization, must register with an ARP server in order to be able to resolve IP addresses to hardware addresses (also see 2.10, “Asynchronous transfer mode (ATM)” on page 47).

ARP was designed to be used on networks that support hardware broadcast.

This means, for example, that ARP will not work on an X.25 network.

#### 3.4.2 ARP detailed concept

ARP is used on IEEE 802 networks as well as on the older DIX Ethernet networks to map IP addresses to physical hardware addresses (see 2.1, “Ethernet and IEEE 802 local area networks (LANs)” on page 30). To do this, it is closely related to the device driver for that network. In fact, the ARP specifications in RFC 826 only describe its functionality, not its implementation. The implementation depends to a large extent on the device driver for a network type and they are usually coded together in the *adapter microcode*.

##### ARP packet generation

If an application wants to send data to a certain IP destination address, the IP routing mechanism first determines the IP address of the next hop of the packet (it can be the destination host itself, or a router) and the hardware device on which it should be sent. If it is an IEEE 802.3/4/5 network, the ARP module must be consulted to map the <protocol type, target protocol address> to a physical address.

The ARP module tries to find the address in this ARP cache. If it finds the matching pair, it gives the corresponding 48-bit physical address back to the caller (the device driver), which then transmits the packet. If it does not find the pair in its table, it *discards the packet* (the assumption is that a higher-level protocol will retransmit) and generates a network *broadcast* of an ARP request. See Figure 3-39 on page 121 for more details.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | |  |  | physical layer header | | | A  R  P  P a c k e t | hardware address space | | | | Protocol address space | | | | hardware address byte length (n) | | Protocol address byte length (m) | | operation code | | | | hardware address of sender | | | | protocol address of sender | | | | hardware address of target | | | | protocol address of target | | |   x bytes  2 bytes  2 bytes 2bytes  2 bytes n bytes m bytes n bytes  m bytes |

*Figure 3-39 ARP: Request/reply packet*

Where:

Hardware address space: Specifies the type of hardware; examples are Ethernet or Packet Radio Net.

Protocol address space: Specifies the type of protocol, same as the EtherType field in the IEEE 802 header (IP or ARP).

Hardware address length: Specifies the length (in bytes) of the hardware addresses in this packet. For IEEE 802.3 and IEEE 802.5, this is 6.

Protocol address length: Specifies the length (in bytes) of the protocol addresses in this packet. For IP, this is 4.

Operation code: Specifies whether this is an ARP request (1) or reply (2).

Source/target hardware address: Contains the physical network hardware addresses. For IEEE 802.3, these are 48-bit addresses.

Source/target protocol address: Contains the protocol addresses. For TCP/IP, these are the 32-bit IP addresses.

For the ARP request packet, the target hardware address is the only undefined field in the packet.

##### ARP packet reception

When a host receives an ARP packet (either a broadcast request or a point-to-point reply), the receiving device driver passes the packet to the ARP module, which treats it as shown in Figure 3-40.

Yes

Yes

Yes

Yes

Yes

Yes

No

(

discard

)

Do I have the specified

hardware type?

No

(

discard

)

No

No

)

discard

(

No

No

(

discard

)

End

Do I speak the specified

protocol?

Is the pair <protocol type,

sender protocol address>

already in my table?

Am I the target protocol

address?

Is flag = false?

Is the opcode a request?

Add the triplet <protocol

type, sender protocol and

sender hardware> to

table.

Set flag = false.

Update the table with the

sender hardware address.

Set flag=true.

Swap source and target

addressesin the ARP

packet. Put my local

addresses in the source

address fields. Send back

ARP packet as an ARP

reply to the requesting

host.

*Figure 3-40 ARP: Packet reception*

The requesting host will receive this ARP reply, and will follow the same algorithm to treat it. As a result of this, the triplet <protocol type, protocol address, hardware address> for the desired host will be added to its lookup table (ARP cache). The next time a higher-level protocol wants to send a packet to that host, the ARP module will find the target hardware address and the packet will be sent to that host.

Note that because the original ARP request was a broadcast in the network, all hosts on that network will have updated the sender's hardware address in their table (only if it was already in the table).

#### 3.4.3 ARP and subnets

The ARP protocol remains unchanged in the presence of subnets. Remember that each IP datagram first goes through the IP routing algorithm. This algorithm selects the hardware device driver that should send out the packet. Only then, the ARP module associated with that device driver is consulted.

#### 3.4.4 Proxy-ARP or transparent subnetting

Proxy-ARP is described in RFC 1027, which is a subset of the method proposed in RFC 925. It is another method to construct local subnets, without the need for a modification to the IP routing algorithm, but with modifications to the routers that interconnect the subnets.

##### Proxy-ARP concept

Consider one IP network that is divided into subnets and interconnected by routers. We use the “old” IP routing algorithm, which means that no host knows about the existence of multiple physical networks. Consider hosts A and B, which are on different physical networks within the same IP network, and a router R between the two subnetworks as illustrated in Figure 3-41.

A

R

B

*Figure 3-41 ARP: Hosts interconnected by a router*

When host A wants to send an IP datagram to host B, it first has to determine the physical network address of host B through the use of the ARP protocol.

Because host A cannot differentiate between the physical networks, its IP routing algorithm thinks that host B is on the local physical network and sends out a broadcast ARP request. Host B does not receive this broadcast, but router R does. Router R understands subnets, that is, it runs the subnet version of the IP routing algorithm and it will be able to see that the destination of the ARP request (from the target protocol address field) is on another physical network. If router R's routing tables specify that the next hop to that other network is through a different physical device, it will reply to the ARP as though it were host B, saying that the network address of host B is that of the router R itself.

Host A receives this ARP reply, puts it in its cache, and will send future IP packets for host B to the router R. The router will forward such packets to the correct subnet.

The result is transparent subnetting:

Normal hosts (such as A and B) do not know about subnetting, so they use the “old” IP routing algorithm.

The routers between subnets have to:

* Use the subnet IP routing algorithm.
* Use a modified ARP module, which can reply on behalf of other hosts.

See Figure 3-42 for more details.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | | |  | | |  | |
|  | A |  |
|  |
| "o ld " IP ro u tin g |  | B |
|  |
|  |  |  |  |
|  | R |  |
| IP s u b n e t ro u tin g a n d m o d ifie d A R P |

*Figure 3-42 ARP: Proxy-ARP router*

### 3.5 Reverse Address Resolution Protocol (RARP)

Reverse Address Resolution Protocol (RARP) is a network-specific standard protocol. It is described in RFC 903.

Some network hosts, such as diskless workstations, do not know their own IP address when they are booted. To determine their own IP address, they use a mechanism similar to ARP, but now the hardware address of the host is the known parameter and the IP address the queried parameter. It differs more fundamentally from ARP in the fact that a RARP server must exist in the network that maintains that a database of mappings from hardware address to protocol address must be preconfigured.

#### 3.5.1 RARP concept

The reverse address resolution is performed the same way as the ARP address

resolution. The same packet format (see Figure 3-39 on page 121) is used as for

ARP.

An exception is the operation code field that now takes the following values:

1. For the RARP request
2. For the RARP reply

And of course, the physical header of the frame will now indicate RARP as the higher-level protocol (8035 hex) instead of ARP (0806 hex) or IP (0800 hex) in the EtherType field.

Some differences arise from the concept of RARP itself:

ARP only assumes that every host knows the mapping between its own hardware address and protocol address. RARP requires one or more server hosts in the network to maintain a database of mappings between hardware addresses and protocol addresses so that they will be able to reply to requests from client hosts.

Due to the size this database can take, part of the server function is usually implemented outside the adapter's microcode, with optionally a small cache in the microcode. The microcode part is then only responsible for reception and transmission of the RARP frames, the RARP mapping itself being taken care of by server software running as a normal process on the host machine.

The nature of this database also requires some software to create and update the database manually.

If there are multiple RARP servers in the network, the RARP requester only uses the first RARP reply received on its broadcast RARP request and discards the others.

### 3.6 Bootstrap Protocol (BOOTP)

The Bootstrap Protocol (BOOTP) enables a client workstation to initialize with a minimal IP stack and request its IP address, a gateway address, and the address of a name server from a BOOTP server. If BOOTP is to be used in your network, the server and client are usually on the same physical LAN segment. BOOTP can only be used across bridged segments when source-routing bridges are being used, or across subnets, if you have a router capable of BOOTP forwarding.

BOOTP is a draft standard protocol. Its status is recommended. The BOOTP specifications are in RFC 951, which has been updated by RFC1542 and RFC 2132.

There are also updates to BOOTP, some relating to interoperability with DHCP (see 3.7, “Dynamic Host Configuration Protocol (DHCP)” on page 130), described in RFC 1542, which updates RFC 951 and RFC 2132. The updates to BOOTP are draft standards with a status of elective and recommended, respectively.

The BOOTP protocol was originally developed as a mechanism to enable diskless hosts to be remotely booted over a network as workstations, routers, terminal concentrators, and so on. It allows a minimum IP protocol stack with no configuration information to obtain enough information to begin the process of downloading the necessary boot code. BOOTP does not define how the downloading is done, but this process typically uses TFTP (see also 14.2, “Trivial File Transfer Protocol (TFTP)” on page 529), as described in RFC 906. Although still widely used for this purpose by diskless hosts, BOOTP is also commonly used solely as a mechanism to deliver configuration information to a client that has not been manually configured.

The BOOTP process involves the following steps:

1. The client determines its own hardware address; this is normally in a ROM on the hardware.
2. A BOOTP client sends its hardware address in a UDP datagram to the server. Figure 3-43 on page 127 shows the full contents of this datagram. If the client knows its IP address or the address of the server, it should use them, but in general, BOOTP clients have no IP configuration data at all. If the client does not know its own IP address, it uses 0.0.0.0. If the client does not know the server's IP address, it uses the limited broadcast address (255.255.255.255). The UDP port number is 67.
3. The server receives the datagram and looks up the hardware address of the client in its configuration file, which contains the client's IP address. The server fills in the remaining fields in the UDP datagram and returns it to the client using UDP port 68. One of three methods can be used to do this:
   * If the client knows its own IP address (it was included in the BOOTP request), the server returns the datagram directly to this address. It is likely that the ARP cache in the server's protocol stack will not know the

hardware address matching the IP address. ARP will be used to determine it as normal.

* + If the client does not know its own IP address (it was 0.0.0.0 in the BOOTP request), the server must concern itself with its own ARP cache.
  + ARP on the server cannot be used to find the hardware address of the client because the client does not know its IP address and so cannot reply to an ARP request. This is called the “chicken and egg” problem. There are two possible solutions:
    - If the server has a mechanism for directly updating its own ARP cache without using ARP itself, it does so and then sends the datagram directly.
    - If the server cannot update its own ARP cache, it must send a broadcast reply.

1. When it receives the reply, the BOOTP client will record its own IP address (allowing it to respond to ARP requests) and begin the bootstrap process.

Figure 3-43 gives an overview of the BOOTP message format.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 8 16 24 31   |  |  |  |  |  | | --- | --- | --- | --- | --- | | code |  | H/W type | length | hops | |  |  | transaction ID | |  | | seconds | |  | flags | field | |  | | client IP address | |  | |  | | your IP address | |  | |  | | server IP address | |  | |  | | router IP address | |  | |  | | client hardware address (16 bytes) | |  | |  | | server host name (64 bytes) | |  | |  | | boot file name (128 bytes) | |  | |  | | vendor-specific area (64 bytes) | |  | |

*Figure 3-43 BOOTP message format* Where:

|  |  |
| --- | --- |
| **Code** | Indicates a request or a reply:   1. Request 2. Reply |
| **H/W type** | The type of hardware, for example: |

**1** Ethernet

**6** IEEE 802 Networks

Refer to STD 2 – Assigned Internet Numbers for a complete list.

|  |  |
| --- | --- |
| **Length** | Hardware address length in bytes. Ethernet and token ring both use 6, for example. |
| **Hops** | The client sets this to 0.  It is incremented by a router that relays the request to another server and is used to identify loops. RFC 951 suggests that a value of 3 indicates a loop. |
| **Transaction ID** | A random number used to match this boot request with the response it generates. |
| **Seconds** | Set by the client. It is the elapsed time in seconds since the client started its boot process. |
| **Flags field** | The most significant bit of the flags field is used as a broadcast flag. All other bits must be set to zero; they are reserved for future use. Normally, BOOTP servers attempt to deliver BOOTREPLY messages directly to a client using unicast delivery. The destination address in the IP header is set to the BOOTP *your IP address* and the MAC address is set to the BOOTP *client hardware address*. If a host is unable to receive a unicast IP datagram until it knows its IP address, this broadcast bit must be set to indicate to the server that the BOOTREPLY must be sent as an IP and MAC broadcast. Otherwise, this bit must be set to zero. |
| **Client IP address** | Set by the client, either to its known IP address or 0.0.0.0. |
| **Your IP address** | Set by the server if the client IP address field was 0.0.0.0. |
| **Server IP address** | Set by the server. |
| **Router IP address** | This is the address of a BOOTP relay agent, *not* a general IP router to be used by the client. It is set by the forwarding agent when BOOTP forwarding is used (see 3.6.1, “BOOTP forwarding” on page 129). |

#### Client hardware address

Set by the client and used by the server to identify which registered client is booting.

|  |  |
| --- | --- |
| **Server host name** | Optional server host name terminated by X'00'. |
| **Boot file name** | The client either leaves this null or specifies a generic name, such as router indicating the type of boot file to be used. The server returns the fully qualified file name of a boot file suitable for the client. The value is terminated by X'00'. |

**Vendor-specific area** Optional vendor-specific area. Clients should always fill the first four bytes with a “magic cookie.” If a vendor-specific magic cookie is not used, the client should use 99.130.83.99 followed by an end tag (255) and set the remaining bytes to zero. The vendor-specific area can also contain *BOOTP Vendor extensions*. These are options that can be passed to the client at boot time along with its IP address. For example, the client can also receive the address of a default router, the address of a domain name server, and a subnet mask. BOOTP shares the same options as DHCP, with the exception of several DHCP-specific options. See RFC 2132 for full details.

After the BOOTP client has processed the reply, it can proceed with the transfer of the boot file and execute the full boot process. See RFC 906 for the specification of how this is done with TFTP. In the case of a diskless host, the full boot process will normally replace the minimal IP protocol stack, loaded from ROM, and used by BOOTP and TFTP, with a normal IP protocol stack transferred as part of the boot file and containing the correct customization for the client.

#### 3.6.1 BOOTP forwarding

The BOOTP client uses the limited broadcast address for BOOTP requests, which requires the BOOTP server to be on the same subnet as the client. BOOTP forwarding is a mechanism for routers to forward BOOTP requests across subnets. It is a configuration option available on most routers. The router configured to forward BOOTP requests is known as a *BOOTP relay agent*.

A router will normally discard any datagrams containing illegal source addresses, such as 0.0.0.0, which is used by a BOOTP client. A router will also generally discard datagrams with the limited broadcast destination address. However, a

BOOTP relay agent will accept such datagrams from BOOTP clients on port 67.

The process carried out by a BOOTP relay agent on receiving a BOOTPREQUEST is as follows:

1. When the BOOTP relay agent receives a BOOTPREQUEST, it first checks the hops field to check the number of hops already completed in order to decide whether to forward the request. The threshold for the allowable number of hops is normally configurable.

1. If the relay agent decides to relay the request, it checks the contents of the router IP address field. If this field is zero, it fills this field with the IP address of the interface on which the BOOTPREQUEST was received. If this field already has an IP address of another relay agent, it is not touched.
2. The value of the hops field is incremented.
3. The relay agent then forwards the BOOTPREQUEST to one or more BOOTP servers. The address of the BOOTP server or servers is preconfigured at the relay agent. The BOOTPREQUEST is normally forwarded as a unicast frame, although some implementations use broadcast forwarding.
4. When the BOOTP server receives the BOOTPREQUEST with the non-zero router IP address field, it sends an IP unicast BOOTREPLY to the BOOTP relay agent at the address in this field on port 67.
5. When the BOOTP relay agent receives the BOOTREPLY, the H/W type, length, and client hardware address fields in the message supply sufficient link layer information to return the reply to the client. The relay agent checks the broadcast flag. If this flag is set, the agent forwards the BOOTPREPLY to the client as a broadcast. If the broadcast flag is not set, the relay agent sends a reply as a unicast to the address specified in your IP address.

When a router is configured as a BOOTP relay agent, the BOOTP forwarding task is considerably different from the task of switching datagrams between subnets normally carried out by a router. Forwarding of BOOTP messages can be considered to be receiving BOOTP messages as a final destination, and then generating new BOOTP messages to be forwarded to another destination.

#### 3.6.2 BOOTP considerations

The use of BOOTP allows centralized configuration of multiple clients. However, it requires a static table to be maintained with an IP address preallocated for every client that is likely to attach to the BOOTP server, even if the client is seldom active. This means that there is no relief on the number of IP addresses required. There is a measure of security in an environment using BOOTP, because a client will only be allocated an IP address by the server if it has a valid MAC address.

### 3.7 Dynamic Host Configuration Protocol (DHCP)

DHCP is a draft standard protocol. Its status is elective. The current DHCP specifications are in RFC 2131 with updates in RFC 3396 and RFC 4361. The specifications are also in RFC 2132 with updates in RFC3442, RFC3942, and RFC4361.

The Dynamic Host Configuration Protocol (DHCP) provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the BOOTP protocol, adding the capability of automatic allocation of reusable network addresses and additional configuration options. For information regarding BOOTP, refer to 3.6, “Bootstrap Protocol (BOOTP)” on page 125. DHCP messages use UDP port 67, the BOOTP server's well-known port and UDP port 68, the BOOTP client's well-known port. DHCP participants can interoperate with BOOTP participants. See 3.7.8, “BOOTP and DHCP interoperability” on page 140 for further details.

DHCP consists of two components:

A protocol that delivers host-specific configuration parameters from a DHCP server to a host

A mechanism for the allocation of temporary or permanent network addresses to hosts

IP requires the setting of many parameters within the protocol implementation software. Because IP can be used on many dissimilar kinds of network hardware, values for those parameters cannot be guessed at or assumed to have correct defaults. The use of a distributed address allocation scheme based on a polling/defense mechanism, for discovery of network addresses already in use, cannot guarantee unique network addresses because hosts might not always be able to defend their network addresses.

DHCP supports three mechanisms for IP address allocation:

Automatic allocation

DHCP assigns a permanent IP address to the host.

Dynamic allocation

DHCP assigns an IP address for a limited period of time. Such a network address is called a *lease*. This is the only mechanism that allows automatic reuse of addresses that are no longer needed by the host to which it was assigned.

Manual allocation

The host's address is assigned by a network administrator.

#### 3.7.1 The DHCP message format

The format of a DHCP message is shown in Figure 3-44.

*Figure 3-44 DHCP message format*

code

length

31

0

8 16 24

HWtype

hops

ction ID

transa

client IP address

your IP address

server IP address

seconds

flags field

router IP address

client hardware address

(16

bytes

)

server host name

(64

bytes

)

boot file name

(128

bytes

)

options

(312

bytes

)

Where:

|  |  |
| --- | --- |
| **Code** | Indicates a request or a reply:   1. Request 2. Reply |
| **HWtype** | The type of hardware, for example:  **1** Ethernet |
| **Length** | **6** IEEE 802 Networks    Refer to STD 2 – Assigned Internet Numbers for a complete list.  Hardware address length in bytes. |
| **Hops** | The client sets this to 0. It is incremented by a router that relays the request to another server and is used to identify loops. RFC 951 suggests that a value of 3 indicates a loop. | |
| **Transaction ID** | A random number used to match this boot request with the response it generates. | |
| **Seconds** | Set by the client. It is the elapsed time in seconds since the client started its boot process. | |
| **Flags field** | The most significant bit of the flags field is used as a broadcast flag. All other bits must be set to zero, and are reserved for future use. Normally, DHCP servers attempt to deliver DHCP messages directly to a client using unicast delivery. The destination address in the IP header is set to the DHCP *your IP address* and the MAC address is set to the DHCP *client hardware address*. If a host is unable to receive a unicast IP datagram until it knows its IP address, this broadcast bit must be set to indicate to the server that the DHCP reply must be sent as an IP and MAC broadcast.  Otherwise, this bit must be set to zero. | |
| **Client IP address** | Set by the client. Either its known IP address, or 0.0.0.0. | |
| **Your IP address** | Set by the server if the client IP address field was 0.0.0.0. | |
| **Server IP address** | Set by the server. | |
| **Router IP address** | This is the address of a BOOTP relay agent, *not* a general IP router to be used by the client. It is set by the forwarding agent when BOOTP forwarding is used (see 3.6.1, “BOOTP forwarding” on page 129). | |

##### Client hardware address

Set by the client. DHCP defines a client identifier option that is used for client identification. If this option is not used, the client is identified by its MAC address.

|  |  |
| --- | --- |
| **Server host name** | Optional server host name terminated by X'00'. |
| **Boot file name** | The client either leaves this null or specifies a generic name, such as router, indicating the type of boot file to be used. In a DHCPDISCOVER request, this is set to  null. The server returns a fully qualified directory path name in a DHCPOFFER request. The value is terminated by X'00'. |

**Options** The first four bytes of the options field of the DHCP

message contain the magic cookie (99.130.83.99). The remainder of the options field consists of tagged parameters that are called *options*. See RFC 2132, with updates in RFC3942, for details.

#### 3.7.2 DHCP message types

DHCP messages fall into one of the following categories:

DHCPDISCOVER: Broadcast by a client to find available DHCP servers.

DHCPOFFER: Response from a server to a DHCPDISCOVER and offering IP address and other parameters.

DHCPREQUEST: Message from a client to servers that does one of the following:

* Requests the parameters offered by one of the servers and declines all other offers.
* Verifies a previously allocated address after a system or network change (a reboot for example).
* Requests the extension of a lease on a particular address.

DHCPACK: Acknowledgement from server to client with parameters, including IP address.

DHCPNACK: Negative acknowledgement from server to client, indicating that the client's lease has expired or that a requested IP address is incorrect.

DHCPDECLINE: Message from client to server indicating that the offered address is already in use.

DHCPRELEASE: Message from client to server cancelling remainder of a lease and relinquishing network address.

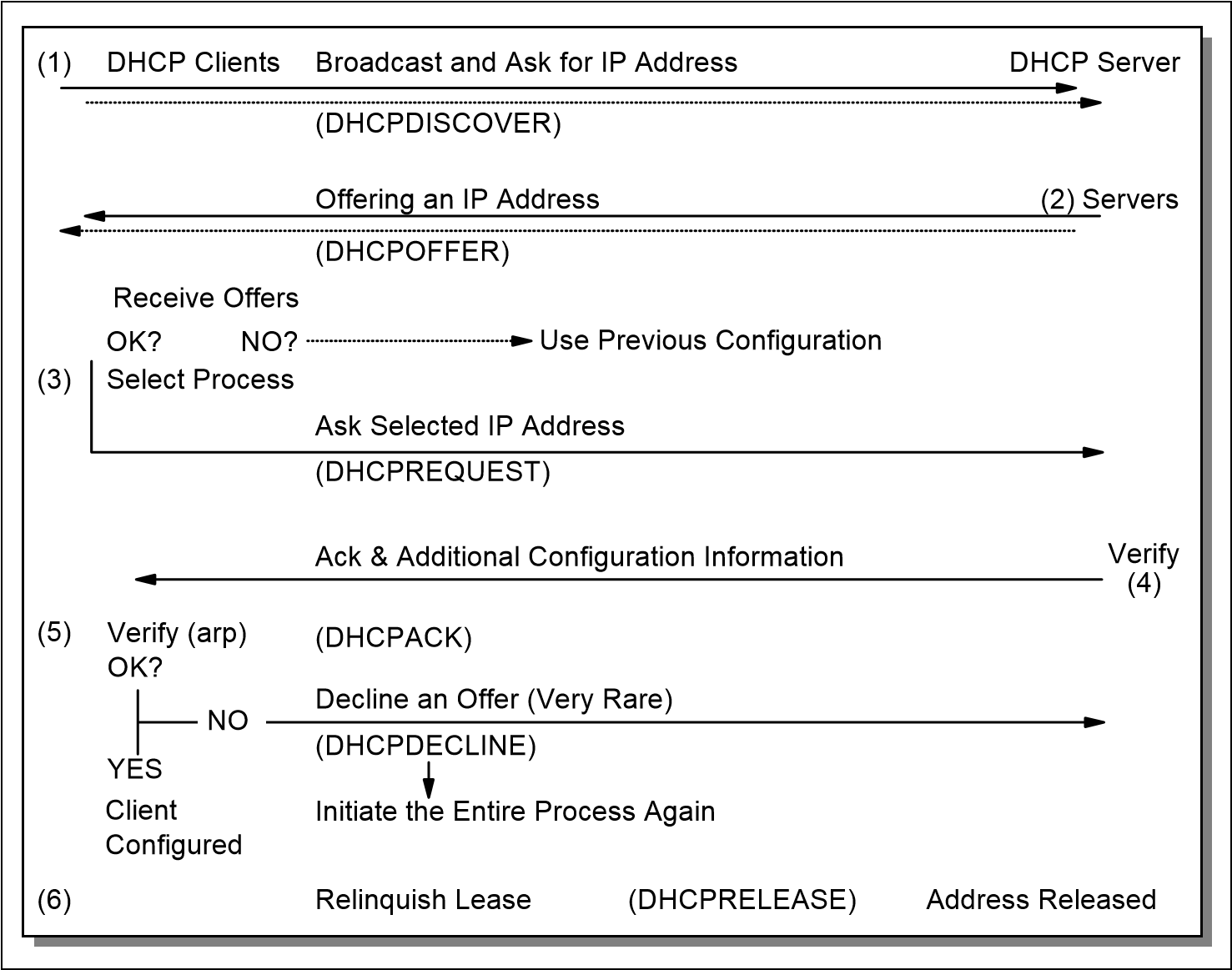
DHCPINFORM: Message from a client that already has an IP address (manually configured, for example), requesting further configuration parameters from the DHCP server.

#### 3.7.3 Allocating a new network address

This section describes the client/server interaction if the client does not know its network address. Assume that the DHCP server has a block of network

addresses from which it can satisfy requests for new addresses. Each server also maintains a database of allocated addresses and leases in permanent local storage.

The DHCP client/server interaction steps are illustrated in Figure 3-45.



*Figure 3-45 DHCP client and DHCP server interaction*

The following procedure describes the DHCP client/server interaction steps illustrated in Figure 3-45:

1. The client broadcasts a DHCPDISCOVER message on its local physical subnet. At this point, the client is in the INIT state. The DHCPDISCOVER message might include some options such as network address suggestion or lease duration.
2. Each server responds with a DHCPOFFER message that includes an available network address (your IP address) and other configuration options. The servers record the address as offered to the client to prevent the same address being offered to other clients in the event of further

DHCPDISCOVER messages being received before the first client has

completed its configuration.

1. The client receives one or more DHCPOFFER messages from one or more servers. The client chooses one based on the configuration parameters offered and broadcasts a DHCPREQUEST message that includes the server identifier option to indicate which message it has selected and the requested IP address option taken from your IP address in the selected offer.
2. In the event that no offers are received, if the client has knowledge of a previous network address, the client can reuse that address if its lease is still valid until the lease expires.
3. The servers receive the DHCPREQUEST broadcast from the client. Those servers not selected by the DHCPREQUEST message use the message as

notification that the client has declined that server's offer. The server selected in the DHCPREQUEST message commits the binding for the client to persistent storage and responds with a DHCPACK message containing the configuration parameters for the requesting client. The combination of client hardware and assigned network address constitute a unique identifier for the client's lease and are used by both the client and server to identify a lease referred to in any DHCP messages. The your IP address field in the DHCPACK messages is filled in with the selected network address.

1. The client receives the DHCPACK message with configuration parameters. The client performs a final check on the parameters, for example, with ARP for allocated network address, and notes the duration of the lease and the lease identification cookie specified in the DHCPACK message. At this point, the client is configured.
2. If the client detects a problem with the parameters in the DHCPACK message (the address is already in use in the network, for example), the client sends a DHCPDECLINE message to the server and restarts the configuration process. The client should wait a minimum of ten seconds before restarting the configuration process to avoid excessive network traffic in case of looping. On receipt of a DHCPDECLINE, the server must mark the offered address as unavailable (and possibly inform the system administrator that there is a configuration problem).
3. If the client receives a DHCPNAK message, the client restarts the configuration process.
4. The client may choose to relinquish its lease on a network address by sending a DHCPRELEASE message to the server. The client identifies the lease to be released by including its network address and its hardware address.

#### 3.7.4 DHCP lease renewal process

This section describes the interaction between DHCP servers and clients that

have already been configured and the process that ensures lease expiration and renewal.

The process involves the following steps:

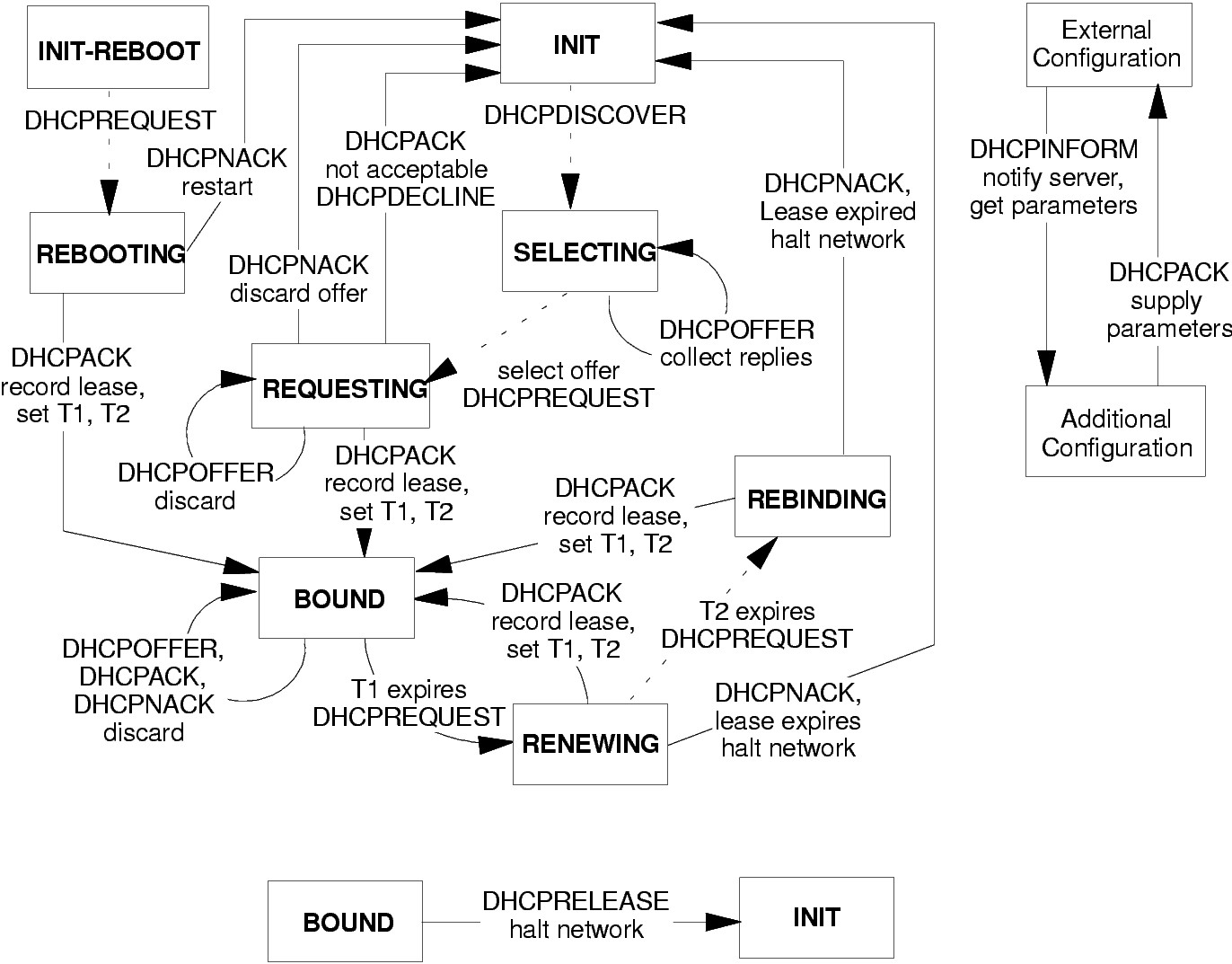
1. When a server sends the DHCPACK to a client with IP address and configuration parameters, it also registers the start of the lease time for that address. This lease time is passed to the client as one of the options in the DHCPACK message, together with two timer values, T1 and T2. The client is rightfully entitled to use the given address for the duration of the lease time. On applying the received configuration, the client also starts the timers T1 and T2. At this time, the client is in the BOUND state. Times T1 and T2 are options configurable by the server, but T1 must be less than T2, and T2 must be less than the lease time. According to RFC 2132, T1 defaults to (0.5 \* lease time) and T2 defaults to (0.875 \* lease time).
2. When timer T1 expires, the client will send a DHCPREQUEST (unicast) to the server that offered the address, asking to extend the lease for the given configuration. The client is now in the RENEWING state. The server usually responds with a DHCPACK message indicating the new lease time, and timers T1 and T2 are reset at the client accordingly. The server also resets its record of the lease time. In normal circumstances, an active client continually renews its lease in this way indefinitely, without the lease ever expiring.
3. If no DHCPACK is received until timer T2 expires, the client enters the

REBINDING state. It now broadcasts a DHCPREQUEST message to extend its lease. This request can be confirmed by a DHCPACK message from any DHCP server in the network.

1. If the client does not receive a DHCPACK message after its lease has expired, it has to stop using its current TCP/IP configuration. The client can then return to the INIT state, issuing a DHCPDISCOVER broadcast to try and obtain any valid address.

Figure 3-46 shows the DHCP process and changing client state during that process.

*Figure 3-46 DHCP client state and DHCP process*



#### 3.7.5 Reusing a previously allocated network address

If the client remembers and wants to reuse a previously allocated network address, the following steps are carried out:

1. The client broadcasts a DHCPREQUEST message on its local subnet. The DHCPREQUEST message includes the client's network address.
2. A server with knowledge of the client's configuration parameters responds with a DHCPACK message to the client (provided the lease is still current), renewing the lease at the same time.
3. If the client's lease has expired, the server with knowledge of the client responds with DHCPNACK.
4. The client receives the DHCPACK message with configuration parameters. The client performs a final check on the parameters and notes the duration of the lease and the lease identification cookie specified in the DHCPACK message. At this point, the client is configured and its T1 and T2 timers are reset.
5. If the client detects a problem with the parameters in the DHCPACK message, the client sends a DHCPDECLINE message to the server and restarts the configuration process by requesting a new network address. If the client receives a DHCPNAK message, it cannot reuse its remembered network address. It must instead request a new address by restarting the configuration process as described in 3.7.3, “Allocating a new network address” on page 134.

For further information, refer to the previously mentioned RFCs.

#### 3.7.6 Configuration parameters repository

DHCP provides persistent storage of network parameters for network clients. A DHCP server stores a key-value entry for each client, the key being some unique identifier, for example, an IP subnet number and a unique identifier within the subnet (normally a hardware address), and the value contains the configuration parameters last allocated to this particular client.

One effect of this is that a DHCP client will tend always to be allocated to the same IP address by the server, provided the pool of addresses is not over-subscribed and the previous address has not already been allocated to another client.

#### 3.7.7 DHCP considerations

DHCP dynamic allocation of IP addresses and configuration parameters relieves the network administrator of a great deal of manual configuration work. The ability for a device to be moved from network to network and to automatically obtain valid configuration parameters for the current network can be of great benefit to mobile users. Also, because IP addresses are only allocated when clients are actually active, it is possible, by the use of reasonably short lease times and the fact that mobile clients do not need to be allocated more than one address, to reduce the total number of addresses in use in an organization. However, consider the following points when DHCP is implemented:

DHCP is built on UDP, which is inherently insecure. In normal operation, an unauthorized client can connect to a network and obtain a valid IP address and configuration. To prevent this, it is possible to preallocate IP addresses to particular MAC addresses (similar to BOOTP), but this increases the administration workload and removes the benefit of recycling of addresses. Unauthorized DHCP servers can also be set up, sending false and potentially disruptive information to clients.

In a DHCP environment where automatic or dynamic address allocation is used, it is generally not possible to predetermine the IP address of a client at any particular point in time. In this case, if static DNS servers are also used, the DNS servers will not likely contain valid host name to IP address mappings for the clients. If having client entries in the DNS is important for the network, you can use DHCP to manually assign IP addresses to those clients and then administer the client mappings in the DNS accordingly.

#### 3.7.8 BOOTP and DHCP interoperability

The format of DHCP messages is based on the format of BOOTP messages, which enables BOOTP and DHCP clients to interoperate in certain circumstances. Every DHCP message contains a DHCP message type (51) option. Any message without this option is assumed to be from a BOOTP client.

Support for BOOTP clients at a DHCP server must be configured by a system administrator, if required. The DHCP server responds to BOOTPREQUEST messages with BOOTPREPLY, rather than DHCPOFFER. Any DHCP server that is not configured in this way will discard any BOOTPREQUEST frames sent to it. A DHCP server can offer static addresses, or automatic addresses (from its pool of unassigned addresses), to a BOOTP client (although not all BOOTP implementations will understand automatic addresses). If an automatic address *is* offered to a BOOTP client, that address must have an infinite lease time, because the client will not understand the DHCP lease mechanism.

DHCP messages can be forwarded by routers configured as BOOTP relay agents.

### 3.8 RFCs relevant to this chapter

The following RFCs provide detailed information about the connection protocols and architectures presented throughout this chapter:

[RFC 791 – Internet Protocol (September 1981)](http://www.ietf.org/rfc/rfc791.txt)

[RFC 792 – Internet Control Message Protocol (September 1981)](http://www.ietf.org/rfc/rfc792.txt)

[RFC 826 – Ethernet Address Resolution Protocol: Or converting network](http://www.ietf.org/rfc/rfc826.txt)   [protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware (November 1982)](http://www.ietf.org/rfc/rfc826.txt)

[RFC 903 – A Reverse Address Resolution Protocol (June 1984)](http://www.ietf.org/rfc/rfc903.txt)

[RFC 906 – Bootstrap loading using TFTP (June 1984)](http://www.ietf.org/rfc/rfc906.txt)

[RFC919 – Broadcasting Internet Datagrams (October 1984)](http://www.ietf.org/rfc/rfc919.txt)

[RFC922 – Broadcasting Internet datagrams in the presence of subnets (October 1984)](http://www.ietf.org/rfc/rfc922.txt)

[RFC 925 – Multi-LAN address resolution (October 1984)](http://www.ietf.org/rfc/rfc925.txt)

[RFC 950 – Internet Standard Subnetting Procedure (August 1985)](http://www.ietf.org/rfc/rfc950.txt)

[RFC 951 – Bootstrap Protocol (September 1985)](http://www.ietf.org/rfc/rfc951.txt)

[RFC 1027 – Using ARP to implement transparent subnet gateways](http://www.ietf.org/rfc/rfc1027.txt)

[(October](http://www.ietf.org/rfc/rfc1027.txt) [1987)](http://www.ietf.org/rfc/rfc1027.txt)

[RFC 1112 – Host extensions for IP multicasting (August 1989)](http://www.ietf.org/rfc/rfc1112.txt)

[RFC 1122 – Requirements for Internet Hosts – Communication Layers (October 1989)](http://www.ietf.org/rfc/rfc1122.txt)

[RFC 1166 – Internet numbers (July 1990)](http://www.ietf.org/rfc/rfc1166.txt)

[RFC 1191 – Path MTU discovery (November 1990)](http://www.ietf.org/rfc/rfc1191.txt)

[RFC 1256 – ICMP Router Discovery Messages (September 1991)](http://www.ietf.org/rfc/rfc1256.txt)

[RFC 1349 – Type of Service in the Internet Protocol Suite (July 1992)](http://www.ietf.org/rfc/rfc1349.txt)

[RFC 1393 Traceroute Using an IP Option G (January 1993)](http://www.ietf.org/rfc/rfc1393.txt)

[RFC 1466 – Guidelines for Management of IP Address Space (May 1993)](http://www.ietf.org/rfc/rfc1466.txt)

[RFC 1518 – An Architecture for IP Address Allocation with CIDR](http://www.ietf.org/rfc/rfc1518.txt)

[(September](http://www.ietf.org/rfc/rfc1518.txt) [1993)](http://www.ietf.org/rfc/rfc1518.txt)

[RFC 1519 – Classless Inter-Domain Routing (CIDR): an Address Assignment (September 1993)](http://www.ietf.org/rfc/rfc1519.txt)

[RFC 1520 – Exchanging Routing Information Across Provider Boundaries in the CIDR Environment (September 1993)](http://www.ietf.org/rfc/rfc1520.txt)

[RFC 1542 – Clarifications and Extensions for the Bootstrap Protocol](http://www.ietf.org/rfc/rfc1524.txt)

[(October](http://www.ietf.org/rfc/rfc1524.txt) [1993)](http://www.ietf.org/rfc/rfc1524.txt)

[RFC 1788 – ICMP Domain Name Messages (April 1995)](http://www.ietf.org/rfc/rfc1788.txt)

[RFC 1812 – Requirements for IP Version 4 Routers (June 1995)](http://www.ietf.org/rfc/rfc1812.txt)

[RFC 1918 – Address Allocation for Private Internets (February 1996)](http://www.ietf.org/rfc/rfc1918.txt)

[RFC 2050 – Internet Registry IP Allocation Guidelines (November 1996)](http://www.ietf.org/rfc/rfc2050.txt)

[RFC 2131 – Dynamic Host Configuration Protocol (March 1997)](http://www.ietf.org/rfc/rfc2131.txt)

[RFC 2132 – DHCP Options and BOOTP Vendor Extensions (March 1997)](http://www.ietf.org/rfc/rfc2132.txt)

[RFC 2236 – Internet Group Management Protocol, Version 2](http://www.ietf.org/rfc/rfc2236.txt)

[(November](http://www.ietf.org/rfc/rfc2236.txt) [1997)](http://www.ietf.org/rfc/rfc2236.txt)

[RFC 2474 – Definition of the Differentiated Services Field (DS Field) in the](http://www.ietf.org/rfc/rfc2474.txt)

[IPv4 and IPv6 Headers (December 1998)](http://www.ietf.org/rfc/rfc2474.txt)

[RFC 2644 – Changing the Default for Directed Broadcasts in Router](http://www.ietf.org/rfc/rfc2644.txt)

[(August](http://www.ietf.org/rfc/rfc2644.txt) [1999)](http://www.ietf.org/rfc/rfc2644.txt)

[RFC 2663 – IP Network Address Translator (NAT) Terminology and](http://www.ietf.org/rfc/rfc2663.txt)

[Considerations (August 1999)](http://www.ietf.org/rfc/rfc2663.txt)

[RFC 3022 – Traditional IP Network Address Translator (Traditional NAT) (January 2001)](http://www.ietf.org/rfc/rfc3022.txt)

[RFC 3168 – The Addition of Explicit Congestion Notification (ECN) to IP (September 2001)](http://www.ietf.org/rfc/rfc3168txt)

[RFC 3260 – New Terminology and Clarifications for Diffserv (April 2002)](http://www.ietf.org/rfc/rfc3260.txt)

[RFC 3330 – Special-Use IPv4 Addresses (September 2002)](http://www.ietf.org/rfc/rfc3330.txt)

[RFC 3396 – Encoding Long Options in the Dynamic Host Configuration](http://www.ietf.org/rfc/rfc3396.txt)

[Protocol (DHCPv4) (November 2002)](http://www.ietf.org/rfc/rfc3396.txt)

[RFC 3442 – The Classless Static Route Option for Dynamic Host](http://www.ietf.org/rfc/rfc3442.txt)

[Configuration Protocol (DHCP) version 4 (December 2002)](http://www.ietf.org/rfc/rfc3442.txt)

[RFC 3942 – Reclassifying Dynamic Host Configuration Protocol version 4](http://www.ietf.org/rfc/rfc3942txt)

[(DHCPv4) Options (November 2004)](http://www.ietf.org/rfc/rfc3942txt)

[RFC 4361 – Node-specific Client Identifiers for Dynamic Host Configuration](http://www.ietf.org/rfc/rfc4361.txt)

[Protocol Version Four (DHCPv4) (February 2006)](http://www.ietf.org/rfc/rfc4361.txt)

[RFC 4379 – Detecting Multi-Protocol Label Switched (MPLS) Data Plane](http://www.ietf.org/rfc/rfc479.txt)

[Failures (February 2006)](http://www.ietf.org/rfc/rfc479.txt)

|  |  |  |
| --- | --- | --- |
|  | |  | | --- | | **4** | |

## Chapter 4. Transport layer protocols

This chapter provides an overview of the most important and commonly used protocols of the TCP/IP transport layer. These include:

User Datagram Protocol (UDP)

Transmission Control Protocol (TCP)

By building on the functionality provided by the Internet Protocol (IP), the transport protocols deliver data to applications executing in the internet. This is done by making use of ports, as described in 4.1, “Ports and sockets” on page 144. The transport protocols can provide additional functionality such as congestion control, reliable data delivery, duplicate data suppression, and flow control as is done by TCP.

© Copyright IBM Corp. 1989-2006. All rights reserved.

### 4.1 Ports and sockets

This section introduces the concepts of the port and socket, which are needed to determine which local process at a given host actually communicates with which process, at which remote host, using which protocol. If this sounds confusing, consider the following points:

An application process is assigned a process identifier number (process ID), which is likely to be different each time that process is started.

Process IDs differ between operating system platforms, thus they are not uniform.

A server process can have multiple connections to multiple clients at a time, thus simple connection identifiers are not unique.The concept of ports and sockets provides a way to uniformly and uniquely identify connections and the programs and hosts that are engaged in them, irrespective of specific process IDs.

The concept of ports and sockets provides a way to uniformly and uniquely identify connections and the programs and hosts that are engaged in them, irrespective of specific process IDs.

#### 4.1.1 Ports

Each process that wants to communicate with another process identifies itself to the TCP/IP protocol suite by one or more ports. A port is a 16-bit number used by the host-to-host protocol to identify to which higher-level protocol or application program (process) it must deliver incoming messages. There are two types of ports:

Well-known: Well-known ports belong to standard servers, for example, Telnet uses port 23. Well-known port numbers range between 1 and 1023 (prior to 1992, the range between 256 and 1023 was used for UNIX-specific servers). Well-known port numbers are typically odd, because early systems using the port concept required an odd/even pair of ports for duplex operations. Most servers require only a single port. Exceptions are the BOOTP server, which uses two: 67 and 68 (see 3.6, “Bootstrap Protocol (BOOTP)” on page 125) and the FTP server, which uses two: 20 and 21 (see (14.1, “File Transfer Protocol (FTP)” on page 514).

The well-known ports are controlled and assigned by the Internet Assigned Number Authority (IANA) and on most systems can only be used by system processes or by programs executed by privileged users. Well-known ports allow clients to find servers without configuration information. The well-known port numbers are defined in STD 2 – Assigned Internet Numbers.

Ephemeral: Some clients do not need well-known port numbers because they initiate communication with servers, and the port number they are using is contained in the UDP/TCP datagrams sent to the server. Each client process is allocated a port number, for as long as it needs, by the host on which it is running. Ephemeral port numbers have values greater than 1023, normally in the range of 1024 to 65535.

Ephemeral ports are not controlled by IANA and can be used by ordinary user-developed programs on most systems.

Confusion, due to two different applications trying to use the same port numbers on one host, is avoided by writing those applications to request an available port from TCP/IP. Because this port number is dynamically assigned, it can differ from one invocation of an application to the next.

UDP, TCP, and ISO TP-4 all use the same port principle. To the best possible extent, the same port numbers are used for the same services on top of UDP, TCP, and ISO TP-4.

**Note:** Normally, a server will use either TCP or UDP, but there are exceptions. For example, domain name servers (see 12.1, “Domain Name System (DNS)” on page 426) use both UDP port 53 and TCP port 53.

#### 4.1.2 Sockets

The socket interface is one of several application programming interfaces to the communication protocols (see 11.2, “Application programming interfaces (APIs)” on page 410). Designed to be a generic communication programming interface, socket APIs were first introduced by 4.2 Berkeley Software Distribution (BSD). Although it has not been standardized, Berkeley socket API has become a de facto industry standard abstraction for network TCP/IP socket implementation.

Consider the following terminologies:

A *socket* is a special type of *file handle*, which is used by a process to request network services from the operating system.

A *socket address* is the triple:

<protocol, local-address, local port>

For example, in the TCP/IP (version 4) suite:

<tcp, 192.168.14.234, 8080>

A *conversation* is the communication link between two processes.

An *association* is the 5-tuple that completely specifies the two processes that comprise a connection:

<protocol, local-address, local-port, foreign-address, foreign-port>

In the TCP/IP (version 4) suite, the following could be a valid association:

<tcp, 192.168.14.234, 1500, 192.168.44, 22>

A *half-association* is either one of the following, which each specify half of a connection:

<protocol, local-address, local-process> Or:

<protocol, foreign-address, foreign-process>

The half-association is also called a *socket* or a *transport address*. That is, a socket is an endpoint for communication that can be named and addressed in a network.

Two processes communicate through TCP sockets. The socket model provides a process with a full-duplex byte stream connection to another process. The application need not concern itself with the management of this stream; these facilities are provided by TCP.

TCP uses the same port principle as UDP to provide multiplexing. Like UDP, TCP uses well-known and ephemeral ports. Each side of a TCP connection has a socket that can be identified by the triple <TCP, IP address, port number>. If two processes are communicating over TCP, they have a logical connection that is uniquely identifiable by the two sockets involved, that is, by the combination <TCP, local IP address, local port, remote IP address, remote port>. Server processes are able to manage multiple conversations through a single port. Refer to 11.2.1, “The socket API” on page 410 for more information about socket APIs.

### 4.2 User Datagram Protocol (UDP)

UDP is a standard protocol with STD number 6. UDP is described by RFC 768 – User Datagram Protocol. Its status is standard and almost every TCP/IP implementation intended for small data units transfer or those which can afford to lose a little amount of data (such as multimedia streaming) will include UDP.

UDP is basically an application interface to IP. It adds no reliability, flow-control, or error recovery to IP. It simply serves as a multiplexer/demultiplexer for sending and receiving datagrams, using ports to direct the datagrams, as shown in Figure 4-1. For a more detailed discussion of ports, refer to 4.1, “Ports and sockets” on page 144.

port b

process 2

port z

...

UDP - Port De-Multiplexing

IP

process n

process 1

port a

*Figure 4-1 UDP: Demultiplexing based on ports*

UDP provides a mechanism for one application to send a datagram to another. The UDP layer can be regarded as being extremely thin and is, consequently, very efficient, but it requires the application to take responsibility for error recovery and so on.

Applications sending datagrams to a host need to identify a target that is more specific than the IP address, because datagrams are normally directed to certain processes and not to the system as a whole. UDP provides this by using ports. We discuss the port concept in 4.1, “Ports and sockets” on page 144.

#### 4.2.1 UDP datagram format

Each UDP datagram is sent within a single IP datagram. Although, the IP datagram might be fragmented during transmission, the receiving IP implementation will reassemble it before presenting it to the UDP layer. All IP implementations are required to accept datagrams of 576 bytes, which means that, allowing for maximum-size IP header of 60 bytes, a UDP datagram of 516 bytes is acceptable to all implementations. Many implementations will accept larger datagrams, but this is not guaranteed.

The UDP datagram has an 8-byte header, as described in Figure 4-2 on page 148.

*Figure 4-2 UDP: Datagram format*

Destination Port

Source Port

Da

ta...

Checksum

Length

Where:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Source Port** | | Indicates the port of the sending process. It is the port to which replies are addressed. | | | |
| **Destination Port** | | Specifies the port of the destination process on the destination host. | | | |
| **Length** | | The length (in bytes) of this user datagram, including the header. | | | |
| **Checksum** | | An optional 16-bit one's complement of the one's complement sum of a pseudo-IP header, the UDP header, and the UDP data. In Figure 4-3, we see a pseudo-IP header. It contains the source and destination IP addresses, the protocol, and the UDP length. | | | |
|  | | Source IP address |  |
|  | | Destination IP addr | ess |
| Zero | | Protocol | TCP Length |

*Figure 4-3 UDP: Pseudo-IP header*

The pseudo-IP header effectively extends the checksum to include the original (unfragmented) IP datagram.

#### 4.2.2 UDP application programming interface

The application interface offered by UDP is described in RFC 768. It provides for:

The creation of new receive ports

The receive operation that returns the data bytes and an indication of source port and source IP address

The send operation that has, as parameters, the data, source, and destination ports and addresses

The way this interface is implemented is left to the discretion of each vendor.

Be aware that UDP and IP do not provide guaranteed delivery, flow-control, or error recovery, so these must be provided by the application.

Standard applications using UDP include:

Trivial File Transfer Protocol (see 14.2, “Trivial File Transfer Protocol (TFTP)” on page 529).

Domain Name System name server (see 12.2, “Dynamic Domain Name System” on page 453).

Remote Procedure Call, used by the Network File System (see both 11.2.2, “Remote Procedure Call (RPC)” on page 415 and 14.4, “Network File System (NFS)” on page 538).

Simple Network Management Protocol (see 17.1, “The Simple Network Management Protocol (SNMP)” on page 624).

Lightweight Directory Access Protocol (see 12.4, “Lightweight Directory Access Protocol (LDAP)” on page 459).

### 4.3 Transmission Control Protocol (TCP)

TCP is a standard protocol with STD number 7. TCP is described by RFC 793 – Transmission Control Protocol. Its status is standard, and in practice, every TCP/IP implementation that is not used exclusively for routing will include TCP.

TCP provides considerably more facilities for applications than UDP. Specifically, this includes error recovery, flow control, and reliability. TCP is a *connection-oriented* protocol, unlike UDP, which is *connectionless*. Most of the user application protocols, such as Telnet and FTP, use TCP. The two processes communicate with each other over a TCP connection (InterProcess Communication, or IPC), as shown in Figure 4-4. In the figure, processes 1 and 2 communicate over a TCP connection carried by IP datagrams. See 4.1, “Ports and sockets” on page 144 for more details about ports and sockets.

port m

reliable

TCP connection

...

TCP

IP

...

port n

process 2

...

TCP

IP

...

host A

unreliable

IP datagrams

process 1

host B

*Figure 4-4 TCP: Connection between processes*

#### 4.3.1 TCP concept

As noted earlier, the primary purpose of TCP is to provide a reliable logical circuit or connection service between pairs of processes. It does *not* assume reliability from the lower-level protocols (such as IP), so TCP must guarantee this itself.

TCP can be characterized by the following facilities it provides for the applications using it:

Stream data transfer: From the application's viewpoint, TCP transfers a contiguous stream of bytes through the network. The application does not have to bother with chopping the data into basic blocks or datagrams. TCP does this by grouping the bytes into TCP segments, which are passed to the IP layer for transmission to the destination. Also, TCP itself decides how to segment the data, and it can forward the data at its own convenience. Sometimes, an application needs to be sure that all the data passed to TCP has actually been transmitted to the destination. For that reason, a push function is defined. It will push all remaining TCP segments still in storage to

the destination host. The normal close connection function also pushes the data to the destination.

Reliability: TCP assigns a sequence number to each byte transmitted, and expects a positive acknowledgment (ACK) from the receiving TCP layer. If the ACK is not received within a timeout interval, the data is retransmitted. Because the data is transmitted in blocks (TCP segments), only the sequence number of the first data byte in the segment is sent to the destination host.

The receiving TCP uses the sequence numbers to rearrange the segments when they arrive out of order, and to eliminate duplicate segments.

Flow control: The receiving TCP, when sending an ACK back to the sender, also indicates to the sender the number of bytes it can receive (beyond the last received TCP segment) without causing overrun and overflow in its internal buffers. This is sent in the ACK in the form of the highest sequence number it can receive without problems. This mechanism is also referred to as a window-mechanism, and we discuss it in more detail later in this chapter.

Multiplexing: Achieved through the use of ports, just as with UDP.

Logical connections: The reliability and flow control mechanisms described here require that TCP initializes and maintains certain status information for each data stream. The combination of this status, including sockets, sequence numbers, and window sizes, is called a logical connection. Each connection is uniquely identified by the pair of sockets used by the sending and receiving processes.

Full duplex: TCP provides for concurrent data streams in both directions.

##### The window principle

A simple transport protocol might use the following principle: send a packet and then wait for an acknowledgment from the receiver before sending the next packet. If the ACK is not received within a certain amount of time, retransmit the packet. See Figure 4-5 for more details.

|  |  |
| --- | --- |
| Sender | Receiver |
| Send packet 1  Receive ACK  Send packet 2 | Receive packet 1 and reply with an ACK 1 |

*Figure 4-5 TCP: The window principle*

Although this mechanism ensures reliability, it only uses a part of the available network bandwidth.

Now, consider a protocol where the sender groups its packets to be transmitted, as in Figure 4-6, and uses the following rules:

The sender can send all packets within the window without receiving an ACK, but must start a timeout timer for each of them.

The receiver must acknowledge each packet received, indicating the sequence number of the last well-received packet.

The sender slides the window on each ACK received.

*Figure 4-6 TCP: Message packets*

window

packets

3

4

5

6

7

8

9

...

2

1

As shown in Figure 4-7, the sender can transmit packets 1 to 5 without waiting for any acknowledgment.

*Figure 4-7 TCP: Window principle*

Sender

Network

Send packet 1

Send packet 2

Send packet 3

Send packet 4

Send packet 5

ACK for packet 1 received

ACK 1

As shown in Figure 4-8, at the moment the sender receives ACK 1

(acknowledgment for packet 1), it can slide its window one packet to the right.

|  |  |
| --- | --- |
| Sender | Receiver |
| Send packet 1  Receive ACK  Send packet 2 | Receive packet 1 and reply with an ACK 1 |

*Figure 4-8 TCP: Message packets*

At this point, the sender can also transmit packet 6.

Imagine some special cases:

Packet 2 gets lost: The sender will not receive ACK 2, so its window will remain in position 1 (as in Figure 4-8 on page 153). In fact, because the receiver did not receive packet 2, it will acknowledge packets 3, 4, and 5 with an ACK 1, because packet 1 was the last one received in sequence. At the sender's side, eventually a timeout will occur for packet 2 and it will be retransmitted. Note that reception of this packet by the receiver will generate ACK 5, because it has now successfully received all packets 1 to 5, and the sender's window will slide four positions upon receiving this ACK 5.

Packet 2 did arrive, but the acknowledgment gets lost: The sender does not receive ACK 2, but will receive ACK 3. ACK 3 is an acknowledgment for *all* packets up to 3 (including packet 2) and the sender can now slide its window to packet 4.

This window mechanism ensures:

Reliable transmission.

Better use of the network bandwidth (better throughput).

Flow-control, because the receiver can delay replying to a packet with an acknowledgment, knowing its free buffers are available and the window size of the communication.

##### The window principle applied to TCP

The previously discussed window principle is used in TCP, but with a few differences:

Because TCP provides a byte-stream connection, sequence numbers are assigned to each byte in the stream. TCP divides this contiguous byte stream into TCP segments to transmit them. The window principle is used at the byte level, that is, the segments sent and ACKs received will carry byte-sequence numbers and the window size is expressed as a number of bytes, rather than a number of packets.

The window size is determined by the receiver when the connection is established and is variable during the data transfer. Each ACK message will include the window size that the receiver is ready to deal with at that particular time.

The sender's data stream can now be seen as follows in Figure 4-9.

5

4

2

1

...

1

14

13

12

11

10

9

8

7

3

6

5

A

B

C

D

window (size expressed in bytes)

bytes

*Figure 4-9 TCP: Window principle applied to TCP*

Where:

1. Bytes that are transmitted and have been acknowledged
2. Bytes that are sent but not yet acknowledged
3. Bytes that can be sent without waiting for any acknowledgment
4. Bytes that cannot be sent yet

Remember that TCP will block bytes into segments, and a TCP segment only carries the sequence number of the first byte in the segment.

##### TCP segment format

Figure 4-10 shows the TCP segment format.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | | 1 | | | 2 | | | | | | 3 |
| 0 1 2 3 4 5 6 7 8 9 | | 0 1 2 3 4 5 6 7 8 9 | | | 0 1 2 3 4 5 6 7 8 9 | | | | | | 0 1 2 3 4 5 6 7 8 9 |
| Source Port | | | | | Destination Port | | | | | | |
| Sequence Number | | | | | | | | | | | |
| Acknowledgment Number | | | | | | | | | | | |
| Data  Offset | Reserved | | U  R  G | A  C  K | | P  S  H | R  S  T | S  Y N | F  I  N | Window | |
| Checksum | | | | | | | | Urgent Pointer | | | |
| Options …|… Padding | | | | | | | | | | | |
| Data Bytes | | | | | | | | | | | |

*Figure 4-10 TCP: Segment format*

Where:

**Source Port** The 16-bit source port number, used by the receiver to

reply.

**Destination Port** The 16-bit destination port number.

**Sequence Number** The sequence number of the first data byte in this segment. If the SYN control bit is set, the sequence number is the initial sequence number (n) and the first data byte is n+1.

###### Acknowledgment Number

If the ACK control bit is set, this field contains the value of the next sequence number that the receiver is expecting to receive.

|  |  |  |
| --- | --- | --- |
| **Data Offset** | The number of 32-bit words in the TCP header. It indicates where the data begins. | |
| **Reserved** | Six bits reserved for future use; must be zero. | |
| **URG** | Indicates that the urgent pointer field is significant in this segment. | |
| **ACK**  **PSH**  **RST** | Indicates that the acknowledgment field is significant in this segment.  Push function.  Resets the connection. | |
| **SYN** | Synchronizes the sequence numbers. |
| **FIN** | No more data from sender. |
| **Window** | Used in ACK segments. It specifies the number of data bytes, beginning with the one indicated in the acknowledgment number field that the receiver (the sender of this segment) is willing to accept. |
| **Checksum** | The 16-bit one's complement of the one's complement sum of all 16-bit words in a pseudo-header, the TCP header, and the TCP data. While computing the checksum, the checksum field itself is considered zero. |

The pseudo-header is the same as that used by UDP for calculating the checksum. It is a pseudo-IP-header, only used for the checksum calculation, with the format shown in Figure 4-11.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Source IP address |  |  |
|  |  | Destination IP addr | ess |
|  | Zero | Protocol | TCP Length |

*Figure 4-11 TCP: Pseudo-IP header*

**Urgent Pointer** Points to the first data octet following the urgent data. Only significant when the URG control bit is set.

**Options** Just as in the case of IP datagram options, options can be

either:

* A single byte containing the option number
* A variable length option in the following format as shown in Figure 4-12

3

3

option

length

option data...

*Figure 4-12 TCP: IP datagram option, variable length option*

There are currently seven options defined, as shown in Table 4-1.

*Table 4-1 TCP: IP datagram options*

|  |  |  |
| --- | --- | --- |
| **Kind** | **Length** | **Meaning** |
| 0 | - | End of option list |
| 1 | - | No operation |
| 2 | 4 | Maximum segment size |
| 3 | 3 | Window scale |
| 4 | 2 | Sack-permitted |
| 5 | X | Sack |
| 8 | 10 | Time stamps |

###### Maximum segment size option

This option is only used during the establishment of the connection (SYN control bit set) and is sent from the side that is to receive data to indicate the maximum segment length it can handle. If this option is not used, any segment size is allowed. See Figure 4-13 for more details.

3

3

2

max.

seg size

4

*Figure 4-13 TCP: Maximum segment size*

###### Window scale option

This option is not mandatory. Both sides must send the Window scale option in their SYN segments to enable windows scaling in their direction. The Window scale expands the definition of the TCP window to 32 bits. It defines the 32-bit window size by using scale factor in the SYN segment over standard 16-bit window size. The receiver rebuilds the 32-bit window size by using the 16-bit window size and scale factor. This option is determined while handshaking. There is no way to change it after the connection has been established. See Figure 4-14 for more details.

3

3

shift.cnt

*Figure 4-14 TCP: Window scale option*

###### SACK-permitted option

This option is set when selective acknowledgment is used in that TCP connection. See Figure 4-15 for details.

4

2

*Figure 4-15 TCP: SACK-permitted option*

**SACK option** Selective Acknowledgment (SACK) allows the receiver to inform the sender about all the segments that are received successfully. Therefore, the sender will only send the segments that got lost. If the number of the segments that have been lost since the last SACK is too large, the SACK option will be too large. As a result, the number of blocks that can be reported by the SACK option is limited to four. To reduce this, the SACK option should be used for the most recent received data. See Figure 4-16 for more details.

*Figure 4-16 TCP: SACK option*

Length

5

Left Edge of 1st Block

Right Edge of 1st Block

-

- - - - -

-

Left Edge of Nth Block

Right Edge of Nth Bloc

k

/

/

/

/

**Timestamps option** The timestamps option sends a time stamp value that

indicates the current value of the time stamp clock of the TCP sending the option. The Timestamp Echo Value can only be used if the ACK bit is set in the TCP header. See Figure 4-17 for more details.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | |  |  | | | |
|  | |  |  |  |  | |
|  | 8 | 10 | TS Valve | TS Echo Reply |  |  |
|  |  |  |  |  |
| 1 | 1 | 4 | 4 | |

*Figure 4-17 TCP: Timestamps option*

**Padding** All zero bytes are used to fill up the TCP header to a total length that is a multiple of 32 bits.

##### Acknowledgments and retransmissions

TCP sends data in variable length segments. Sequence numbers are based on a byte count. Acknowledgments specify the sequence number of the next byte that the receiver expects to receive.

Consider that a segment gets lost or corrupted. In this case, the receiver will acknowledge all further well-received segments with an acknowledgment referring to the first byte of the missing packet. The sender will stop transmitting when it has sent all the bytes in the window. Eventually, a timeout will occur and the missing segment will be retransmitted.

Figure 4-18 illustrates and example where a window size of 1500 bytes and segments of 500 bytes are used.

Sender

Receiver

Segment 1 (seq. 1000)

Receives 1000, sends ACK 1500

Segment 2 (seq. 1500)

\\\

gets lost

Segment 3 (seq. 2000)

Receives the ACK 1500,

which slides window

Segment 4 (seq. 2500)

Receives one of the frames

and replies with ACK 1500

(

receiver is still expecting

byte 1500)

window size reached,

waiting for ACK

Receives the ACK 1500,

which does not slide the

window

Timeout for Segment 2

Retransmission

*Figure 4-18 TCP: Acknowledgment and retransmission process*

A problem now arises, because the sender does know that segment 2 is lost or corrupted, but does not know anything about segments 3 and 4. The sender should at least retransmit segment 2, but it could also retransmit segments 3 and 4 (because they are within the current window). It is possible that:

Segment 3 has been received, and we do not know about segment 4. It might be received, but ACK did not reach us yet, or it might be lost.

Segment 3 was lost, and we received the ACK 1500 on the reception of segment 4.

Each TCP implementation is free to react to a timeout as those implementing it want. It can retransmit only segment 2, but in the second case, we will be waiting again until segment 3 times out. In this case, we lose all of the throughput advantages of the window mechanism. Or TCP might immediately resend all of the segments in the current window.

Whatever the choice, maximal throughput is lost. This is because the ACK does not contain a second acknowledgment sequence number indicating the actual frame received.

###### Variable timeout intervals

Each TCP should implement an algorithm to adapt the timeout values to be used for the round trip time of the segments. To do this, TCP records the time at which a segment was sent, and the time at which the ACK is received. A weighted average is calculated over several of these round trip times, to be used as a timeout value for the next segment or segments to be sent.

This is an important feature, because delays can vary in IP network, depending on multiple factors, such as the load of an intermediate low-speed network or the saturation of an intermediate IP gateway.

##### Establishing a TCP connection

Before any data can be transferred, a connection has to be established between the two processes. One of the processes (usually the server) issues a *passive OPEN* call, the other an *active OPEN* call. The passive OPEN call remains dormant until another process tries to connect to it by an active OPEN.

As shown in Figure 4-19, in the network, three TCP segments are exchanged.

Initiating

)

client

(

TCP Layer

Listening

(

server

)

TCP Layer

1)

SYN SEQ:999 ACK

:

2)

SYN ACK SEQ:4999 ACK

:1000

3)

ACK SEQ:1000 ACK

:5000

*Figure 4-19 TCP: Connection establishment*

This whole process is known as a three-way handshake. Note that the exchanged TCP segments include the initial sequence numbers from both sides, to be used on subsequent data transfers.

Closing the connection is done implicitly by sending a TCP segment with the FIN bit (no more data) set. Because the connection is full-duplex (that is, there are two independent data streams, one in each direction), the FIN segment only closes the data transfer in one direction. The other process will now send the remaining data it still has to transmit and also ends with a TCP segment where the FIN bit is set. The connection is deleted (status information on both sides) after the data stream is closed in both directions.

The following is a list of the different states of a TCP connection:

LISTEN: Awaiting a connection request from another TCP layer.

SYN-SENT: A SYN has been sent, and TCP is awaiting the response SYN.

SYN-RECEIVED: A SYN has been received, a SYN has been sent, and TCP is awaiting an ACK.

ESTABLISHED: The three-way handshake has been completed.

FIN-WAIT-1: The local application has issued a CLOSE. TCP has sent a FIN, and is awaiting an ACK or a FIN.

FIN-WAIT-2: A FIN has been sent, and an ACK received. TCP is awaiting a FIN from the remote TCP layer.

CLOSE-WAIT: TCP has received a FIN, and has sent an ACK. It is awaiting a close request from the local application before sending a FIN.

CLOSING: A FIN has been sent, a FIN has been received, and an ACK has been sent. TCP is awaiting an ACK for the FIN that was sent.

LAST-ACK: A FIN has been received, and an ACK and a FIN have been sent.

TCP is awaiting an ACK.

TIME-WAIT: FINs have been received and ACK’d, and TCP is waiting two MSLs to remove the connection from the table.

CLOSED: Imaginary, this indicates that a connection has been removed from the connection table.

#### 4.3.2 TCP application programming interface

The TCP application programming interface is not fully defined. Only some base functions it should provide are described in RFC 793 – Transmission Control Protocol. As is the case with most RFCs in the TCP/IP protocol suite, a great degree of freedom is left to the implementers, thereby allowing for optimal operating system-dependent implementations, resulting in better efficiency and greater throughput.

The following function calls are described in the RFC:

Open: To establish a connection takes several parameters, such as:

* Active/Passive
* Foreign socket
* Local port number
* Timeout value (optional)

This returns a local connection name, which is used to reference this particular connection in all other functions.

Send: Causes data in a referenced user buffer to be sent over the connection. Can optionally set the URGENT flag or the PUSH flag.

Receive: Copies incoming TCP data to a user buffer.

Close: Closes the connection; causes a push of all remaining data and a TCP segment with FIN flag set.

Status: An implementation-dependent call that can return information, such as:

* Local and foreign socket
* Send and receive window sizes
* Connection state
* Local connection name

Abort: Causes all pending Send and Receive operations to be aborted, and a RESET to be sent to the foreign TCP.

For full details, see RFC 793 – Transmission Control Protocol.

#### 4.3.3 TCP congestion control algorithms

One big difference between TCP and UDP is the congestion control algorithm. The TCP congestion algorithm prevents a sender from overrunning the capacity of the network (for example, slower WAN links). TCP can adapt the sender's rate

to network capacity and attempt to avoid potential congestion situations. In order to understand the difference between TCP and UDP, understanding basic TCP congestion control algorithms is very helpful.

Several congestion control enhancements have been added and suggested to TCP over the years. This is still an active and ongoing research area, but modern implementations of TCP contain four intertwined algorithms as basic Internet standards:

Slow start

Congestion avoidance

Fast retransmit

Fast recovery

##### Slow start

Old implementations of TCP start a connection with the sender injecting multiple segments into the network, up to the window size advertised by the receiver. Although this is OK when the two hosts are on the same LAN, if there are routers and slower links between the sender and the receiver, problems can arise. Some intermediate routers cannot handle it, packets get dropped, and retransmission results and performance is degraded.

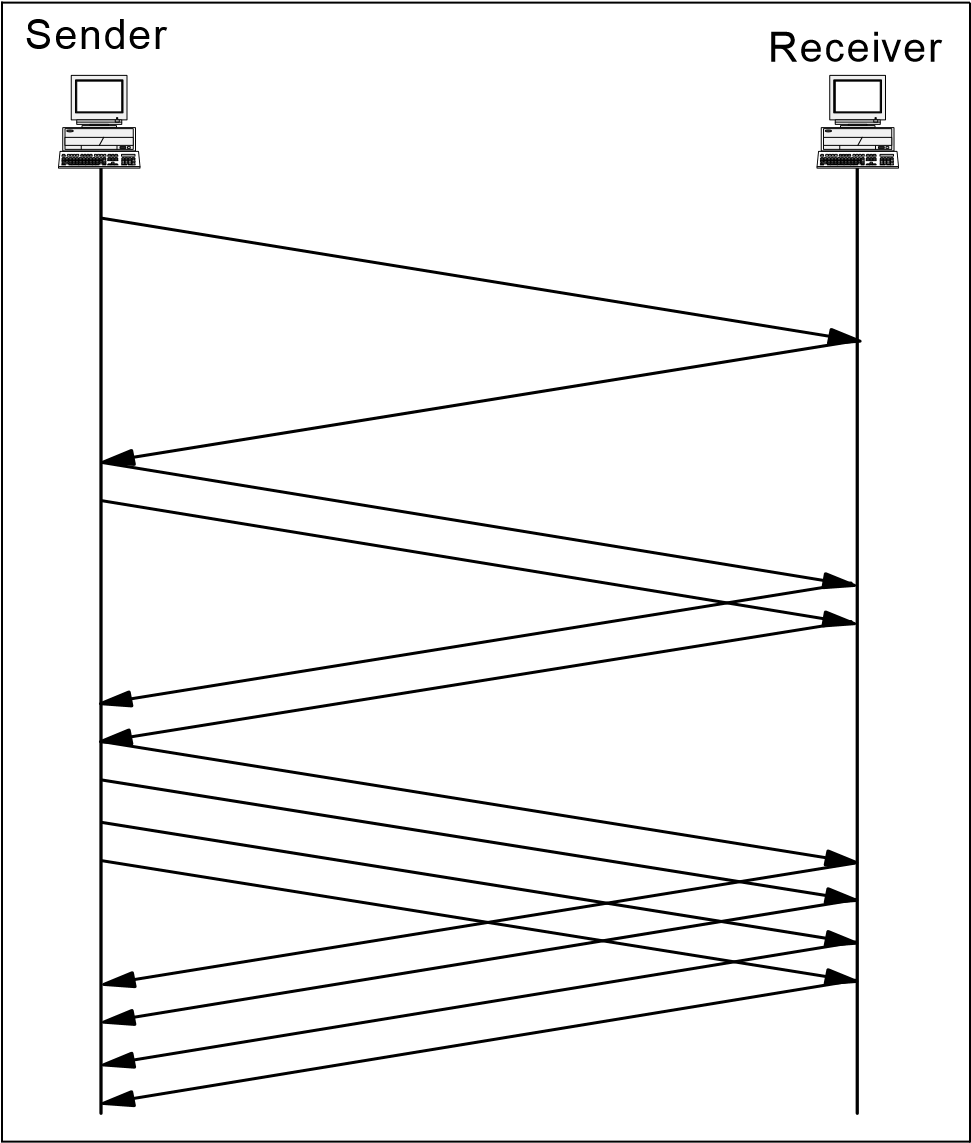
The algorithm to avoid this is called slow start. It operates by observing that the rate at which new packets should be injected into the network is the rate at which the acknowledgments are returned by the other end. Slow start adds another window to the sender's TCP: the congestion window, called cwnd. When a new connection is established with a host on another network, the congestion window is initialized to one segment (for example, the segment size announced by the other end, or the default, typically 536 or 512).

**Note:** Congestion control is defined in RFC 2581. Additionally, RFC 3390 updates RFC 2581 such that TCP implementations can initialize the congestion window to between two and four segments, with an upper limit of 4 K.

Each time an ACK is received, the congestion window is increased by one segment. The sender can transmit the lower value of the congestion window or the advertised window. The congestion window is flow control imposed by the sender, while the advertised window is flow control imposed by the receiver. The former is based on the sender's assessment of perceived network congestion; the latter is related to the amount of available buffer space at the receiver for this connection.

The sender starts by transmitting one segment and waiting for its ACK. When that ACK is received, the congestion window is incremented from one to two, and two segments can be sent. When each of those two segments is acknowledged, the congestion window is increased to four. This provides an exponential growth, although it is not exactly exponential, because the receiver might delay its ACKs, typically sending one ACK for every two segments that it receives.

At some point, the capacity of the IP network (for example, slower WAN links) can be reached, and an intermediate router will start discarding packets. This tells the sender that its congestion window has gotten too large. See Figure 4-20 for an overview of slow start in action.



*Figure 4-20 TCP: Slow start in action*

##### Congestion avoidance

The assumption of the algorithm is that packet loss caused by damage is very small (much less than 1%). Therefore, the loss of a packet signals congestion somewhere in the network between the source and destination. There are two indications of packet loss:

A timeout occurs.

Duplicate ACKs are received.

Congestion avoidance and slow start are independent algorithms with different objectives. But when congestion occurs, TCP must slow down its transmission rate of packets into the network and invoke slow start to get things going again. In practice, they are implemented together.

Congestion avoidance and slow start require that two variables be maintained for each connection:

A congestion window, cwnd A slow start threshold size, ssthresh

The combined algorithm operates as follows:

1. Initialization for a given connection sets cwnd to one segment and ssthresh to 65535 bytes.
2. The TCP output routine never sends more than the lower value of cwnd or the receiver's advertised window.
3. When congestion occurs (timeout or duplicate ACK), one-half of the current window size is saved in ssthresh. Additionally, if the congestion is indicated by a timeout, cwnd is set to one segment.
4. When new data is acknowledged by the other end, increase cwnd, but the way it increases depends on whether TCP is performing slow start or congestion avoidance. If cwnd is less than or equal to ssthresh, TCP is in slow start; otherwise, TCP is performing congestion avoidance.

Slow start continues until TCP is halfway to where it was when congestion occurred (since it recorded half of the window size that caused the problem in step 2), and then congestion avoidance takes over. Slow start has cwnd begin at one segment, and incremented by one segment every time an ACK is received. As mentioned earlier, this opens the window exponentially: send one segment, then two, then four, and so on.

Congestion avoidance dictates that cwnd be incremented by segsize\*segsize/cwnd each time an ACK is received, where segsize is the segment size and cwnd is maintained in bytes. This is a linear growth of cwnd, compared to slow start's exponential growth. The increase in cwnd should be at most one segment each round-trip time (regardless of how many ACKs are received in that round-trip time), while slow start increments cwnd by the number of ACKs received in a round-trip time. Many implementations incorrectly add a small fraction of the segment size (typically the segment size divided by 8) during congestion avoidance. This is wrong and should not be emulated in future releases. See Figure 4-21 for an example of TCP slow start and congestion avoidance in action.

Round Trip Times

CWND

cwnd

ssthresh

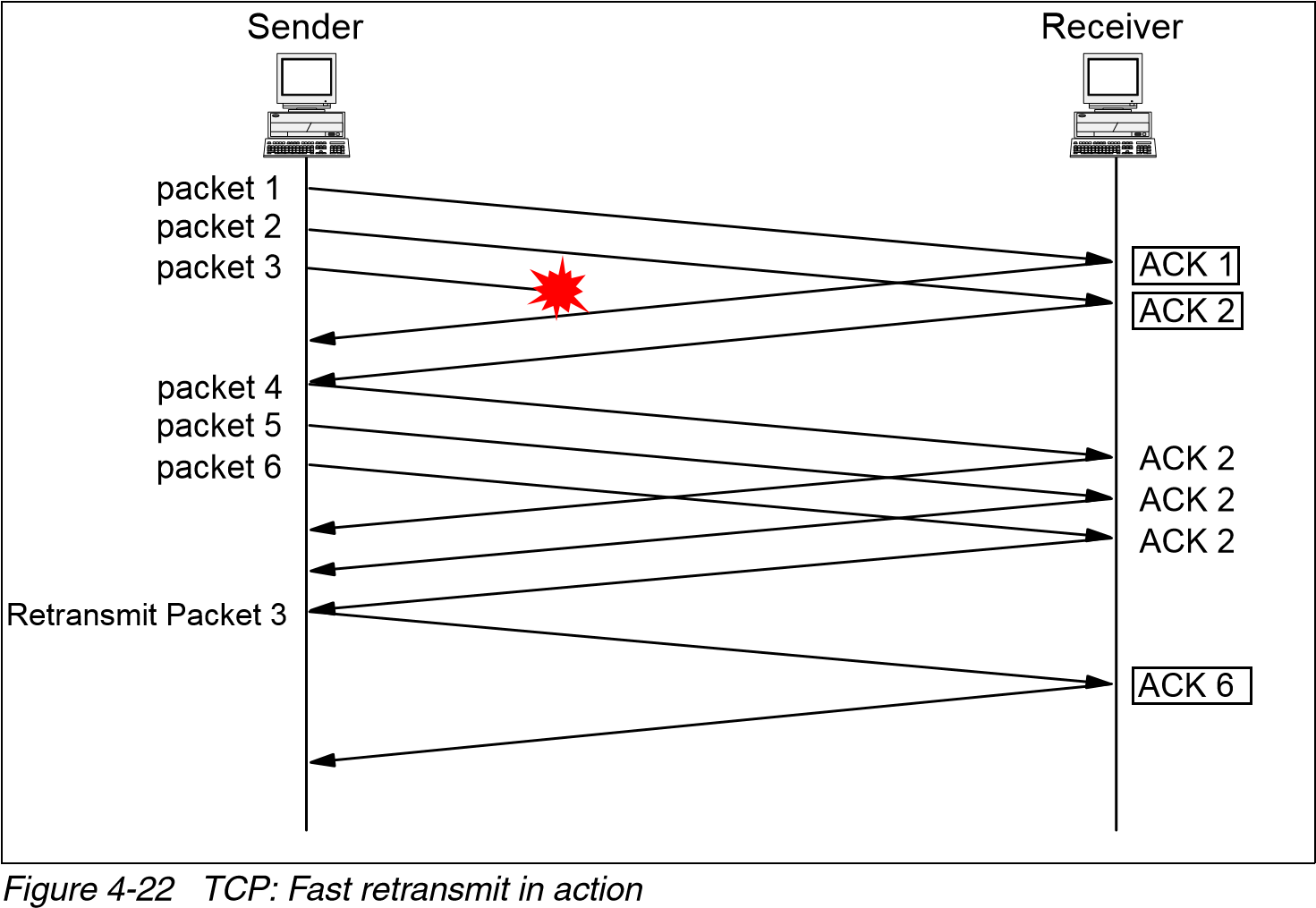
*Figure 4-21 TCP: Slow start and congestion avoidance behavior in action*

##### Fast retransmit

Fast retransmit avoids having TCP wait for a timeout to resend lost segments.

Modifications to the congestion avoidance algorithm were proposed in 1990. Before describing the change, realize that TCP can generate an immediate acknowledgment (a duplicate ACK) when an out-of-order segment is received. This duplicate ACK should not be delayed. The purpose of this duplicate ACK is to let the other end know that a segment was received out of order and to tell it what sequence number is expected.

Because TCP does not know whether a duplicate ACK is caused by a lost segment or just a reordering of segments, it waits for a small number of duplicate ACKs to be received. It is assumed that if there is just a reordering of the segments, there will be only one or two duplicate ACKs before the reordered segment is processed, which will then generate a new ACK. If three or more duplicate ACKs are received in a row, it is a strong indication that a segment has been lost. TCP then performs a retransmission of what appears to be the missing segment, without waiting for a retransmission timer to expire. See Figure 4-22 for an overview of TCP fast retransmit in action.



##### Fast recovery

After fast retransmit sends what appears to be the missing segment, congestion avoidance, but not slow start, is performed. This is the fast recovery algorithm. It is an improvement that allows high throughput under moderate congestion, especially for large windows.

The reason for not performing slow start in this case is that the receipt of the duplicate ACKs tells TCP more than just a packet has been lost. Because the receiver can only generate the duplicate ACK when another segment is received, that segment has left the network and is in the receiver's buffer. That is, there is still data flowing between the two ends, and TCP does not want to reduce the flow abruptly by going into slow start. The fast retransmit and fast recovery algorithms are usually implemented together as follows:

1. When the third duplicate ACK in a row is received, set ssthresh to one-half the current congestion window, cwnd, but no less than two segments. Retransmit the missing segment. Set cwnd to ssthresh plus three times the segment size. This inflates the congestion window by the number of segments that have left the network and the other end has cached (3).
2. Each time another duplicate ACK arrives, increment cwnd by the segment size. This inflates the congestion window for the additional segment that has left the network. Transmit a packet, if allowed by the new value of cwnd.
3. When the next ACK arrives that acknowledges new data, set cwnd to ssthresh (the value set in step 1). This ACK is the acknowledgment of the retransmission from step 1, one round-trip time after the retransmission. Additionally, this ACK acknowledges all the intermediate segments sent between the lost packet and the receipt of the first duplicate ACK. This step is congestion avoidance, because TCP is down to one-half the rate it was at when the packet was lost.

### 4.4 RFCs relevant to this chapter

The following RFCs provide detailed information about the connection protocols and architectures presented throughout this chapter:

RFC 761 – DoD standard Transmission Control Protocol (January 1980)

RFC 768 – User Datagram Protocol (August 1980)

RFC 793 – Updated by RFC 3168 - The Addition of Explicit Congestion

Notification (ECN) to IP (September 2001)

|  |  |  |
| --- | --- | --- |
|  | |  | | --- | | **5** | |

## Chapter 5. Routing protocols

This chapter provides an overview of IP routing and discusses the various routing protocols used.

One of the basic functions provided by the IP protocol is the ability to form connections between different physical networks. A system that performs this function is called an *IP router*. This type of device attaches to two or more physical networks and forwards datagrams between the networks.

When sending data to a remote destination, a host passes datagrams to a local router. The router forwards the datagrams toward the final destination. They travel from one router to another until they reach a router connected to the destination’s LAN segment. Each router along the end-to-end path selects the *next hop* device used to reach the destination. The next hop represents the next device along the path to reach the destination. It is located on a physical network connected to this intermediate system. Because this physical network differs from the one on which the system originally received the datagram, the intermediate host has *forwarded* (that is, routed) the IP datagram from one physical network to another.

© Copyright IBM Corp. 1989-2006. All rights reserved.

Figure 5-1 shows an environment where Host C is positioned to forward packets between network X and network Y.

*Figure 5-1 IP routing operations*

Application

TCP

IP

Interface X

Host A

Application

TCP

IP

Interface Y

Host

B

Host C Acting as

Router

IP Routing

Interface X

Interface Y

Network Y

Network X

The IP routing table in each device is used to forward packets between network segments. The basic table contains information about a router’s locally connected networks. The configuration of the device can be extended to contain information detailing remote networks. This information provides a more complete view of the overall environment.

A robust routing protocol provides the ability to dynamically build and manage the information in the IP routing table. As network topology changes occur, the routing tables are updated with minimal or no manual intervention. This chapter details several IP routing protocols and how each protocol manages this information.

**Note:** In other sections of this book, the position of each protocol within the layered model of the OSI protocol stack is shown. The routing function is included as part of the internetwork layer. However, the primary function of a routing protocol is to exchange routing information with other routers. In this respect, routing protocols behave more like an application protocol. Therefore, this chapter makes no attempt to represent the position of these protocols within the overall protocol stack.

**Note:** Early IP routing documentation often referred to an IP router as an *IP gateway.*

### 5.1 Autonomous systems

The definition of an autonomous system (AS) is integral to understanding the function and scope of a routing protocol. An AS is defined as a logical portion of

a larger IP network. An AS normally consists of an internetwork within an organization. It is administered by a single management authority. As shown in Figure 5-2, an AS can connect to other autonomous systems managed by the same organization. Alternatively, it can connect to other public or private networks.

Router

Router

IGPs

Autonomous System A

Router

IGPs

Autonomous System C

Router

Router

Router

Single Management Authority

EGP

Router

Router

Router

Autonomous System B

IGPs

Internet

*Figure 5-2 Autonomous systems*

Some routing protocols are used to determine routing paths within an AS. Others are used to interconnect a set of autonomous systems:

Interior Gateway Protocols (IGPs): Interior Gateway Protocols allow routers to exchange information within an AS. Examples of these protocols are Open

Short Path First (OSPF) and Routing Information Protocol (RIP).

Exterior Gateway Protocols (EGPs): Exterior Gateway Protocols allow the exchange of summary information between autonomous systems. An example of this type of routing protocol is Border Gateway Protocol (BGP).

Figure 5-2 on page 173 depicts the interaction between Interior and Exterior Gateway Protocols. It shows the Interior Gateway Protocols used to maintain routing information within each AS. The figure also shows the Exterior Gateway Protocols maintaining the routing information between autonomous systems.

Within an AS, multiple interior routing processes can be used. When this occurs, the AS must appear to other autonomous systems as having a single coherent interior routing plan. The AS must present a consistent view of the internal destinations.

### 5.2 Types of IP routing and IP routing algorithms

Routing algorithms build and maintain the IP routing table on a device. There are two primary methods used to build the routing table:

Static routing: Static routing uses preprogrammed definitions representing paths through the network.

Dynamic routing: Dynamic routing algorithms allow routers to automatically discover and maintain awareness of the paths through the network. This automatic discovery can use a number of currently available dynamic routing protocols. The difference between these protocols is the way they discover and calculate new routes to destination networks. They can be classified into four broad categories:

* Distance vector protocols
* Link state protocols
* Path vector protocols
* Hybrid protocols

The remainder of this section describes the operation of each algorithm.

There are several reasons for the multiplicity of protocols:

Routing within a network and routing between networks typically have different requirements for security, stability, and scalability. Different routing protocols have been developed to address these requirements.

New protocols have been developed to address the observed deficiencies in established protocols.

Different-sized networks can use different routing algorithms. Small to medium-sized networks often use routing protocols that reflect the simplicity of the environment.

However, these protocols do not scale to support large, interconnected networks. More complex routing algorithms are required to support these environments.

#### 5.2.1 Static routing

Static routing is manually performed by the network administrator. The administrator is responsible for discovering and propagating routes through the network. These definitions are manually programmed in every routing device in the environment.

After a device has been configured, it simply forwards packets out the predetermined ports. There is no communication between routers regarding the current topology of the network.

In small networks with minimal redundancy, this process is relatively simple to administer. However, there are several disadvantages to this approach for maintaining IP routing tables:

Static routes require a considerable amount of coordination and maintenance in non-trivial network environments.

Static routes cannot dynamically adapt to the current operational state of the network. If a destination subnetwork becomes unreachable, the static routes pointing to that network remain in the routing table. Traffic continues to be forwarded toward that destination. Unless the network administrator updates the static routes to reflect the new topology, traffic is unable to use any alternate paths that may exist.

Normally, static routes are used only in simple network topologies. However, there are additional circumstances when static routing can be attractive. For example, static routes can be used:

To manually define a default route. This route is used to forward traffic when the routing table does not contain a more specific route to the destination.

To define a route that is not automatically advertised within a network.

When utilization or line tariffs make it undesirable to send routing advertisement traffic through lower-capacity WAN connections.

When complex routing policies are required. For example, static routes can be used to guarantee that traffic destined for a specific host traverses a designated network path.

To provide a more secure network environment. The administrator is aware of all subnetworks defined in the environment. The administrator specifically authorizes all communication permitted between these subnetworks.

To provide more efficient resource utilization. This method of routing table management requires no network bandwidth to advertise routes between neighboring devices. It also uses less processor memory and CPU cycles to calculate network paths.

#### 5.2.2 Distance vector routing

Distance vector algorithms are examples of dynamic routing protocols. These algorithms allow each device in the network to automatically build and maintain a local IP routing table.

The principle behind distance vector routing is simple. Each router in the internetwork maintains the *distance* or *cost* from itself to every known destination. This value represents the overall desirability of the path. Paths associated with a smaller cost value are more attractive to use than paths associated with a larger value. The path represented by the smallest cost becomes the preferred path to reach the destination.

This information is maintained in a *distance vector table.* The table is periodically

advertised to each neighboring router. Each router processes these advertisements to determine the best paths through the network.

The main advantage of distance vector algorithms is that they are typically easy to implement and debug. They are very useful in small networks with limited redundancy. However, there are several disadvantages with this type of protocol:

During an adverse condition, the length of time for every device in the network to produce an accurate routing table is called the *convergence time*. In large, complex internetworks using distance vector algorithms, this time can be excessive. While the routing tables are converging, networks are susceptible to inconsistent routing behavior. This can cause routing loops or other types of unstable packet forwarding.

To reduce convergence time, a limit is often placed on the maximum number of hops contained in a single route. Valid paths exceeding this limit are not usable in distance vector networks.

Distance vector routing tables are periodically transmitted to neighboring devices. They are sent even if no changes have been made to the contents of the table. This can cause noticeable periods of increased utilization in reduced capacity environments.

Enhancements to the basic distance vector algorithm have been developed to reduce the convergence and instability exposures. We describe these enhancements in 5.3.5, “Convergence and counting to infinity” on page 185.

RIP is a popular example of a distance vector routing protocol.

#### 5.2.3 Link state routing

The growth in the size and complexity of networks in recent years has necessitated the development of more robust routing algorithms. These algorithms address the shortcoming observed in distance vector protocols.

These algorithms use the principle of a *link state* to determine network topology. A link state is the description of an interface on a router (for example, IP address, subnet mask, type of network) and its relationship to neighboring routers. The collection of these link states forms a link state database.

The process used by link state algorithms to determine network topology is straightforward:

1. Each router identifies all other routing devices on the directly connected networks.
2. Each router advertises a list of all directly connected network links and the associated cost of each link. This is performed through the exchange of link state advertisements (LSAs) with other routers in the network.
3. Using these advertisements, each router creates a database detailing the current network topology. The topology database in each router is identical.
4. Each router uses the information in the topology database to compute the most desirable routes to each destination network. This information is used to update the IP routing table.

##### Shortest-Path First (SPF) algorithm

The SPF algorithm is used to process the information in the topology database. It provides a tree-representation of the network. The device running the SPF algorithm is the root of the tree. The output of the algorithm is the list of shortest-paths to each destination network. Figure 5-3 on page 178 provides an example of the shortest-path algorithm executed on router A.

*Figure 5-3 Shortest-Path First (SPF) example*

A

B

C

D

Link State

Database

4

2

1

D

1

3

3

E

A

B

C

D

B-2

C-1

A-2

D-4

A-1

D-1

E-3

C-1

B-4

E-3

C-3

D-3

A

B

C

D

E

Because each router is processing the same set of LSAs, each router creates an identical link state database. However, because each device occupies a different place in the network topology, the application of the SPF algorithm produces a different tree for each router.

The OSPF protocol is a popular example of a link state routing protocol.

#### 5.2.4 Path vector routing

Path vector routing is discussed in RFC 1322; the following paragraphs are based on the RFC.

The path vector routing algorithm is somewhat similar to the distance vector algorithm in the sense that each border router advertises the destinations it can reach to its neighboring router. However, instead of advertising networks in terms of a destination and the distance to that destination, networks are advertised as destination addresses and path descriptions to reach those destinations.

A route is defined as a pairing between a destination and the attributes of the path to that destination, thus the name, path vector routing, where the routers receive a vector that contains paths to a set of destinations.

The path, expressed in terms of the domains (or confederations) traversed so far, is carried in a special path attribute that records the sequence of routing domains through which the reachability information has passed. The path represented by the smallest number of domains becomes the preferred path to reach the destination.

The main advantage of a path vector protocol is its flexibility. There are several other advantages regarding using a path vector protocol:

The computational complexity is smaller than that of the link state protocol. The path vector computation consists of evaluating a newly arrived route and comparing it with the existing one, while conventional link state computation requires execution of an SPF algorithm.

Path vector routing does not require all routing domains to have homogeneous policies for route selection; route selection policies used by one routing domain are not necessarily known to other routing domains. The support for heterogeneous route selection policies has serious implications for the computational complexity. The path vector protocol allows each domain to make its route selection autonomously, based only on local policies. However, path vector routing can accommodate heterogeneous route selection with little additional cost.

Only the domains whose routes are affected by the changes have to recompute.

Suppression of routing loops is implemented through the path attribute, in contrast to link state and distance vector, which use a globally-defined monotonically thereby increasing metric for route selection. Therefore, different confederation definitions are accommodated because looping is avoided by the use of full path information.

Route computation precedes routing information dissemination. Therefore, only routing information associated with the routes selected by a domain is distributed to adjacent domains.

Path vector routing has the ability to selectively hide information.

However, there are disadvantages to this approach, including: Topology changes only result in the recomputation of routes affected by these

changes, which is more efficient than complete recomputation. However, because of the inclusion of full path information with each distance vector, the effect of a topology change can propagate farther than in traditional distance vector algorithms.

Unless the network topology is fully meshed or is able to appear so, routing loops can become an issue.

BGP is a popular example of a path vector routing protocol.

#### 5.2.5 Hybrid routing

The last category of routing protocols is hybrid protocols. These protocols attempt to combine the positive attributes of both distance vector and link state protocols. Like distance vector, hybrid protocols use metrics to assign a preference to a route. However, the metrics are more accurate than conventional distance vector protocols. Like link state algorithms, routing updates in hybrid protocols are event driven rather than periodic. Networks using hybrid protocols tend to converge more quickly than networks using distance vector protocols. Finally, these protocols potentially reduce the costs of link state updates and distance vector advertisements.

Although open hybrid protocols exist, this category is almost exclusively associated with the proprietary EIGRP algorithm. EIGRP was developed by Cisco Systems, Inc.

### 5.3 Routing Information Protocol (RIP)

RIP is an example of an interior gateway protocol designed for use within small autonomous systems. RIP is based on the Xerox XNS routing protocol. Early implementations of RIP were readily accepted because the code was incorporated in the Berkeley Software Distribution (BSD) UNIX-based operating system. RIP is a distance vector protocol.

In mid-1988, the IETF issued RFC 1058 with updates in RFC2453, which describes the standard operations of a RIP system. However, the RFC was issued after many RIP implementations had been completed. For this reason, some RIP systems do not support the entire set of enhancements to the basic distance vector algorithm (for example, poison reverse and triggered updates).

#### 5.3.1 RIP packet types

The RIP protocol specifies two packet types. These packets can be sent by any device running the RIP protocol:

Request packets: A request packet queries neighboring RIP devices to obtain their distance vector table. The request indicates if the neighbor should return either a specific subset or the entire contents of the table.

Response packets: A response packet is sent by a device to advertise the information maintained in its local distance vector table. The table is sent during the following situations:

* The table is automatically sent every 30 seconds.
* The table is sent as a response to a request packet generated by another RIP node.
* If triggered updates are supported, the table is sent when there is a change to the local distance vector table. We discuss triggered updates in “Triggered updates” on page 188.

When a response packet is received by a device, the information contained in the update is compared against the local distance vector table. If the update contains a lower cost route to a destination, the table is updated to reflect the new path.

#### 5.3.2 RIP packet format

RIP uses a specific packet format to share information about the distances to known network destinations. RIP packets are transmitted using UDP datagrams. RIP sends and receives datagrams using UDP port 520.

RIP datagrams have a maximum size of 512 octets. Updates larger than this size must be advertised in multiple datagrams. In LAN environments, RIP datagrams are sent using the MAC all-stations broadcast address and an IP network broadcast address. In point-to-point or non-broadcast environments, datagrams are specifically addressed to the destination device.

The RIP packet format is shown in Figure 5-4.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Number of Octets  Request=1  1Response=2  Version = 1  1  2  Address Family  2Identifier for IP  2   |  |  | | --- | --- | | Command |  | | Version | | Reserved | | AFI: X'0002' | | Reserved | | IP Address | | Reserved | | Metric | |  |   4 }Routing Entry: May be repeated  }  8  4 |

*Figure 5-4 RIP packet format*

A 512 byte packet size allows a maximum of 25 routing entries to be included in a single RIP advertisement.

#### 5.3.3 RIP modes of operation

RIP hosts have two modes of operation:

Active mode: Devices operating in active mode advertise their distance vector table and also receive routing updates from neighboring RIP hosts. Routing devices are typically configured to operate in active mode.

Passive (or silent) mode: Devices operating in this mode simply receive routing updates from neighboring RIP devices. They do not advertise their distance vector table. End stations are typically configured to operate in passive mode.

#### 5.3.4 Calculating distance vectors

The distance vector table describes each destination network. The entries in this table contain the following information:

The destination network (vector) described by this entry in the table.

The associated cost (distance) of the most attractive path to reach this destination. This provides the ability to differentiate between multiple paths to a destination. In this context, the terms distance and cost can be misleading. They have no direct relationship to physical distance or monetary cost.

The IP address of the next-hop device used to reach the destination network.

Each time a routing table advertisement is received by a device, it is processed to determine if any destination can be reached by a lower cost path. This is done using the RIP distance vector algorithm. The algorithm can be summarized as:

At router initialization, each device contains a distance vector table listing each directly attached networks and configured cost. Typically, each network is assigned a cost of 1. This represents a single hop through the network. The total number of hops in a route is equal to the total cost of the route. However, cost can be changed to reflect other measurements such as utilization, speed, or reliability.

Each router periodically (typically every 30 seconds) transmits its distance vector table to each of its neighbors. The router can also transmit the table when a topology change occurs. Each router uses this information to update its local distance vector table:

* The total cost to each destination is calculated by adding the cost reported in a neighbor's distance vector table to the cost of the link to that neighbor. The path with the least cost is stored in the distance vector table.
* All updates automatically supersede the previous information in the distance vector table. This allows RIP to maintain the integrity of the routes in the routing table.

The IP routing table is updated to reflect the least-cost path to each destination.

Figure 5-5 illustrates the distance vector tables for three routers within a simple internetwork.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| N2  R1 | | | | N3  N4  N5  N6  R2  R3  R4  R5 |
| N1  Router R2  Distance Vector  Table | | | | Router R3 Router R4  Distance Vector Distance Vector  Table Table   |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | Net | Next Hop | Metric |  | Net | Next  Hop | Metric | | N1 | R2 | 3 | N1 | R3 | 4 | | N2 | R2 | 2 | N2 | R3 | 3 | | N3 | Direct | 1 | N3 | R3 | 2 | | N4 | Direct | 1 | N4 | Direct | 1 | | N5 | R4 | 2 | N5 | Direct | 1 | | N6 | R4 | 3 | N6 | R5 | 2 | |
|  | Net | Next Hop | Metric |
|  | N1 | R1 | 2 |
|  | N2 | Direct | 1 |
|  | N3 | Direct | 1 |
|  | N4 | R3 | 2 |
|  | N5 | R3 | 3 |
|  | N6 | R3 | 4 |
|  | | | |

*Figure 5-5 A sample distance vector routing table*

#### 5.3.5 Convergence and counting to infinity

Given sufficient time, this algorithm will correctly calculate the distance vector table on each device. However, during this convergence time, erroneous routes may propagate through the network. Figure 5-6 shows this problem.

*Figure 5-6 Counting to infinity sample network*

Target

Network

A

B

C

D

(

n) = Network Cost

(1)

(1)

(1)

(1)

(1)

(10)

This network contains four interconnected routers. Each link has a cost of 1, except for the link connecting router C and router D; this link has a cost of 10. The costs have been defined so that forwarding packets on the link connecting router C and router D is undesirable. After the network has converged, each device has routing information describing all networks.

For example, to reach the target network, the routers have the following information:

Router D to the target network: Directly connected network. Metric is 1.

Router B to the target network: Next hop is router D. Metric is 2.

Router C to the target network: Next hop is router B. Metric is 3. Router A to the target network: Next hop is router B. Metric is 3.

Consider an adverse condition where the link connecting router B and router D fails. After the network has reconverged, all routes use the link connecting router C and router D to reach the target network. However, this reconvergence time can be considerable. Figure 5-7 illustrates how the routes to the target network are updated throughout the reconvergence period. For simplicity, this figure assumes all routers send updates at the same time.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Time D: | Direct | 1 | Direct | 1 | Direct 1 | Direct | 1 | -- | Direct | 1 | Direct | 1 |
| B: | Unreachable |  | C | 4 | C 5 | C | 6 |  | C | 11 | C | 12 |
| C: | B | 3 | A | 4 | A 5 | A | 6 |  | A | 11 | D | 11 |
| A: | B | 3 | C | 4 | C 5 | C | 6 | -- | C | 11 | C | 12 |

*Figure 5-7 Network convergence sequence*

Reconvergence begins when router B notices that the route to router D is unavailable. Router B is able to immediately remove the failed route because the link has timed out. However, a considerable amount of time passes before the other routers remove their references to the failed route. This is described in the sequence of updates shown in Figure 5-7:

1. Prior to the adverse condition occurring, router A and router C have a route to the target network through router B.
2. The adverse condition occurs when the link connecting router D and router B fails. Router B recognizes that its preferred path to the target network is now invalid.
3. Router A and router C continue to send updates reflecting the route through router B. This route is actually invalid because the link connecting router D and router B has failed.
4. Router B receives the updates from router A and router C. Router B believes it should now route traffic to the target network through either router A or router C. In reality, this is not a valid route, because the routes in router A and router C are vestiges of the previous route through router B.
5. Using the routing advertisement sent by router B, router A and router C are able to determine that the route through router B has failed. However, router A and router C now believe the preferred route exists through the partner.

Network convergence continues as router A and router C engage in an extended period of mutual deception. Each device claims to be able to reach the target network through the partner device. The path to reach the target network now contains a routing loop.

The manner in which the costs in the distance vector table increment gives rise to the term *counting to infinity*. The costs continues to increment, theoretically to infinity. To minimize this exposure, whenever a network is unavailable, the incrementing of metrics through routing updates must be halted as soon as it is practical to do so. In a RIP environment, costs continue to increment until they reach a maximum value of 16. This limit is defined in RFC 1058.

A side effect of the metric limit is that it also limits the number of hops a packet can traverse from source network to destination network. In a RIP environment, any path exceeding 15 hops is considered invalid. The routing algorithm will discard these paths.

There are two enhancements to the basic distance vector algorithm that can minimize the counting to infinity problem:

Split horizon with poison reverse Triggered updates

These enhancements do not impact the maximum metric limit.

##### Split horizon

The excessive convergence time caused by counting to infinity can be reduced with the use of split horizon. This rule dictates that routing information is prevented from exiting the router on an interface through which the information was received.

The basic split horizon rule is not supported in RFC 1058. Instead, the standard specifies the enhanced split horizon with poison reverse algorithm. The basic rule is presented here for background and completeness. The enhanced algorithm is reviewed in the next section.

The incorporation of split horizon modifies the sequence of routing updates shown in Figure 5-7 on page 186. The new sequence is shown in Figure 5-8. The tables show that convergence occurs considerably faster using the split horizon rule.

Time

D:

Direct

1

Direct

1

Direct

1

Direct

1

B:

Unreachable

Unreachable

Unreachable

C

12

C:

B

3

A

4

D

11

D

11

A:

B

3

C

4

Unreachable

C

12

Note: Faster Routing Table Convergence

*Figure 5-8 Network convergence with split horizon*

The limitation to this rule is that each node must wait for the route to the unreachable destination to time out before the route is removed from the distance vector table. In RIP environments, this timeout is at least three minutes after the initial outage. During that time, the device continues to provide erroneous information to other nodes about the unreachable destination. This propagates routing loops and other routing anomalies.

##### Split horizon with poison reverse

Poison reverse is an enhancement to the standard split horizon implementation. It is supported in RFC 1058. With poison reverse, all known networks are advertised in each routing update. However, those networks learned through a specific interface are advertised as unreachable in the routing announcements sent out to that interface.

This drastically improves convergence time in complex, highly-redundant environments. With poison reverse, when a routing update indicates that a network is unreachable, routes are immediately removed from the routing table. This breaks erroneous, looping routes before they can propagate through the network. This approach differs from the basic split horizon rule where routes are eliminated through timeouts.

Poison reverse has no benefit in networks with no redundancy (single path networks).

One disadvantage to poison reverse is that it might significantly increase the size of routing annoucements exchanged between neighbors. This is because all routes in the distance vector table are included in each announcement. Although this is generally not an issue on local area networks, it can cause periods of increased utilization on lower-capacity WAN connections.

##### Triggered updates

Like split horizon with poison reverse, algorithms implementing triggered updates are designed to reduce network convergence time. With triggered updates, whenever a router changes the cost of a route, it immediately sends the modified distance vector table to neighboring devices. This mechanism ensures that topology change notifications are propagated quickly, rather than at the normal periodic interval.

Triggered updates are supported in RFC 1058.

#### 5.3.6 RIP limitations

There are a number of limitations observed in RIP environments:

Path cost limits: The resolution to the counting to infinity problem enforces a maximum cost for a network path. This places an upper limit on the maximum network diameter. Networks requiring paths greater than 15 hops must use an alternate routing protocol.

Network-intensive table updates: Periodic broadcasting of the distance vector table can result in increased utilization of network resources. This can be a concern in reduced-capacity segments.

Relatively slow convergence: RIP, like other distance vector protocols, is relatively slow to converge. The algorithms rely on timers to initiate routing table advertisements.

No support for variable length subnet masking: Route advertisements in a RIP environment do not include subnet masking information. This makes it impossible for RIP networks to deploy variable length subnet masks.

### 5.4 Routing Information Protocol Version 2 (RIP-2)

The IETF recognizes two versions of RIP:

RIP Version 1 (RIP-1): This protocol is described in RFC 1058.

RIP Version 2 (RIP-2): RIP-2 is also a distance vector protocol designed for use within an AS. It was developed to address the limitations observed in RIP-1. RIP-2 is described in RFC 2453. The standard (STD 56) was published in late 1994.

In practice, the term RIP refers to RIP-1. Whenever you encounter the term RIP in TCP/IP literature, it is safe to assume that the reference is to RIP Version 1 unless otherwise stated. This same convention is used in this document. However, when the two versions are being compared, the term RIP-1 is used to avoid confusion.

RIP-2 is similar to RIP-1. It was developed to extend RIP-1 functionality in small networks. RIP-2 provides these additional benefits not available in RIP-1:

Support for CIDR and VLSM: RIP-2 supports supernetting (that is, CIDR) and variable-length subnet masking. This support was the major reason the new standard was developed. This enhancement positions the standard to accommodate a degree of addressing complexity not supported in RIP-1.

Support for multicasting: RIP-2 supports the use of multicasting rather than simple broadcasting of routing annoucements. This reduces the processing load on hosts not listening for RIP-2 messages. To ensure interoperability with RIP-1 environments, this option is configured on each network interface.

Support for authentication: RIP-2 supports authentication of any node transmitting route advertisements. This prevents fraudulent sources from corrupting the routing table.

Support for RIP-1: RIP-2 is fully interoperable with RIP-1. This provides backward-compatibility between the two standards.

As noted in the RIP-1 section, one notable shortcoming in the RIP-1 standard is the implementation of the metric field. RIP-1 specifies the metric as a value between 0 and 16. To ensure compatibility with RIP-1 networks, RIP-2 preserves this definition. In both standards, networks paths with a hop-count greater than 15 are interpreted as unreachable.

#### 5.4.1 RIP-2 packet format

The original RIP-1 specification was designed to support future enhancements. The RIP-2 standard was able to capitalize on this feature. RIP-2 developers noted that a RIP-1 packet already contains a version field and that 50% of the octets are unused.

Figure 5-9 illustrates the contents of a RIP-2 packet. The packet is shown with authentication information. The first entry in the update contains either a routing entry or an authentication entry. If the first entry is an authentication entry, 24 additional routing entries can be included in the message. If there is no authentication information, 25 routing entries can be provided.

*Figure 5-9 RIP-2 packet format*

Command

Version

Reserved

AFI: X'FFFF'

Authentication Type

Authentication Data

AFI:2

Route Tag

IP Address

Subnet Mask

Next Hop

Metric

Number of Octets

Request=1

Response=2

0=

No Authentication

2=

Password Data

Password if Type 2 Selected

Routing Entry: May not be

repeated

}

}

1

1

2

2

2

16

2

2

4

4

4

4

}

}

Authentication

Entry

The use of the command field, IP address field, and metric field in a RIP-2 message is identical to the use in a RIP-1 message. Otherwise, the changes implemented in a RIP-2 packets include:

**Version** The value contained in this field must be two. This instructs RIP-1 routers to ignore any information contained in the previously unused fields.

**AFI (Address Family)** A value of x’0002’ indicates the address contained in the network address field is an IP address. An value of x'FFFF' indicates an authentication entry.

**Authentication Type** This field defines the remaining 16 bytes of the

authentication entry. A value of 0 indicates *no* authentication. A value of two indicates the authentication data field contains password data.

**Authentication Data** This field contains a 16-byte password.

**Route Tag** This field is intended to differentiate between internal and external routes. Internal routes are learned through RIP-2 within the same network or AS.

**Subnet Mask** This field contains the subnet mask of the referenced network.

**Next Hop** This field contains a recommendation about the next hop the router should use when sending datagrams to the referenced network.

#### 5.4.2 RIP-2 limitations

RIP-2 was developed to address many of the limitations observed in RIP-1. However, the path cost limits and slow convergence inherent in RIP-1 networks are also concerns in RIP-2 environments.

In addition to these concerns, there are limitations to the RIP-2 authentication process. The RIP-2 standard does not encrypt the authentication password. It is transmitted in clear text. This makes the network vulnerable to attack by anyone with direct physical access to the environment.

### 5.5 RIPng for IPv6

RIPng was developed to allow routers within an IPv6-based network to exchange information used to compute routes. It is documented in RFC 2080. We provide additional information regarding IPv6 in 9.1, “IPv6 introduction” on page 328.

Like the other protocols in the RIP family, RIPng is a distance vector protocol designed for use within a small autonomous system. RIPng uses the same algorithms, timers, and logic used in RIP-2.

RIPng has many of the same limitations inherent in other distance vector

protocols. Path cost restrictions and convergence time remain a concern in

RIPng networks.

#### 5.5.1 Differences between RIPng and RIP-2

There are two important distinctions between RIP-2 and RIPng:

Support for authentication: The RIP-2 standard includes support for authenticating a node transmitting routing information. RIPng does not include any native authentication support. Rather, RIPng uses the security features inherent in IPv6. In addition to authentication, these security features provide the ability to encrypt each RIPng packet. This can control the set of devices that receive the routing information.One consequence of using IPv6 security features is that the AFI field within the RIPng packet is eliminated. There is no longer a need to distinguish between authentication entries and routing entries within an advertisement.

Support for IPv6 addressing formats: The fields contained in RIPng packets were updated to support the longer IPv6 address format.

#### 5.5.2 RIPng packet format

RIPng packets are transmitted using UDP datagrams. RIPng sends and receives datagrams using UDP port number 521.

The format of a RIPng packet is similar to the RIP-2 format. Specifically, both packets contain a 4 octet command header followed by a set of 20 octet route entries. The RIPng packet format is shown in Figure 5-10.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Number of Octets  Request=1   |  |  | | --- | --- | | Command |  | | Version | | Reserved | | Route Table Entry (RTE) | |  |   1 {Response=2  1  2  20 {May be repeated |

*Figure 5-10 RIPng packet format*

The use of the command field and the version field is identical to the use in a RIP-2 packet. However, the fields containing routing information have been updated to accommodate the 16 octet IPv6 address. These fields are used differently than the corresponding fields in a RIP-1 or RIP-2 packet. The format of the RTE is shown in Figure 5-11.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Number of Octets   |  |  | | --- | --- | | IPv6 Prefix |  | | Route Tag | | Prefix Length | | Metric | |  |   16  2  1  1 |

*Figure 5-11 Route table entry (RTE)*

In RIPng, the combination of the IP prefix and the prefix length identifies the route to be advertised. The metric remains encoded in a 1 octet field. This length is sufficient because RIPng uses a maximum hop-count of 16.

Another difference between RIPng and RIP-2 is the process used to determine the next hop. In RIP-2, each route table entry contains a next hop field. In RIPng, including this information in each RTE would have doubled the size of the advertisement. Therefore, in RIPng, the next hop is included in a special type of RTE. The specified next hop applies to each subsequent routing table entry in the advertisement. The format of an RTE used to specify the next hop is shown in Figure 5-12.

16

2

1

1

IPv6 Next Hop Address

Reserved

Reserved

Metric 0x'FF'

Number of Octets

{

Used to distinguish a

next hop entry

*Figure 5-12 Next Hop route table entry (RTE)*

The next hop RTE is identified by a value of 0x’FF’ in the metric field. This reserved value is outside the valid range of metrics.

The use of RTEs and next hop RTEs is shown in Figure 5-13.

*Figure 5-13 Using the RIPng RTE*

4

20

20

20

20

20

20

20

20

Number of Octets

Command

Routing entry #1

Routing entry #2

Routing entry #3

Next hop RTE A

Routing entry #4

Routing entry #5

Next hop RTE B

Routing entry #6

In this example, the first three routing entries do not have a corresponding next hop RTE. The address prefixes specified by these entries will be routed through the advertising router. The prefixes included in routing entries 4 and 5 will route through the next hop address specified in the next hop RTE A. The prefix included in routing entry 6 will route through the next hop address specified in the next hop RTE B.

### 5.6 Open Shortest Path First (OSPF)

The Open Shortest Path First (OSPF) protocol is another example of an interior gateway protocol. It was developed as a non-proprietary routing alternative to address the limitations of RIP. Initial development started in 1988 and was finalized in 1991. Subsequent updates to the protocol continue to be published. The current version of the standard is documented in RFC 2328.

OSPF provides a number of features not found in distance vector protocols. Support for these features has made OSPF a widely-deployed routing protocol in large networking environments. In fact, RFC 1812 – Requirements for IPv4 Routers, lists OSPF as the only required dynamic routing protocol. The following features contribute to the continued acceptance of the OSPF standard:

Equal cost load balancing: The simultaneous use of multiple paths can provide more efficient utilization of network resources.

Logical partitioning of the network: This reduces the propagation of outage information during adverse conditions. It also provides the ability to aggregate routing announcements that limit the advertisement of unnecessary subnet information.

Support for authentication: OSPF supports the authentication of any node transmitting route advertisements. This prevents fraudulent sources from corrupting the routing tables.

Faster convergence time: OSPF provides instantaneous propagation of routing changes. This expedites the convergence time required to update network topologies.

Support for CIDR and VLSM: This allows the network administrator to efficiently allocate IP address resources.

OSPF is a link state protocol. As with other link state protocols, each OSPF router executes the SPF algorithm (“Shortest-Path First (SPF) algorithm” on page 177) to process the information stored in the link state database. The algorithm produces a shortest-path tree detailing the preferred routes to each destination network.

#### 5.6.1 OSPF terminology

OSPF uses specific terminology to describe the operation of the protocol.

##### OSPF areas

OSPF networks are divided into a collection of *areas*. An area consists of a logical grouping of networks and routers. The area can coincide with geographic or administrative boundaries. Each area is assigned a 32-bit *area ID*.

Subdividing the network provides the following benefits:

Within an area, every router maintains an identical topology database describing the routing devices and links within the area. These routers have no knowledge of topologies outside the area. They are only aware of routes to these external destinations. This reduces the size of the topology database maintained by each router.

Areas limit the potentially explosive growth in the number of link state updates. Most LSAs are distributed only within an area.

Areas reduce the CPU processing required to maintain the topology database. The SPF algorithm is limited to managing changes within the area.

###### Backbone area and area 0

All OSPF networks contain at least one area. This area is known as area 0 or the backbone area. Additional areas can be created based on network topology or other design requirements.

In networks containing multiple areas, the backbone physically connects to all other areas. OSPF expects all areas to announce routing information directly into the backbone. The backbone then announces this information into other areas.

Figure 5-14 on page 198 depicts a network with a backbone area and four additional areas.

##### Intra-area, area border, and AS boundary routers

There are three classifications of routers in an OSPF network. Figure 5-14 illustrates the interaction of these devices.

Area 4

Area 2

Area 1

ASBR

ABR

ABR

ABR

Area 3

ABR

ASBR

IA

IA

AS External Links

Area 0

AS 10

AS External Links

Key

ASBR - AS Border Router

ABR - Area Border Router

IA - Intra-Area Router

*Figure 5-14 OSPF router types*

Where:

|  |  |
| --- | --- |
| **Intra-area routers** | This class of router is logically located entirely within an OSPF area. Intra-area routers maintain a topology database for their local area. |
| **Area border routers (ABR)** | This class of router is logically connected to two or more areas. One area must be the backbone area. An ABR is used to interconnect areas. They maintain a separate topology database for each attached area. ABRs also execute  separate instances of the SPF algorithm for each area. |

**AS boundary routers (ASBR)** This class of router is located at the periphery of an OSPF internetwork. It functions as a gateway exchanging reachability between the OSPF network and other routing environments.

ASBRs are responsible for announcing AS external link advertisements through the AS. We provide more information about external link advertisements in 5.6.4, “OSPF route redistribution” on page 208.

Each router is assigned a 32-bit *router ID* (RID). The RID uniquely identifies the device. One popular implementation assigns the RID from the lowest-numbered IP address configured on the router.

##### Physical network types

OSPF categorizes network segments into three types. The frequency and types of communication occurring between OSPF devices connected to these networks is impacted by the network type:

Point-to-point: Point-to-point networks directly link two routers.

Multi-access: Multi-access networks support the attachment of more than two routers.

They are further subdivided into two types:

* Broadcast networks have the capability of simultaneously directing a packet to all attached routers. This capability uses an address that is recognized by all devices. Ethernet and token-ring LANs are examples of OSPF broadcast multi-access networks.
* Non-broadcast networks do not have broadcasting capabilities. Each packet must be specifically addressed to every router in the network. X.25 and frame relay networks are examples of OSPF non-broadcast multi-access networks.

Point-to-multipoint: Point-to-multipoint networks are a special case of multi-access, non-broadcast networks. In a point-to-multipoint network, a device is not required to have a direct connection to every other device. This is known as a partially meshed environment.

##### Neighbor routers and adjacencies

Routers that share a common network segment establish a neighbor relationship

on the segment. Routers must agree on the following information to become neighbors:

Area ID: The routers must belong to the same OSPF area.

Authentication: If authentication is defined, the routers must specify the same password.

Hello and dead intervals: The routers must specify the same timer intervals used in the Hello protocol. We describe this protocol further in “OSPF packet types” on page 203.

Stub area flag: The routers must agree that the area is configured as a stub area. We describe stub areas further in 5.6.5, “OSPF stub areas” on page 210.

After two routers have become neighbors, an adjacency relationship can be formed between the devices. Neighboring routers are considered adjacent when they have synchronized their topology databases. This occurs through the exchange of link state information.

##### Designated and backup designated router

The exchange of link state information between neighbors can create significant quantities of network traffic. To reduce the total bandwidth required to synchronize databases and advertise link state information, a router does not necessarily develop adjacencies with every neighboring device:

Multi-access networks: Adjacencies are formed between an individual router and the (backup) designated router.

Point-to-point networks: An adjacency is formed between both devices.

Each multi-access network elects a designated router (DR) and backup designated router (BDR). The DR performs two key functions on the network segment:

It forms adjacencies with all routers on the multi-access network. This causes the DR to become the focal point for forwarding LSAs.

It generates network link advertisements listing each router connected to the multi-access network. For additional information regarding network link advertisements, see “Link state advertisements and flooding” on page 201.

The BDR forms the same adjacencies as the designated router. It assumes DR functionality when the DR fails.

Each router is assigned an 8-bit priority, indicating its ability to be selected as the DR or BDR. A router priority of zero indicates that the router is not eligible to be selected. The priority is configured on each interface in the router.

Figure 5-15 illustrates the relationship between neighbors. No adjacencies are formed between routers that are not selected to be the DR or BDR.

DR

Other

Other

BDR

Adjacent

Neighbors

Neighbors

*Figure 5-15 Relationship between adjacencies and neighbors*

##### Link state database

The link state database is also called the *topology database*. It contains the set of link state advertisements describing the OSPF network and any external connections. Each router within the area maintains an identical copy of the link state database.

**Note:** RFC 2328 uses the term link state database in preference to topology database. The former term has the advantage in that it describes the contents of the database. The latter term is more descriptive of the purpose of the database. This book has previously used the term topology database for this reason. However for the remainder of the OSPF section, we refer to it as the link state database.

##### Link state advertisements and flooding

The contents of an LSA describe an individual network component (that is, router, segment, or external destination). LSAs are exchanged between adjacent OSPF routers. This is done to synchronize the link state database on each device.

When a router generates or modifies an LSA, it must communicate this change throughout the network. The router starts this process by forwarding the LSA to each adjacent device. Upon receipt of the LSA, these neighbors store the information in their link state database and communicate the LSA to their neighbors. This store and forward activity continues until all devices receive the update. This process is called *reliable flooding*. Two steps are taken to ensure that this flooding effectively transmits changes without overloading the network with excessive quantities of LSA traffic:

Each router stores the LSA for a period of time before propagating the information to its neighbors. If, during that time, a new copy of the LSA arrives, the router replaces the stored version. However, if the new copy is outdated, it is discarded.

To ensure reliability, each link state advertisement must be acknowledged. Multiple acknowledgements can be grouped together into a single acknowledgement packet. If an acknowledgement is not received, the original link state update packet is retransmitted.

Link state advertisements contain five types of information. Together these advertisements provide the necessary information needed to describe the entire OSPF network and any external environments:

Router LSAs: This type of advertisement describes the state of the router's interfaces (links) within the area. They are generated by every OSPF router. The advertisements are flooded throughout the area.

Network LSAs: This type of advertisement lists the routers connected to a multi-access network. They are generated by the DR on a multi-access segment. The advertisements are flooded throughout the area.

Summary LSAs (Type-3 and Type-4): This type of advertisement is generated by an ABR. There are two types of summary link advertisements:

* Type-3 summary LSAs describe routes to destinations in other areas within the OSPF network (inter-area destinations).
* Type-4 summary LSAs describe routes to ASBRs. Summary LSAs are used to exchange reachability information between areas. Normally, information is announced into the backbone area. The backbone then injects this information into other areas.

AS external LSAs: This type of advertisement describes routes to destinations external to the OSPF network. They are generated by an ASBR. The advertisements are flooded throughout all areas in the OSPF network.

Figure 5-16 illustrates the different types of link state advertisements.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | Router Links | Network Links | | Router  - Advertised by router - Describes state/cost of router's links | DR  - Advertised by designated router - Describes all routers attached to network | | Summary Links  ABR  Area X  Area 0   * Advertised by router * Describes state/cost of | External Links  ASBR  Area 0  Area X   * Advertised by router * Describes state/cost of |   router's links router's links |

*Figure 5-16 OSPF link state advertisements*

##### OSPF packet types

OSPF packets are transmitted in IP datagrams. They are not encapsulated within TCP or UDP packets. The IP header uses protocol identifier 89. OSPF packets are sent with an IP ToS of 0 and an IP precedence of internetwork control. This is used to obtain preferential processing for the packets. We discuss ToS and IP precedence further in “Integrated Services” on page 288.

Wherever possible, OSPF uses multicast facilities to communicate with neighboring devices. In broadcast and point-to-point environments, packets are sent to the reserved multicast address 224.0.0.5. RFC 2328 refers to this as the AllSPFRouters address. In non-broadcast environments, packets are addressed to the neighbor’s specific IP address.

All OSPF packets share the common header shown in Figure 5-17. The header provides general information including area identifier, RID, checksum, and authentication information.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Number of Octets  Version = 2  1  1= Hello   |  |  | | --- | --- | | Version |  | | Packet Type | | Packet Length | | Router ID | | Area ID | | Checksum | | Authentication Type | | Authentication Data | |  |   1 {2=Database Description  3=Link State Request  4=Link State Update  25=Link State Acknowledgement  4  4  2  20=No Authentication  {1=Simple Password  8Password if Type 1 Selected |

*Figure 5-17 OSPF common header*

The type field identifies the OSPF packet as one of five possible types:

|  |  |
| --- | --- |
| **Hello** | This packet type discovers and maintains neighbor relationships. |
| **Database description** | This packet type describes the set of LSAs contained in the router's link state database. |
| **Link state request** | This packet type requests a more current instance of an LSA from a neighbor. |
| **Link state update** | This packet type provides a more current instance of an LSA to a neighbor. |

###### Link state acknowledgement

This packet type acknowledges receipt of a newly received LSA.

We describe the use of these packets in the next section.

#### 5.6.2 Neighbor communication

OSPF is responsible for determining the optimum set of paths through a network. To accomplish this, each router exchanges LSAs with other routers in the network. The OSPF protocol defines a number of activities to accomplish this information exchange:

Discovering neighbors

Electing a designated router

Establishing adjacencies and synchronizing databases

The five OSPF packet types are used to support these information exchanges.

##### Discovering neighbors: The OSPF Hello protocol

The Hello protocol discovers and maintains relationships with neighboring routers. Hello packets are periodically sent out to each router interface. The packet contains the RID of other routers whose hello packets have already been received over the interface.

When a device sees its own RID in the hello packet generated by another router, these devices establish a neighbor relationship.

The hello packet also contains the router priority, DR identifier, and BDR identifier. These parameters are used to elect the DR on multi-access networks.

##### Electing a designated router

All multi-access networks must have a DR. A BDR can also be selected. The backup ensures there is no extended loss of routing capability if the DR fails.

The DR and BDR are selected using information contained in hello packets. The device with the highest OSPF router priority on a segment becomes the DR for that segment. The same process is repeated to select the BDR. In case of a tie, the router with the highest RID is selected. A router declared the DR is ineligible to become the BDR.

After elected, the DR and BDR proceed to establish adjacencies with all routers on the multi-access segment.

##### Establishing adjacencies and synchronizing databases

Neighboring routers are considered adjacent when they have synchronized their link state databases. A router does not develop an adjacency with every neighboring device. On multi-access networks, adjacencies are formed only with the DR and BDR. This is a two step process.

###### Step 1: Database exchange process

The first phase of database synchronization is the database exchange process.

This occurs immediately after two neighbors attempt to establish an adjacency. The process consists of an exchange of database description packets. The packets contain a list of the LSAs stored in the local database.

During the database exchange process, the routers form a master/subordinate relationship. The master is the first to transmit. Each packet is identified by a sequence number. Using this sequence number, the subordinate acknowledges each database description packet from the master. The subordinate also includes its own set of link state headers in the acknowledgements.

###### Step 2: Database loading

During the database exchange process, each router notes the link state headers for which the neighbor has a more current instance (all advertisements are time stamped). After the process is complete, each router requests the more current information from the neighbor. This request is made with a link state request packet.

When a router receives a link state request, it must reply with a set of link state update packets providing the requested LSA. Each transmitted LSA is acknowledged by the receiver. This process is similar to the reliable flooding procedure used to transmit topology changes throughout the network.

Every LSA contains an age field indicating the time in seconds since the origin of the advertisement. The age continues to increase after the LSA is installed in the topology database. It also increases during each hop of the flooding process. When the maximum age is reached, the LSA is no longer used to determining routing information and is discarded from the link state database. This age is also used to distinguish between two otherwise identical copies of an advertisement.

#### 5.6.3 OSPF neighbor state machine

The OSPF specification defines a set of neighbor states and the events that can cause a neighbor to transition from one state to another. A state machine is used to describe these transitions:

Down: This is the initial state. It indicates that no recent information has been received from any device on the segment.

Attempt: This state is used on non-broadcast networks. It indicates that a neighbor appears to be inactive. Attempts continue to reestablish contact.

Init: Communication with the neighbor has started, but bidirectional communication has not been established. Specifically, a hello packet was received from the neighbor, but the local router was not listed in the neighbor's hello packet.

2-way: Bidirectional communication between the two routers has been established. Adjacencies can be formed. Neighbors are eligible to be elected as designated routers.

ExStart: The neighbors are starting to form an adjacency.

Exchange: The two neighbors are exchanging their topology databases.

Loading: The two neighbors are synchronizing their topology databases.

Full: The two neighbors are fully adjacent and their databases are synchronized.

Network events cause a neighbor’s OSPF state to change. For example, when a router receives a hello packet from a neighboring device, the OSPF neighbor state changes from Down to Init. When bidirectional communication has been established, the neighbor state changes from Init to 2-Way. RFC 2328 contains a complete description of the events causing a state change.

##### OSPF virtual links and transit areas

Virtual links are used when a network does not support the standard OSPF network topology. This topology defines a backbone area that directly connects to each additional OSPF area. The virtual link addresses two conditions:

It can logically connect the backbone area when it is not contiguous.

It can connect an area to the backbone when a direct connection does not exist.

A virtual link is established between two ABRs sharing a common non-backbone area. The link is treated as a point-to-point link. The common area is known as a *transit area*. Figure 5-18 on page 208 illustrates the interaction between virtual links and transit areas when used to connect an area to the backbone.

*Figure 5-18 OSPF virtual link and transit areas*

Area 0

Area 1

Area 2

Transit Area

ABR

ABR

Virtual link

This diagram shows that area 1 does not have a direct connection to the backbone. Area 2 can be used as a transit area to provide this connection. A virtual link is established between the two ABRs located in area 2. Establishing this virtual link logically extends the backbone area to connect to area 1.

A virtual link is used only to transmit routing information. It does not carry regular traffic between the remote area and the backbone. This traffic, in addition to the virtual link traffic, is routed using the standard intra-area routing within the transit area.

#### 5.6.4 OSPF route redistribution

Route redistribution is the process of introducing external routes into an OSPF network. These routes can be either static routes or routes learned through another routing protocol. They are advertised into the OSPF network by an ASBR. These routes become OSPF external routes. The ASBR advertises these routes by flooding OSPF AS external LSAs throughout the entire OSPF network.

The routes describe an end-to-end path consisting of two portions:

External portion: This is the portion of the path external to the OSPF network. When these routes are distributed into OSPF, the ASBR assigns an initial cost. This cost represents the *external cost* associated with traversing the external portion of the path.

Internal portion: This is the portion of the path internal to the OSPF network. Costs for this portion of the network are calculated using standard OSPF algorithms.

OSPF differentiates between two types of external routes. They differ in the way the cost of the route is calculated. The ASBR is configured to redistribute the route as:

External type 1: The total cost of the route is the sum of the external cost and any internal OSPF costs.

External type 2: The total cost of the route is always the external cost. This ignores any internal OSPF costs required to reach the ASBR.

Figure 5-19 illustrates an example of the types of OSPF external routes.

*Figure 5-19 OSPF route redistribution*

**R1 Routing Table**

10.99.5.0/24

E1: Cost 60

or

E2: Cost 50

**R2 Routing Table**

10.99.5.0/24

E1: Cost 65

or

E2: Cost 50

R1

R2

(20)

(10)

(15)

OSPF

Network

ASBR

10.99.5.0/24

redistributed

with external cost 50

External

Internal

RIP

Network

10.99.5.0/24

In this example, the ASBR is redistributing the 10.99.5.0/24 route into the OSPF network. This subnet is located within the RIP network. The route is announced into OSPF with an external cost of 50. This represents the cost for the portion of the path traversing the RIP network:

If the ASBR redistributed the route as an E1 route, R1 will contain an external route to this subnet with a cost of 60 (50 + 10). R2 will have an external route with a cost of 65 (50 + 15).

If the ASBR redistributed the route as an E2 route, both R1 and R2 will contain an external route to this subnet with a cost of 50. Any costs associated with traversing segments within the OSPF network are not included in the total cost to reach the destination.

#### 5.6.5 OSPF stub areas

OSPF allows certain areas to be defined as a stub area. A stub area is created when the ABR connecting to a stub area excludes AS external LSAs from being flooded into the area. This is done to reduce the size of the link state database maintained within the stub area routers. Because there are no specific routes to external networks, routing to these destinations is based on a default route generated by the ABR. The link state databases maintained within the stub area contain only the default route and the routes from within the OSPF environment (for example, intra-area and inter-area routes).

Because a stub area does not allow external LSAs, a stub area cannot contain an ASBR. No external routes can be generated from within the stub area.

Stub areas can be deployed when there is a single exit point connecting the area to the backbone. An area with multiple exit points can also be a stub area. However, there is no guarantee that packets exiting the area will follow an optimal path. This is due to the fact that each ABR generates a default route. There is no ability to associate traffic with a specific default routes.

All routers within the area must be configured as stub routers. This configuration is verified through the exchange of hello packets.

##### Not-so-stubby areas

An extension to the stub area concept is the *not-so-stubby area* (NSSA). This alternative is documented in RFC 3101. An NSSA is similar to a stub area in that the ABR servicing the NSSA does not flood any external routes into the NSSA. The only routes flooded into the NSSA are the default route and any other routes from within the OSPF environment (for example, intra-area and inter-area).

However, unlike a stub area, an ASBR can be located within an NSSA. This

ASBR can generate external routes. Therefore, the link state databases

maintained within the NSSA contain the default route, routes from within the OSPF environment (for example, intra-area and inter-area routes), and the external routes generated by the ASBR within the area.

The ABR servicing the NSSA floods the external routes from within the NSSA throughout the rest of the OSPF network.

#### 5.6.6 OSPF route summarization

Route summarization is the process of consolidating multiple contiguous routing entries into a single advertisement. This reduces the size of the link state database and the IP routing table. In an OSPF network, summarization is performed at a border router. There are two types of summarization:

Inter-area route summarization: Inter-area summarization is performed by the ABR for an area. It is used to summarize route advertisements originating within the area. The summarized route is announcement into the backbone. The backbone receives the aggregated route and announces the summary into other areas.

External route summarization: This type of summarization applies specifically to external routes injected into OSPF. This is performed by the ASBR distributing the routes into the OSPF network. Figure 5-20 illustrates an example of OSPF route summarization.

*Figure 5-20 OSPF route summarization*

**OSPF**

**Area 1**

ASBR

10.99.192.0/24

through

10.99.254.0/24

RIP

Network

10.99.0.0/24

through

10.99.83.0/24

ABR

R1

**OSPF Area 2**

10.99.0.0/28

10.99.192.0/28

**OSPF**

**Area 0**

External Summary

10.99.0.0/28

Inter-area Summary

10.99.192.0/28

In this figure, the ASBR is advertising a single summary route for the 64 subnetworks located in the RIP environment. This single summary route is flooded throughout the entire OSPF network. In addition, the ABR is generating a single summary route for the 64 subnetworks located in area 1. This summary route is flooded through area 0 and area 2. Depending of the configuration of the ASBR, the inter-area summary route can also be redistributed into the RIP network.

### 5.7 Enhanced Interior Gateway Routing Protocol (EIGRP)

The Enhanced Interior Gateway Routing Protocol (EIGRP) is categorized as a hybrid routing protocol. Similar to a distance vector algorithm, EIGRP uses metrics to determine network paths. However, like a link state protocol, topology updates in an EIGRP environment are event driven.

EIGRP, as the name implies, is an interior gateway protocol designed for use within an AS. In properly designed networks, EIGRP has the potential for improved scalability and faster convergence over standard distance vector algorithms. EIGRP is also better positioned to support complex, highly redundant networks.

EIGRP is a proprietary protocol developed by Cisco Systems, Inc. At the time of this writing, it is not an IETF standard protocol.

#### 5.7.1 Features of EIGRP

EIGRP has several capabilities. Some of these capabilities are also available in distance vector or link state algorithms.

EIGRP maintains a list of alternate routes that can be used if a preferred path fails. When the path fails, the new route is immediately installed in the IP routing table. No route recomputation is performed.

EIGRP allows partial routing updates. When EIGRP discovers a neighboring router, each device exchanges their entire routing table. After the initial information exchange, only routing table changes are propagated. There is no periodic rebroadcasting of the entire routing table.

EIGRP uses a low amount of bandwidth. During normal network operations, only hello packets are transmitted through a stable network.

EIGRP supports supernetting (CIDR) and variable length subnet masks (VLSM). This enables the network administrator to efficiently allocate IP address resources.

EIGRP supports the ability to summarize routing annoucements. This limits the advertisement of unnecessary subnet information.

EIGRP can provide network layer routing for multiple protocols such as AppleTalk, IPX, and IP networks.

EIGRP supports the simultaneous use of multiple unequal cost paths to a destination. Each route is installed in the IP routing table. EIGRP also intelligently load balances traffic over the multiple paths.

EIGRP uses a topology table to install routes into the IP routing table. The topology table lists all destination networks currently advertised by neighboring routers. The table contains all the information needed to build a set of distances and vectors to each destination.

EIGRP maintains a table to track the state of each adjacent neighbor. This is called a neighbor table.

EIGRP can guarantee the ordered delivery of packets to a neighbor. However, not all types of packets must be reliably transmitted. For example, in a network that supports multicasting, there is no need to send individual, acknowledged hello packets to each neighbor. To provide efficient operation, reliability is provided only when needed. This improves convergence time in networks containing varying speed connections.

##### Neighbor discovery and recovery

EIGRP can dynamically learn about other routers on directly attached networks. This is similar to the Hello protocol used for neighbor discovery in an OSPF environment.

Devices in an EIGRP network exchange hello packets to verify each neighbor is operational. Like OSPF, the frequency used to exchange packets is based on the network type. Packets are exchanged at a five second interval on high bandwidth links (for example, LAN segments). Otherwise, hello packets on lower bandwidth connections are exchanged every 60 seconds.

Also like OSPF, EIGRP uses a hold timer to remove inactive neighbors. This timer indicates the amount of time that a device will continue to consider a neighbor active without receiving a hello packet from the neighbor.

##### EIGRP routing algorithm

EIGRP does not rely on periodic updates to converge on the topology. Instead, it builds a topology table containing each of its neighbor’s advertisements. Unlike a distance vector protocol, this data is not discarded.

EIGRP processes the information in the topology table to determine the best paths to each destination network. EIGRP implements an algorithm known as Diffusing Update ALgorithm (DUAL).

##### Route recomputation

For a specific destination, the successor is the neighbor router currently used for packet forwarding. This device has the least-cost path to the destination and is guaranteed not to be participating in a routing loop. A feasible successor assumes forwarding responsibility when the current successor router fails. The set of feasible successors represent the devices that can become a successor without requiring a route recomputation or introducing routing loops.

A route recomputation occurs when there is no known feasible successor to the destination. The successor is the neighbor router currently used for packet forwarding. The process starts with a router sending a multicast query packet to determine if any neighbor is aware of a feasible successor to the destination. A neighbor replies if it has an feasible successor.

If the neighbor does not have a feasible successor, the neighbor can return a query indicating it also is performing a route recomputation. When the link to a neighbor fails, all routes that used that neighbor as the only feasible successor require a route recomputation.

#### 5.7.2 EIGRP packet types

EIGRP uses five types of packets to establish neighbor relationships and advertise routing information:

Hello/acknowledgement: These packets are used for neighbor discovery. They are multicast advertised on each network segment. Unicast responses to the hello packet are returned. A hello packet without any data is considered an acknowledgement.

Updates: These packets are used to convey reachability information for each destination. When a new neighbor is discovered, unicast update packets are exchanged to allow each neighbor to build their topology table. Other types of advertisements (for example, metric changes) use multicast packets. Update packets are always transmitted reliably.

Queries and replies: These packets are exchanged when a destination enters an active state. A multicast query packet is sent to determine if any neighbor contains a feasible successor to the destination. Unicast reply packets are sent to indicate that the neighbor does not need to go into an active state because a feasible successor has been identified. Query and reply packets are transmitted reliably.

Request: These packets are used to obtain specific information from a neighbor. These packets are used in route server applications.

### 5.8 Exterior Gateway Protocol (EGP)

EGP is an exterior gateway protocol of historical merit. It was one of the first protocols developed for communication between autonomous systems. It is described in RFC 904.

EGP assumes the network contains a single backbone and a single path exists between any two autonomous systems. Due to this limitation, the current use of EGP is minimal. In practice, EGP has been replaced by BGP.

EGP is based on periodic polling using a hello/I-hear-you message exchange.

These are used to monitor neighbor reachability and solicit update responses.

The gateway connecting to an AS is permitted to advertise only those destination networks reachable within the local AS. It does not advertise reachability information about its EGP neighbors outside the AS.

### 5.9 Border Gateway Protocol (BGP)

The Border Gateway Protocol (BGP) is an exterior gateway protocol. It was originally developed to provide a loop-free method of exchanging routing information between autonomous systems. BGP has since evolved to support aggregation and summarization of routing information.

BGP is an IETF draft standard protocol described in RFC 4271. The version described in this RFC is BGP Version 4. Following standard convention, this document uses the term BGP when referencing BGP Version 4.

#### 5.9.1 BGP concepts and terminology

BGP uses specific terminology to describe the operation of the protocol. Figure 5-21 illustrates this terminology.

AS1

AS2

AS3

ASX

OSPF/RIP

OSPF/RIP

OSPF/RIP

OSPF/RIP

OSPF/RIP

OSPF/RIP

OSPF/RIP

BGP Speaker

OSPF/RIP

BGP Speaker

OSPF/RIP

BGP Speaker

OSPF/RIP

BGP Speaker

OSPF/RIP

BGP Speaker

IBGP

IBGP

EBGP

EBGP

EBGP

*Figure 5-21 Components of a BGP network*

BGP uses the following terms:

BGP speaker: A router configured to support BGP.

BGP neighbors (peers): A pair of BGP speakers that exchange routing information. There are two types of BGP neighbors:

* Internal (IBGP) neighbor: A pair of BGP speakers within the same AS.
* External (EBGP) neighbor: A pair of BGP neighbors, each in a different

AS. These neighbors typically share a directly connected network.

BGP session: A TCP session connecting two BGP neighbors. The session is used to exchange routing information. The neighbors monitor the state of the

session by sending keepalive messages.1

Traffic type: BGP defines two types of traffic:

* Local: Traffic local to an AS either originates or terminates within the AS. Either the source or the destination IP address resides in the AS.
* Transit: Any traffic that is not local traffic is transit traffic. One of the goals of BGP is to minimize the amount of transit traffic.

AS type: BGP defines three types of autonomous systems:

* Stub: A stub AS has a single connection to one other AS. A stub AS carries only local traffic.
* Multihomed: A multihomed AS has connections to two or more autonomous systems. However, a multihomed AS has been configured so that it does not forward transit traffic.
* Transit: A transit AS has connections to two or more autonomous systems and carries both local and transit traffic. The AS can impose policy restrictions on the types of transit traffic that will be forwarded.

Depending on the configuration of the BGP devices within AS 2 in Figure 5-21 on page 216, this autonomous system can be either a multihomed AS or a transit AS.

AS number: A 16-bit number uniquely identifying an AS.

AS path: A list of AS numbers describing a route through the network. A BGP neighbor communicates paths to its peers.

Routing policy: A set of rules constraining the flow of data packets through the network. Routing policies are not defined in the BGP protocol. Rather, they are used to configure a BGP device. For example, a BGP device can be configured so that:

* A multihomed AS can refuse to act as a transit AS. This is accomplished by advertising only those networks contained within the AS.
* A multihomed AS can perform transit AS routing for a restricted set of adjacent autonomous systems. It does this by tailoring the routing advertisements sent to EBGP peers.
* An AS can optimize traffic to use a specific AS path for certain categories of traffic.

Network layer reachability information (NLRI): NLRI is used by BGP to advertise routes. It consists of a set of networks represented by the tuple

<length,prefix>. For example, the tuple <14,220.24.106.0> represents the CIDR route 220.24.106.0/14.

1 This keepalive message is implemented in the application layer. It is independent of the keepalive message available in many TCP implementations.

Routes and paths: A route associates a destination with a collection of attributes describing the path to the destination. The destination is specified in NRLI format. The path is reported as a collection of path attributes. This information is advertised in UPDATE messages. For additional information describing the UPDATE message, see 5.9.3, “Protocol description” on page 220.

#### 5.9.2 IBGP and EBGP communication

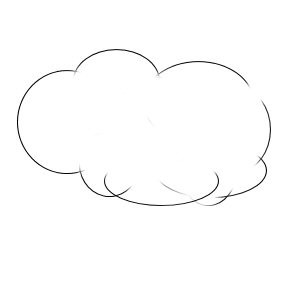
BGP does not replace the IGP operating within an AS. Instead, it cooperates with the IGP to establish communication between autonomous systems. BGP within an AS is used to advertise the local IGP routes. These routes are advertised to BGP peers in other autonomous systems. Figure 5-22 on page 219 illustrates the communication that occurs between BGP peers. This example shows four autonomous systems. AS 2, AS 3, and AS 4 each have an EBGP connection to AS 1. A full mesh of IBGP sessions exists between BGP devices within AS 1.

Network 10.0.0.0/8 is located within AS 3. Using BGP, the existence of this network is advertised to the rest of the environment:

R4 in AS 3 uses its EBGP connection to announce the network to AS 1.

R1 in AS 1 uses its IBGP connections to announce the network to R2 and R3.

R2 in AS 1 uses its EBGP session to announce the network into AS 2. R3 in AS 1 uses its EBGP session 5 to announce the network into AS 4.



BGP

R6

**AS 2**

BGP

R5

**AS 4**

BGP

R4

10.0.0.0/8

**AS 3**

BGP

R2

**AS 1**

BGP

R1

BGP

R3

IGP

Interconnection

IBGP

IBGP

IBGP

EBGP

EBGP

EBGP

*Figure 5-22 EBGP and IBGP communication*

Several additional operational issues are shown in Figure 5-22:

Role of BGP and the IGP: The diagram shows that while BGP alone carries information between autonomous systems, both BGP and the IGP are used to carry information through an AS.

Establishing the TCP session between peers: Before establishing a BGP session, a device verifies that routing information is available to reach the peer:

* EBGP peers: EBGP peers typically share a directly connected network. The routing information needed to exchange BGP packets between these peers is trivial.
* IBGP peers: IBGP peers can be located anywhere within the AS. They do not need to be directly connected. BGP relies on the IGP to locate a peer.

Packet forwarding between IBGP peers uses IGP-learned routes.

Full mesh of BGP sessions within an AS: IBGP speakers assume a full mesh of BGP sessions have been established between peers in the same AS. In Figure 5-22 on page 219, all three BGP peers in AS 1 are interconnected with BGP sessions.

When a BGP speaker receives a route update from an IBGP peer, the receiving speaker uses EBGP to propagate the update to external peers. Because the receiving speaker assumes a full mesh of IBGP sessions have been established, it does not propagate the update to other IBGP peers.

For example, assume that there was no IBGP session between R1 and R3 in Figure\_82. R1 receives the update about 10.0.0.0/8 from AS 3. R1 forwards the update to its BGP peers, namely R2. R2 receives the IBGP update and forwards it to its EBGP peers, namely R6. No update is sent to R3. If R3 needs to receive this information, R1 and R3 must be configured to be BGP peers.

#### 5.9.3 Protocol description

BGP establishes a reliable TCP connection between peers. Sessions are established using TCP port 179. BGP assumes the transport connection will manage fragmentation, retransmission, acknowledgement, and sequencing.

When two speakers initially form a BGP session, they exchange their entire routing table. This routing information contains the complete AS path used to reach each destination. The information avoids the routing loops and counting-to-infinity behavior observed in RIP networks. After the entire table has been exchanged, changes to the table are communicated as incremental updates.

##### BGP packet types

All BGP packets contain a standard header. The header specifies the BGP packet type. The valid BGP packet types include:

OPEN[[2]](#footnote-2): This message type establishes a BGP session between two peer nodes.

UPDATE: This message type transfers routing information between GP peers.

NOTIFICATION: This message is sent when an error condition is detected.

KEEPALIVE: This message determines if peers are reachable.

Figure 5-23 shows the flow of these message types between two autonomous systems.

BGP

BGP

ASY

BGP

ASX

Open

Keep Alive

Update

Notification

*Figure 5-23 BGP message flows between BGP speakers*

##### Opening and confirming a BGP connection

After a TCP session has been established between two peer nodes, each router sends an OPEN message to the neighbor. The OPEN message includes:

The originating router's AS number and BGP router identifier.

A suggested value for the hold timer. We discuss the function of this timer in the next section.

Optional parameters. This information is used to authenticate a peer.

An OPEN message contains support for authenticating the identity of a BGP peer. However, the BGP standard does not specify a specific authorization mechanism. This allows BGP peers to select any supported authorization scheme.

An OPEN message is acknowledged by a KEEPALIVE message. After peer routers have established a BGP connection, they can exchange additional information.

##### Maintaining the BGP connection

BGP does not use any transport-based keepalive to determine if peers are reachable. Instead, BGP messages are periodically exchanged between peers. If no messages are received from the peer for the duration specified by the hold timer, the originating router assumes that an error has occurred. When this happens, an error notification is sent to the peer and the connection is closed.

RFC 4271 recommends a 90 second hold timer and a 30 second keepalive timer.

##### Sending reachability information

Reachability information is exchanged between peers in UPDATE messages.

BGP does not require a periodic refresh of the entire BGP routing table. Therefore, each BGP speaker must retain a copy of the current BGP routing table used by each peer. This information is maintained for the duration of the connection. After neighbors have performed the initial exchange of complete routing information, only incremental updates to that information are exchanged.

An UPDATE message is used to advertise feasible routes or withdraw infeasible routes. The message can simultaneously advertise a feasible route and withdraw multiple infeasible routes from service. Figure 5-24 depicts the format of an UPDATE message:

Network layer reachability information (NLRI).

Path attributes (we discuss path attributes in “Path attributes” on page 223.

Withdrawn routes.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Number of Octets   |  |  | | --- | --- | | Common Header |  | | Unfeasible Routes Length | | Withdrawn Routes | | Total Path Attribute Length | | Path Attributes | | Network Layer Reachability Information | |  |   19Type = 2  2  Variable  2  Variable  Variable |

*Figure 5-24 BGP UPDATE message*

Several path attributes can be used to describe a route.

###### Withdrawn routes

The unfeasible routes length field indicates the total length of the withdrawn routes field.

The withdrawn routes field provides a list of IP addresses prefixes that are not feasible or are no longer in service. These addresses need to be withdrawn from the BGP routing table. The withdrawn routes are represented in the same tuple-format as the NLRI.

##### Notification of error conditions

A BGP device can observe error conditions impacting the connection to a peer. NOTIFICATION messages are sent to the neighbor when these conditions are detected. After the message is sent, the BGP transport connection is closed. This means that all resources for the BGP connection are deallocated. The routing table entries associated with the remote peer are marked as invalid. Finally, other peers are notified that these routes are invalid.

Notification messages include an error code and an error subcode.The error codes provided by BGP include:

Message header error

OPEN message error

UPDATE message error

Hold timer expired

Finite state machine error

Cease

The error subcode further qualifies the specific error. Each error code can have multiple subcodes associated with it.

#### 5.9.4 Path selection

BGP is a path vector protocol. In path vector routing, the path is expressed in terms of the domains (or confederations) traversed so far. The best path is obtained by comparing the number of domains of each feasible route. However, inter-AS routing complicates this process. There are no universally agreed-upon metrics that can be used to evaluate external paths. Each AS has its own set of criteria for path evaluation.

##### Path attributes

Path attributes are used to describe and evaluate a route. Peers exchange path attributes along with other routing information. When a device advertises a route,

it can add or modify the path attributes before advertising the route to a peer. The combination of attributes are used to select the best path.

Each path attribute is placed into one of four separate categories:

Well-known mandatory: The attribute must be recognized by all BGP implementations. It must be sent in every UPDATE message.

Well-known discretionary: The attribute must be recognized by all BGP implementations. However, it is not required to be sent in every UPDATE message.

Optional transitive: It is not required that every BGP implementation recognize this type of attribute. A path with an unrecognized optional transitive attribute is accepted and simply forwarded to other BGP peers.

Optional non-transitive: It is not required that every BGP implementation recognize this type of attribute. These attributes can be ignored and not passed along to other BGP peers.

BGP defines seven attribute types to define an advertised route:

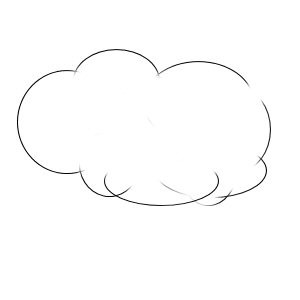
ORIGIN: This attribute defines the origin of the path information. Valid selections are IGP (interior to the AS), EGP, or INCOMPLETE. This is a well-known mandatory attribute.

AS\_PATH: This attribute defines the set of autonomous systems that must be traversed to reach the advertised network. Each BGP device prepends its AS number onto the AS path sequence before sending the routing information to an EBGP peer. Using the sample network depicted in Figure 5-22 on page 219, R4 advertises network 10.0.0.0 with an AS\_PATH of 3. When the update traverses AS 1, R2 prepends its own AS number to it. When the routing update reaches R6, the AS\_PATH attribute for network 10.0.0.0 is <1 3>. This is a well-known mandatory attribute.

NEXT\_HOP: This attribute defines the IP address of the next hop used to reach the destination. This is a well-known mandatory attribute.

For routing updates received over EBGP connections, the next hop is typically the IP address of the EBGP neighbor in the remote AS. BGP specifies that this next hop is passed without modification to each IBGP neighbor. As a result, each IBGP neighbor must have a route to reach the neighbor in the remote AS. Figure 5-25 on page 225 illustrates this interaction.

*Figure 5-25 NEXT\_HOP attribute*



AS 1

AS 3

BGP

R1

BGP

R3

BGP

R4

172.16.1.2

172.16.1.1

10.0.0.0/8

EBGP

IBGP

In this example, when a routing update for network 10.0.0.0/8 is sent from AS 3, R1 receives the update with the NEXT\_HOP attribute set to 172.16.1.1.

When this update is forwarded to R3, the next hop address remains 172.16.1.1. R3 must have appropriate routing information to reach this address. Otherwise, R3 will drop packets destined for AS 3 if the next hop is inaccessible.

MULTI\_EXIT\_DISC (multi-exit discriminator, MED): This attribute is used to discriminate among multiple exit points to a neighboring AS. If this information is received from an EBGP peer, it is propagated to each IBGP peer. This attribute is not propagated to peers in other autonomous systems. If all other attributes are equal, the exit point with the lowest MED value is preferred. This is an optional non-transitive attribute. MED is discussed further in RFC 4451.

LOCAL\_PREF (local preference): This attribute is used by a BGP speaker to inform other speakers within the AS of the originating speaker's degree of preference for the advertised route. Unlike MED, this attribute is used only within an AS. The value of the local preference is not distributed outside an AS. If all other attributes are equal, the route with the higher degree of preference is preferred. This is a well-known discretionary attribute.

ATOMIC\_AGGREGATE: This attribute is used when a BGP peer receives advertisements for the same destination identified in multiple, non-matching routes (that is, overlapping routes). One route describes a smaller set of destinations (a more specific prefix), other routes describe a larger set of destinations (a less specific prefix). This attribute is used by the BGP speaker to inform peers that it has selected the less specific route without selecting the more specific route. This is a well-known discretionary attribute. A route with this attribute included may actually traverse autonomous systems not listed in the AS\_PATH.

AGGREGATOR: This attribute indicates the last AS number that formed the aggregate route, followed by the IP address of the BGP speaker that formed the aggregate route. For further information about route aggregation, refer to

5.9.6, “BGP aggregation” on page 228. This is an optional transitive attribute.

##### Decision process

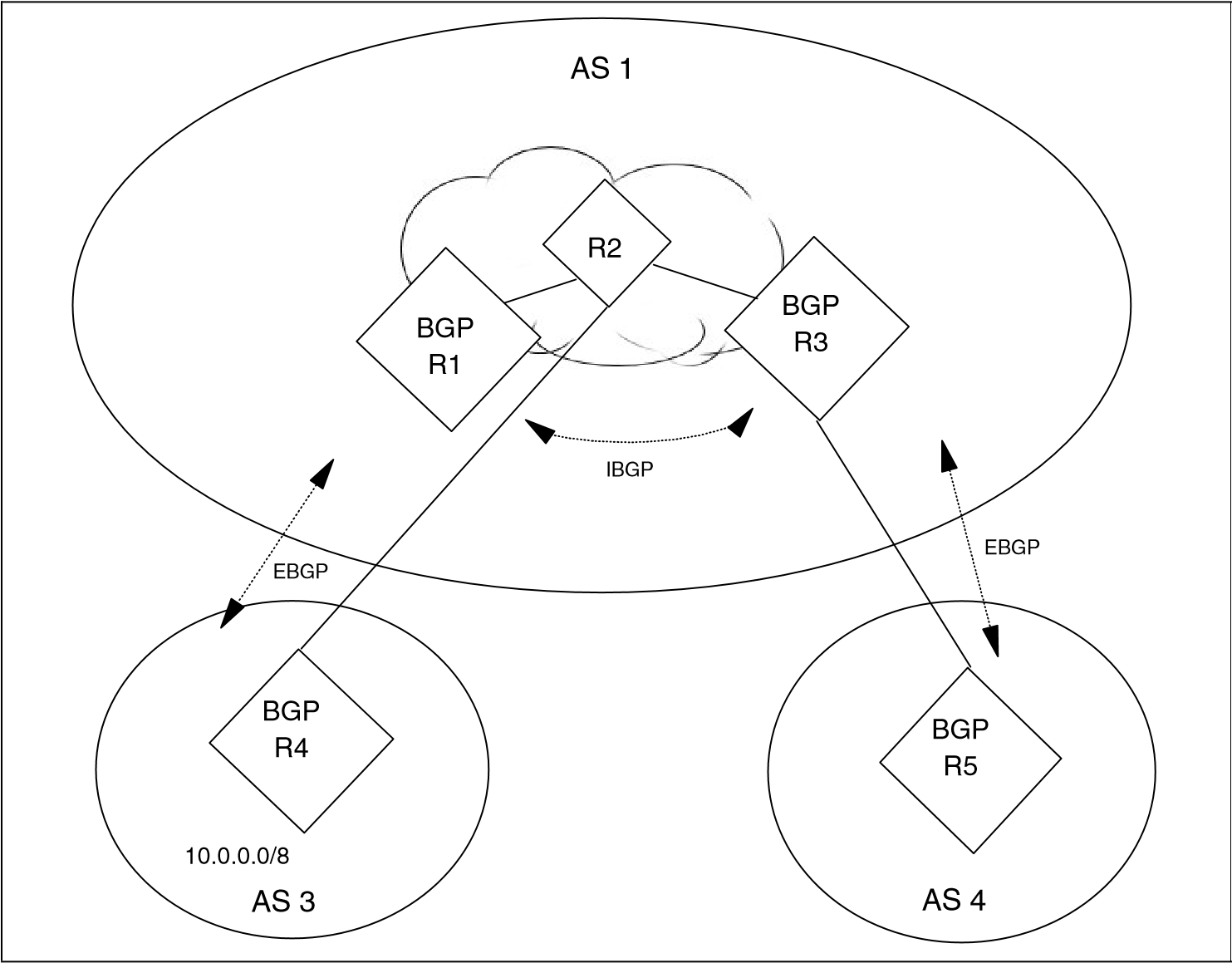
The process to select the best path uses the path attributes describing each route. The attributes are analyzed and a *degree of preference* is assigned. Because there can be multiple paths to a given destination, the route selection process determines the degree of preference for each feasible route. The path with the highest degree of preference is selected as the best path. This is the path advertised to each BGP neighbor. Route aggregation can also be performed during this process. Where there are multiple paths to a destination, BGP tracks each individual path. This allows faster convergence to the alternate path when the primary path fails.

#### 5.9.5 BGP synchronization

Figure 5-26 on page 227 shows an example of an AS providing transit service. In this example, AS 1 is used to transport traffic between AS 3 and AS 4. Within AS 1, R2 is not configured for BGP. However, R2 is used for communication between R1 and R3. Traffic between these two BGP nodes physically traverses through R2.

Using the routing update flow described earlier, the 10.0.0.0/8 network is advertised using the EBGP connection between R4 and R1. R1 passes the network advertisement to R3 using its existing IBGP connection. Because R2 is not configured for BGP, it is unaware of any networks in AS 3. A problem occurs if R3 needs to communicate with a device in AS 3. R3 passes the traffic to R2. However, because R2 does not have any routes to AS 3 networks, the traffic is dropped.

If R3 advertises the 10.0.0.0/8 network to AS 4, the problem continues. If AS 4 needs to communicate with a device in AS 3, the packets are forwarded from R5 to R3. R3 forwards the packets to R2 where they are discarded.



*Figure 5-26 BGP synchronization*

This situation is addressed by the synchronization rule of BGP. The rule states that a transit AS will not advertise a route before all routers within the AS have learned about the route. In this example, R3 will not advertise the existence of the networks in AS 3 until R2 has built a proper routing table.

There are three methods to implement the synchronization rule:

Enable BGP on all devices within the transit AS. In this solution, R2 has an IBGP session with both R1 and R3. R2 learns of the 10.0.0.0/8 network at the same time it is advertised to R3. At that time, R3 announces the routes to its peer in AS 4.

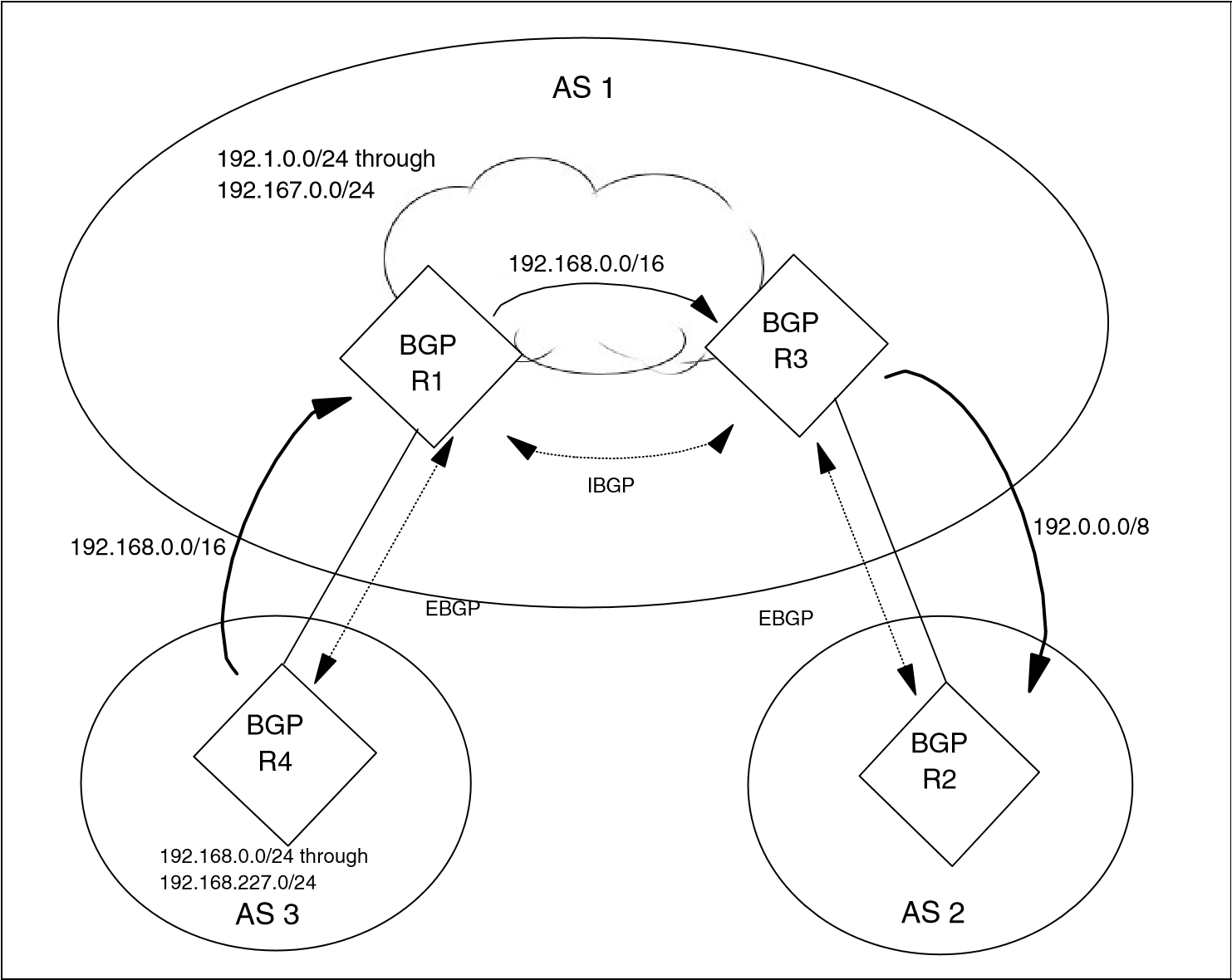
Redistribute the routes into the IGP used within the transit area. In this solution, R1 redistributes the 10.0.0.0/8 network into the IGP within AS 1. R3 learns of the network through two routing protocols: BGP and the IGP. After

R3 learns of the network through the IGP, it is certain that other routers within the AS have also learned of the routes. At that time, R3 announces the routes to its peer in AS 4.

Encapsulate the transit traffic across the AS. In this solution, transit traffic is encapsulated within IP datagrams addressed to the exit gateway. Because this does not require the IGP to carry exterior routing information, no synchronization is required between BGP and the IGP. R3 can immediately announce the routes to its peer in AS 4.

#### 5.9.6 BGP aggregation

The major improvement introduced in BGP Version 4 was support for CIDR and route aggregation. These features allow BGP peers to consolidate multiple contiguous routing entries into a single advertisement. It significantly enhances the scalability of BGP into large internetworking environments. Figure 5-27 on page 229 illustrates these functions.



*Figure 5-27 BGP route aggregation*

This diagrams depicts three autonomous systems interconnected by BGP. In this example, networks 192.168.0.0 through 182.168.227.0 are located within AS 3. To reduce the size of routing announcements, R4 aggregates these individual networks into a single route entry prior to advertising into AS 1. The single entry 192.168.0.0/16 represents a valid CIDR supernet even though it is an illegal Class C network.

BGP aggregate routes contain additional information within the AS\_PATH path attribute. When aggregate entries are generated from a set of more specific routes, the AS\_PATH attributes of the more specific routes are combined. For example, in Figure 5-27, the aggregate route 192.0.0.0/8 is announced from AS 1 into AS 2. This aggregate represents the set of more specific routes deployed within AS 1 and AS 3. When this aggregate route is sent to AS 2, the

AS\_PATH attribute consists of <1 3>. This is done to prevent routing information

loops. A loop can occur if AS 1 generated an aggregate with an AS\_PATH attribute of <1>. If AS 2 had a direct connection to AS 3, the route with the less-specific AS\_PATH advertised from AS 1 can generate a loop. This is because AS 2 does not know this aggregate contains networks located within

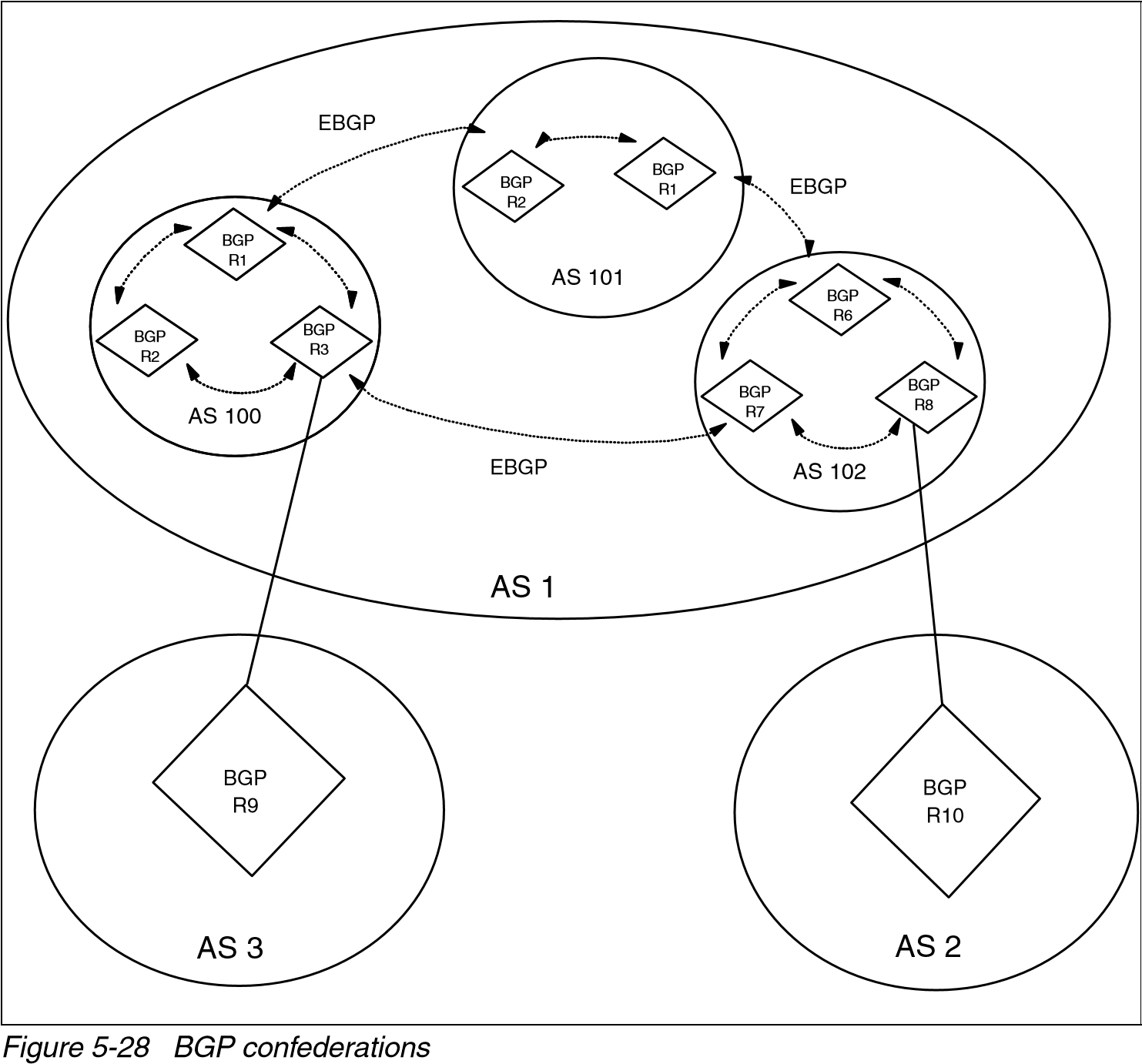
AS 3.

#### 5.9.7 BGP confederations

BGP requires that all speakers within a single AS have a fully meshed set of IBGP connections. This can be a scaling problem in networks containing a large number of IBGP peers. The use of BGP confederations addresses this problem.

A BGP confederation creates a set of autonomous systems that represent a single AS to peers external to the confederation. This removes the full mesh requirement and reduces management complexity.

Figure 5-28 illustrates the operation of a BGP confederation. In this sample network, AS 1 contains eight BGP speakers. A standard BGP network would require 28 IBGP sessions to fully mesh the speakers.



A confederation divides the AS into a set of domains. In this example, AS 1 contains three domains. Devices within a domain have a fully meshed set of IBGP connections. Each domain also has an EBGP connection to other domains within the confederation. In the example network, R1, R2, and R3 have fully meshed IBGP sessions. R1 has an EBGP session within the confederation to R4. R3 has an EBGP session outside the confederation to R9.

Each router in the confederation is assigned a confederation ID. A member of the confederation uses this ID in all communications with devices outside the confederation. In this example, each router is assigned a confederation ID of AS 1.

All communications from AS 1 to AS 2 or AS 3 appear to have originated from the confederation ID of AS 1. Even though communication between domains within a confederation occurs with EBGP, the domains exchange routing updates as though they were connected by IBGP. Specifically, the information contained in the NEXT\_HOP, MULTI\_EXIT\_DESC, and LOCAL\_PREF attributes is preserved between domains. The confederation appears to be a single AS to other autonomous systems.

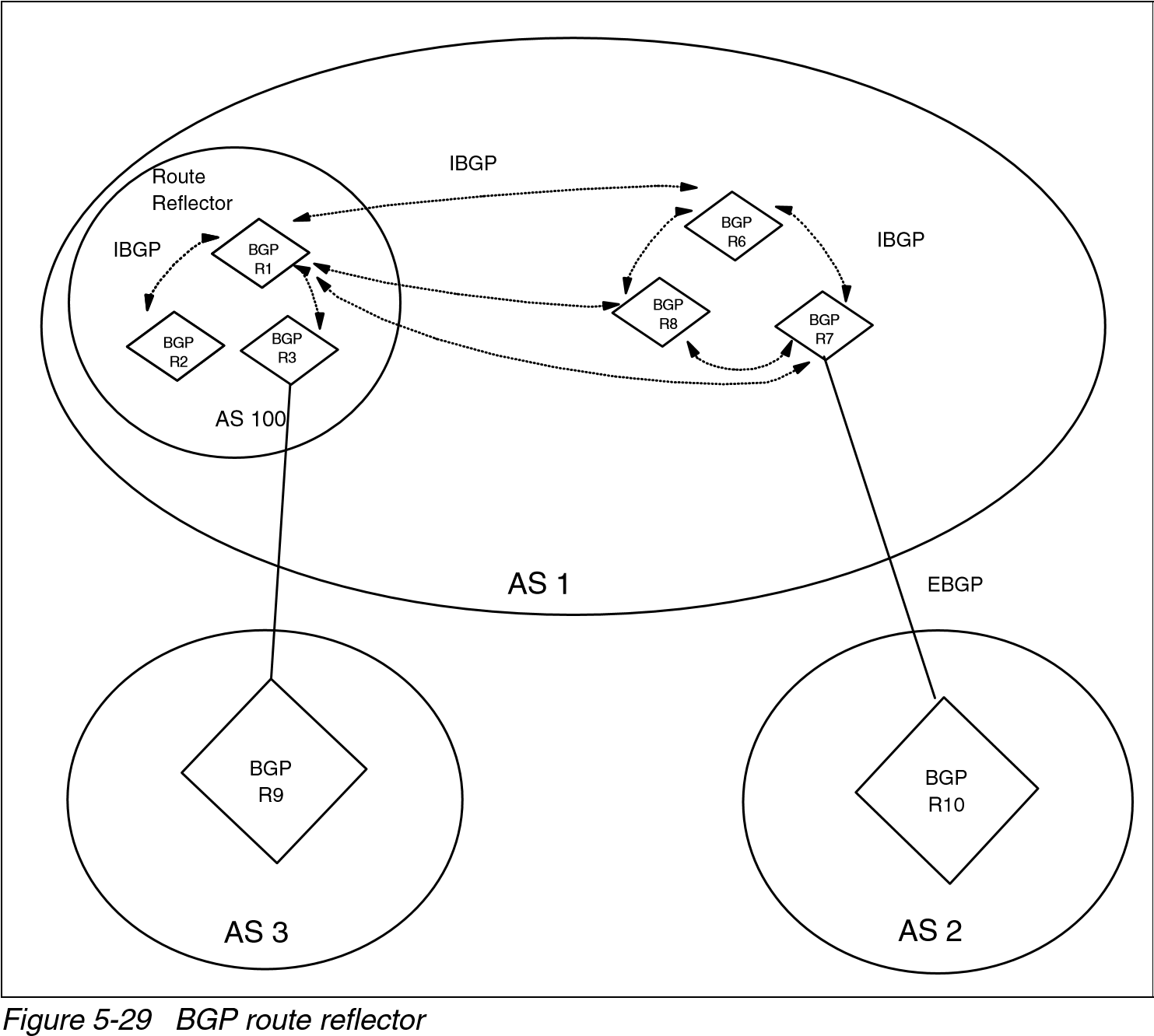
BGP confederations are described in RFC 3065. At the time of this writing, this is a proposed standard. Regardless, BGP confederations have been widely deployed throughout the Internet. Numerous vendors support this feature.

#### 5.9.8 BGP route reflectors

Route reflectors are another solution to address the requirement for a full mesh of IBGP sessions between peers in an AS. As noted previously, when a BGP speaker receives an update from an IBGP peer, the receiving speaker propagates the update only to EBGP peers. The receiving speaker does not forward the update to other IBGP peers.

Route reflectors relax this restriction. BGP speakers are permitted to advertise IBGP learned routes to certain IBGP peers. Figure 5-29 on page 232 depicts an environment using route reflectors. R1 is configured as a route reflector for R2 and R3. R2 and R3 are route reflector clients of R1. No IBGP session is defined between R2 and R3. When R3 receives an EBGP update from AS 3, it is passed to R1 using IBGP. Because R1 is configured as a reflector, R1 forwards the IBGP update to R2.

Figure 5-29 also illustrates the interaction between route reflectors and conventional BGP speakers within an AS.



In Figure 5-29, R1, R2, and R3 are in the route reflector domain. R6, R7, and R8 are conventional BGP speakers containing a full mesh of IBGP peer connections. In addition, each of these speakers is peered with the route reflector. This configuration permits full IBGP communication within AS 1.

Although not shown in Figure 5-29, an AS can contain more than one route reflector. When this occurs, each reflector treats other reflectors as a conventional IBGP peer.

Route reflectors are described inRFC 4456. At the time of this writing, this is a proposed standard.

### 5.10 Routing protocol selection

The choice of a routing protocol is a major decision for the network administrator.

It has a major impact on overall network performance. The selection depends on network complexity, size, and administrative policies.

The protocol chosen for one type of network might not be appropriate for other types of networks. Each unique environment must be evaluated against a number of fundamental design requirements:

Scalability to large environments: The potential growth of the network dictates the importance of this requirement. If support is needed for large, highly-redundant networks, consider link state or hybrid algorithms. Distance vector algorithms do not scale into these environments.

Stability during outages: Distance vector algorithms might introduce network instability during outage periods. The counting to infinity problems (5.3.5, “Convergence and counting to infinity” on page 185) can cause routing loops or other non-optimal routing paths. Link state or hybrid algorithms reduce the potential for these problems.

Speed of convergence: Triggered updates provide the ability to immediately initiate convergence when a failure is detected. All three types of protocols support this feature. One contributing factor to convergence is the time required to detect a failure. In OSPF and EIGRP networks, a series of hello packets must be missed before convergence begins. In RIP environments, subsequent route advertisements must be missed before convergence in initiated. These detection times increase the time required to restore communication.

Metrics: Metrics provide the ability to groom appropriate routing paths through the network. Link state algorithms consider bandwidth when calculating routes. EIGRP improves this to include network delay in the route calculation.

Support for VLSM: The availability of IP address ranges dictates the importance of this requirement. In environments with an constrained supply of addresses, the network administrator must develop an addressing scheme that intelligently overlays the network. VLSM is a major component of this plan. The use of private addresses ranges can also address this concern.

Vendor interoperability: The types of devices deployed in a network indicate the importance of this requirement. If the network contains equipment from a number of vendors, use standard routing protocols. The IETF has dictated the operating policies for the distance vector and link state algorithms described in this document. Implementing these algorithms avoids any interoperability problems encountered with nonstandard protocols.

Ease of implementation: Distance vector protocols are the simplest routing protocol to configure and maintain. Because of this, these protocols have the largest implementation base. Limited training is required to perform problem resolution in these environments.

In small, non-changing environments, static routes are also simple to implement. These definitions change only when sites are added or removed from the network. The administrator must assess the importance of each of these requirements when determining the appropriate routing protocol for an environment.

### 5.11 Additional functions performed by the router

The main functions performed by a router relate to managing the IP routing table and forwarding data. However, the router should be able to provide information alerting other devices to potential network problems.

This information is provided by the ICMP protocol described in 3.2, “Internet Control Message Protocol (ICMP)” on page 109. The information includes:

ICMP Destination Unreachable: The destination address specified in the IP packet references an unknown IP network.

ICMP Redirect: Redirect forwarding of traffic to a more suitable router along the path to the destination.

ICMP Source Quench: Congestion problems (for example, too many incoming datagrams for the available buffer space) have been encountered in a device along the path to the destination.

ICMP Time Exceeded: The Time-to-Live field of an IP datagram has reached zero. The packet is not able to be delivered to the final destination.

In addition, each IP router should support the following base ICMP operations and messages:

Parameter problem: This message is returned to the packet’s source if a problem with the IP header is found. The message indicates the type and location of the problem. The router discards the errored packet.

Address mask request/reply: A router must implement support for receiving ICMP Address Mask Request messages and responding with ICMP Address Mask Reply messages.

Timestamp: The router must return a Timestamp Reply to every Timestamp message that is received. It should be designed for minimum variability in delay. To synchronize the clock on the router, the UDP Time Server Protocol or the Network Time Protocol (NTP) can be used.

Echo request/reply: A router must implement an ICMP Echo server function that receives requests sent to the router and sends corresponding replies. The router can ignore ICMP Echo requests addressed to IP broadcast or IP multicast addresses.

### 5.12 Routing processes in UNIX-based systems

This chapter focuses on protocols available in standard IP routers. However, several of these protocols are also available in UNIX-based systems.

These protocols are often implemented using one of two processes:

Routed (pronounced route-D): This is a basic routing process for interior routing. It is supplied with the majority of TCP/IP implementations. It implements the RIP protocol.

Gated (pronounced gate-D): This is a more sophisticated process allowing for both interior and exterior routing. It can implement a number of protocols including OSPF, RIP-2, and BGP-4.

### 5.13 RFCs relevant to this chapter

The following RFCs provide detailed information about the connection protocols and architectures presented throughout this chapter:

[RFC 904 – Exterior Gateway Protocol formal specification (April 1984)](http://www.ietf.org/rfc/rfc904.txt)

[RFC 1058 – Routing Information Protocol (June 1988)](http://www.ietf.org/rfc/rfc1058.txt)

[RFC 1322 – A Unified Approach to Inter-Domain Routing (May 1992)](http://www.ietf.org/rfc/rfc1322.txt)

[RFC 1812 – Requirements for IP Version 4 Routers. (June 1995)](http://www.ietf.org/rfc/rfc1812.txt)

[RFC 2080 – RIPng for IPv6 (January 1997)](http://www.ietf.org/rfc/rfc2080.txt)

[RFC 2328 – OSPF Version 2 (April 1998)](http://www.ietf.org/rfc/rfc2328.txt)

[RFC 2453 – RIP Version 2 (November 1998)](http://www.ietf.org/rfc/rfc2453.txt)

[RFC 3065 – Autonomous System Confederations for BGP (February 2001)](http://www.ietf.org/rfc/rfc3065.txt)

[RFC 3101 – The OSPF Not-So-Stubby Area (NSSA) Option (January 2003)](http://www.ietf.org/rfc/rfc3101.txt)

[RFC 4271 – A Border Gateway Protocol 4 (BGP-4) (January 2006)](http://www.ietf.org/rfc/rfc4271.txt)

[RFC 4451 – BGP MULTI\_EXIT\_DISC (MED) Considerations (March 2006)](http://www.ietf.org/rfc/rfc4451.txt)

[RFC 4456 – BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP) (April 2006)](http://www.ietf.org/rfc/rfc4456.txt)

|  |  |  |
| --- | --- | --- |
|  | |  | | --- | | **12** | |

## Chapter 12. Directory and naming protocols

An inherent problem in making resources available through a network is creating an easy way of accessing these resources. On small networks, it might be easy enough to simply remember or write down the information needed to remotely access resources. However, this solution does not scale as networks, and the number of available resources, continue to grow. This becomes increasingly more complex as resources are made available outside of individual networks, to multiple networks, or even across the Internet, on multiple platforms and across a variety of differing hardware. To overcome this, directory and naming methods were devised to provide a uniform method of obtaining the information needed to access a networked resource. This chapter reviews four of these methods:

Domain Name System (DNS)

Dynamic Domain Name System (DDNS)

Network Information System (NIS)

Lightweight Directory Access Protocol (LDAP)

© Copyright IBM Corp. 1989-2006. All rights reserved.

### 12.1 Domain Name System (DNS)

The Domain Name System is a standard protocol with STD number 13, and its status is recommended. It is described in RFC 1034 and RFC 1035. This section explains the implementation of the Domain Name System and the implementation of name servers.

The early Internet configurations required the use of only numeric IP addresses. Because this was burdensome and much harder to remember than just the name of a system, this evolved into the use of symbolic host names. For example, instead of typing: TELNET 10.12.7.14

You can type:

TELNET MyHost

MyHost is then translated in some way to the IP address 10.12.7.14. Though using host names makes the process of accessing a resource easier, it also introduces the problem of maintaining the mappings between IP addresses and high-level machine names in a coordinated and centralized way.

Initially, host names to address mappings were maintained by the Network Information Center (NIC) in a single file (HOSTS.TXT), which was fetched by all hosts using FTP. This is called a *flat namespace*. But due to the explosive growth in the number of hosts, this mechanism became too cumbersome (consider the work involved in the addition of just one host to the Internet) and was replaced by a new concept: *Domain Name System*. Hosts on smaller networks can continue to use a local flat namespace (the HOSTS.LOCAL file) instead of or in addition to the Domain Name System. Outside of small networks, however, the Domain Name System is essential. This system allows a program running on a host to perform the mapping of a high-level symbolic name to an IP address for any other host without requiring every host to have a complete database of host names.

#### 12.1.1 The hierarchical namespace

Consider the typical internal structure of a large organization. Because the chief executive cannot do everything, the organization will probably be partitioned into divisions, each of them having autonomy within certain limits. Specifically, the executive in charge of a division has authority to make direct decisions, without permission from the chief executive.

Domain names are formed in a similar way, and will often reflect the hierarchical delegation of authority used to assign them. For example, consider the name: myHost.myDept.myDiv.myCorp.com

In this example, we know that there is a single host name *myHost*, which exists within the *myDept.myDiv.myCorp* subdomain. The *myDept.myDiv.myCorp* subdomain is one of the subdomains of *myDiv.myCorp.com* subdomain, which is in turn one of the subdomains of *myCorp.com.* Finally, *myCorp.com* is a subdomain of *com.* This hierarchy is better illustrated in Figure 12-1.

(

root

)

du

e

ov

g

mil

m

co

Pentagon

RPA

DA

Corp

my

SF

N

OT

D

me

Na

Ti

tle

Name

Title

my

Di

v

y

ourDiv

yourDept

myDept

*Figure 12-1 DNS hierarchical namespace*

We discuss this hierarchical structure at greater length in the following sections.

**12.1.2**  **Fully qualified domain names (FQDNs)**  When using the Domain Name System, it is common to work with only a part of the domain hierarchy, such as the myDivision.myCorp.com domain. The Domain Name System provides a simple method of minimizing the typing necessary in this circumstance. If a domain name ends in a dot (for example,

myDept.myDiv.myCorp.com.), it is assumed to be complete. This is called a *fully qualified domain name (FQDN)* or an *absolute domain name*. However, if it does not end in a dot (for example, myDept.myDiv), it is incomplete and the DNS resolver may complete this by appending a suffix such as .myCorp.com to the domain name. The rules for doing this are implementation-dependent and locally configurable.

#### 12.1.3 Generic domains

The top-level names are called the generic top-level domains (gTLDs), and can be three characters or more in length. Table 12-1 shows some of the top-level domains of today's Internet domain namespace.

*Table 12-1 Current generic domains*

|  |  |
| --- | --- |
| **Domain name** | **Meaning** |
| aero | The air transport industry |
| biz | Business use |
| cat | The Catalan culture |
| com | Commercial organizations |
| coop | Cooperatives |
| edu | Educational organizations |
| gov | U.S. governmental agencies |
| info | Informational sites |
| int | International organizations |
| jobs | Employment-related sites |
| mil | The U.S. military |
| mobi | Mobile devices sites |
| museum | Museums |
| **Domain name** | **Meaning** |
| name | Family and individual sites |
| net | Network infrastructures |
| org | Non-commercial organizations |
| pro | Professional sites |
| travel | The travel industry |

These names are registered with and maintained by the Internet Corporation for Assigned Names and Numbers (ICANN). For current information, see the ICANN Web site at:

[http://www.icann.org](http://www.icann.org/)

#### 12.1.4 Country domains

There are also top-level domains named for the each of the ISO 3166 international 2-character country codes (from *ae* for the United Arab Emirates to *zw* for Zimbabwe). These are called the *country* domains or the *geographical* domains. Many countries have their own second-level domains underneath which parallel the generic top-level domains. For example, in the United Kingdom, the domains equivalent to the generic domains .*com* and .*edu* are .*co*.*uk* and .*ac*.*uk* (ac is an abbreviation for academic). There is a .us top-level domain, which is organized geographically by state (for example, .ny.us refers to the state of New York). See RFC 1480 for a detailed description of the .us domain.

#### 12.1.5 Mapping domain names to IP addresses

The mapping of names to addresses consists of independent, cooperative systems called name servers. A name server is a server program that holds a master or a copy of a name-to-address mapping database, or otherwise points to a server that does, and that answers requests from the client software, called a name resolver.

Conceptually, all Internet domain servers are arranged in a tree structure that corresponds to the naming hierarchy in Figure 12-1 on page 427. Each leaf represents a name server that handles names for a single subdomain. Links in the conceptual tree do not indicate physical connections. Instead, they show which other name server a given server can contact.

#### 12.1.6 Mapping IP addresses to domain names: Pointer queries

The Domain Name System provides for a mapping of symbolic names to IP addresses and vice versa. While the hierarchical structure makes it easy in principle to search the database for an IP address using its symbolic name, the

process of mapping an IP address to a symbolic name cannot use the same process. Therefore, there is another namespace that facilitates the reverse mapping of IP address to symbolic name. It is found in the domain in-addr.arpa (arpa is used because the Internet was originally the *ARPAnet*).

Not including IPv6, IP addresses are normally written in dotted decimal format, and there is one layer of domain for each hierarchy. Contrary to domain names, which have the least-significant parts of the name first, the dotted decimal format has the most significant bytes first. Therefore, in the Domain Name System, the dotted decimal address is shown in reverse order.

For example, consider the following IPv4 address:

129.34.139.30

The in-add.arpa address for this is:

30.139.34.129.in-addr.arpa.

This is handled slightly different for IPv6 addresses. Because of the IPv6 address’ structure, the reverse order is done in nibbles in stead of octets. Also, the in-addr.arpa domain does not include IPv6. Instead, the domain used is IP6.ARPA. For example, consider the following IPv6 address:

4321:0:1:2:3:4:567:89ab

Breaking this into nibbles, reversing the odder, and appending the domain yields:

b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.ARPA

Given an IP address, the Domain Name System can be used to find the matching host name. A domain name query to do this is called a *pointer query*.

#### 12.1.7 The distributed name space

The Domain Name System uses the concept of a *distributed name space*. Symbolic names are grouped into *zones of authority*, more commonly referred to as *zones*. In each of these zones, one or more hosts has the task of maintaining a database of symbolic names and IP addresses within that zone, and provides a server function for clients who want to translate between symbolic names and IP addresses. These local name servers are then (through the internetwork on which they are connected) logically interconnected into a hierarchical tree of *domains*. Each zone contains a part or a *subtree* of the hierarchical tree, and the names within the zone are administered independently of names in other zones. Authority over zones is vested in the name servers.

Normally, the name servers that have authority for a zone will have domain names belonging to that zone, but this is not required. Where a domain contains a subtree that falls in a different zone, the name server or servers with authority over the superior domain are said to *delegate authority* to the name server or servers with authority over the subdomain. Name servers can also delegate authority to themselves; in this case, the domain name space is still divided into zones moving down the domain name tree, but authority for two zones is held by the same server. The division of the domain name space into zones is accomplished using resource records stored in the Domain Name System.

At the top-level root domain there is an exception to this. There is no higher system to which authority can be delegated, but it is not desirable to have all queries for fully qualified domain names to be directed to just one system. Therefore, authority for the top-level zones is shared among a set of *root name servers*[[3]](#footnote-3) coordinated by the ICANN.

To better illustrate the process of resolving a symbolic name to an IP address, consider a query for myHost.myDept.myCorp.com, and let us assume that our name server does not have the answer already in its cache. The query goes to the .com root name server, which in turn forwards the query to a server with an NS record for myCorp.com. At this stage, it is likely that a name server has been reached that has cached the needed answer. However, the query could be further delegated to a name server for myDept.myCorp.com

As a result of this scheme:

Rather than having a central server for the database, the work that is involved in maintaining this database is off-loaded to hosts throughout the name space.

Authority for creating and changing symbolic host names and responsibility for maintaining a database for them is delegated to the organization owning the zone (within the name space) containing those host names.

From the user's standpoint, there is a single database that deals with these address resolutions. The user might be aware that the database is distributed, but generally need not be concerned about this.

**Note:** Although domains within the namespace will frequently map in a logical fashion to networks and subnets within the IP addressing scheme, this is not a requirement of the Domain Name System. Consider a router between two subnets. It has two IP addresses, one for each network adapter, but it would not normally have two symbolic names.

#### 12.1.8 Domain name resolution

The domain name resolution process can be summarized in the following steps:

1. A user program issues a request such as the **gethostbyname()** system call (this particular call asks for the IP address of a host by passing the host name) or the **gethostname()** system call (which asks for a host name of a host by passing the IP address).
2. The resolver formulates a query to the name server. (Full resolvers have a local name cache to consult first; stub resolvers do not. See “Domain name full resolver” and “Domain name stub resolver” on page 434.)
3. The name server checks to see if the answer is in its local authoritative database or cache, and if so, returns it to the client. Otherwise, it queries other available name servers, starting down from the root of the DNS tree or as high up the tree as possible.
4. The user program is finally given a corresponding IP address (or host name, depending on the query) or an error if the query could not be answered. Normally, the program will not be given a list of all the name servers that have been consulted to process the query.

Domain name resolution is a client/server process (see 11.1.1, “The client/server model” on page 408). The client function (called the *resolver* or *name resolver*) is transparent to the user and is called by an application to resolve symbolic high-level names into real IP addresses or vice versa. The name server (also called a *domain name server*) is the server application providing the translation between high-level machine names and the IP addresses. The query/reply messages can be transported by either UDP or TCP.

##### Domain name full resolver

Figure 12-2 shows a program called a *full resolver*, which is distinct from the user program, that forwards all queries to a name server for processing. Responses are cached by the name server for future use.

User

Program

Full

Resolver

Cache

Name

Server

Foreign

Name

Server

C

a

c

h

e

Database

user

query

user

response

query

response

r

q

*Figure 12-2 DNS: Using a full resolver for domain name resolution*

##### Domain name stub resolver

Figure 12-3 shows a *stub resolver*, a routine linked with the user program, that forwards the queries to a name server for processing. Responses are cached by the name server, but not usually by the resolver, although this is implementation dependent. On most platforms, the stub resolver is implemented by two library routines (or by some variation of these routines): **gethostbyname()** and **gethostbyaddr()**. These are used for converting host names to IP addresses and vice versa. Stub resolvers are much more common than full resolvers.

User

Program

Stub

Resolver

Name

Server

Database

Foreign

Name

Server

C

a

c

h

e

query

response

r

q

*Figure 12-3 DNS: Using a stub resolver for domain name resolution*

##### Domain name resolver operation

Domain name queries can be one of two types: *recursive* or *iterative* (also called *non-recursive*). A flag bit in the domain name query specifies whether the client desires a recursive query, and a flag bit in the response specifies whether the server supports recursive queries. The difference between a recursive and an iterative query arises when the server receives a request for which it cannot supply a complete answer by itself. A recursive query requests that the server issues a query itself to determine the requested information and returns the complete answer to the client. An iterative query means that the name server

returns what information it has available and also a list of additional servers for the client to contact to complete the query.

Domain name responses can be one of two types: *authoritative* and *non-authoritative*. A flag bit in the response indicates which type a response is. When a name server receives a query for a domain in a zone over which it has authority, it returns all of the requested information in a response with the authoritative answer flag set. When it receives a query for a domain over which it does not have authority, its actions depend on the setting of the recursion desired flag in the query:

If the recursion desired flag is set and the server supports recursive queries, it will direct its query to another name server. This will either be a name server with authority for the domain given in the query, or it will be one of the root name servers. If the second server does not return an authoritative answer (for example, if it has delegated authority to another server), the process is repeated.

When a server (or a full resolver program) receives a response, it will cache it to improve the performance of repeat queries. The cache entry is stored for a maximum length of time specified by the originator in a 32-bit *time-to-live (TTL)* field contained in the response. A typical TTL value is 86,400 seconds (one day).

If the recursion desired flag is not set or the server does not support recursive queries, it will return whatever information it has in its cache and also a list of additional name servers to be contacted for authoritative information.

##### Domain name server operation

Each name server has *authority* for zero or more zones. There are three types of

|  |  |
| --- | --- |
| name servers: |  |
| **Primary** | A primary name server loads a zone's information from disk and has authority over the zone. |
| **Secondary** | A secondary name server has authority for a zone, but obtains its zone information from a primary server using a process called *zone transfer*. To remain synchronized, the secondary name servers query the primary on a regular basis (typically three hours) and re-execute the zone transfer if the primary has been updated. A name server can operate as a primary or a secondary name server for multiple domains, or a primary for some domains and as a secondary for others. A primary or secondary name server performs all of the functions of a caching-only name server. |
| **Caching-only** | A name server that does not have authority for any zone is called a caching-only name server. A caching-only name server obtains all of its data from primary or secondary name servers as required. It requires at least one NS record to point to a name server from which it can initially obtain information. |

When a domain is registered with the root and a separate zone of authority established, the following rules apply:

The domain must be registered with the root administrator.

There must be an identified administrator for the domain.

There must be at least two name servers with authority for the zone that are accessible from outside and inside the domain to ensure no single point of failure.

We also recommend that name servers that delegate authority apply these rules, because the delegating name servers are responsible for the behavior of name servers under their authority.

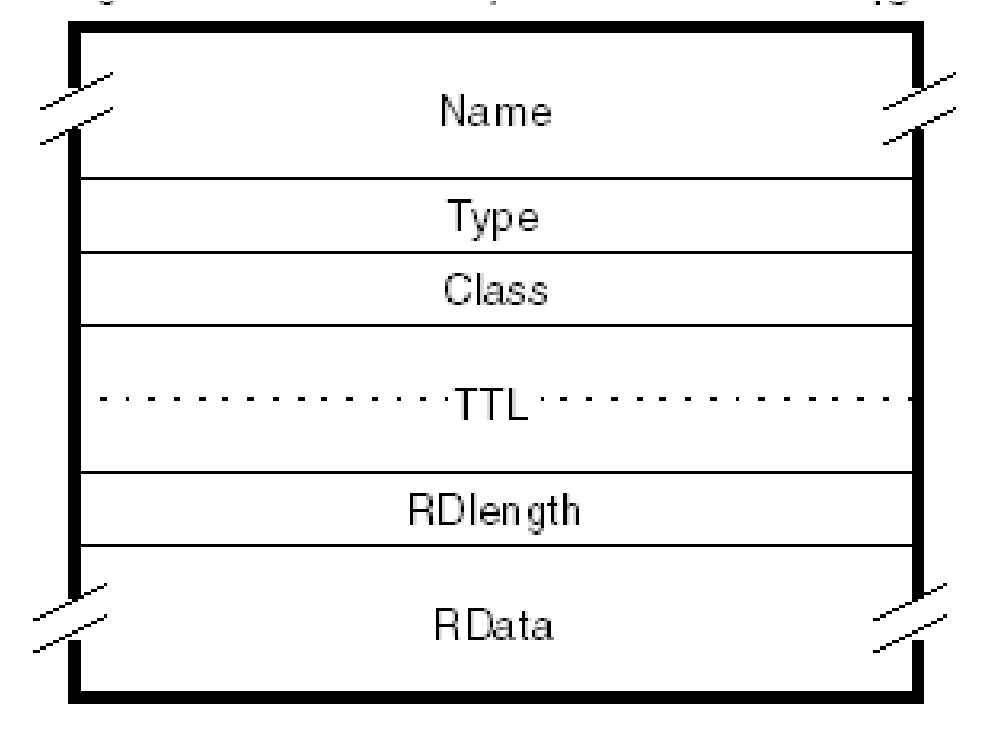
#### 12.1.9 Domain Name System resource records

The Domain Name System's distributed database is composed of *resource records* (RRs), which are divided into classes for different kinds of networks. We only discuss the Internet class of records. Resource records provide a mapping between domain names and *network objects*. The most common network objects are the addresses of Internet hosts, but the Domain Name System is designed to accommodate a wide range of different objects.

A zone consists of a group of resource records, beginning with a Start of

Authority (SOA) record. The SOA record identifies the domain name of the zone. There will be a name server (NS) record for the primary name server for this zone. There might also be NS records for the secondary name servers. The NS records are used to identify which of the name servers are authoritative (see “Domain name resolver operation” on page 434). Following these records are the resource records, which might map names to IP addresses or aliases to names.

The following figure shows the general format of a resource record (Figure 12-4).



*Figure 12-4 DNS general resource record format*

Where:

|  |  |
| --- | --- |
| **Name** | The domain name to be defined. The Domain Name System is very general in its rules for the composition of domain names. However, it recommends a syntax for domain names that minimizes the likelihood of applications that use a DNS resolver (that is, nearly all TCP/IP applications) from misinterpreting a domain name. A domain name adhering to this recommended syntax will consist of a series of labels consisting of alphanumeric characters or hyphens, each label having a length of between 1 and 63 characters, starting with an alphabetic character. Each pair of labels is separated by a dot (period) in human-readable form, but not in the form used within DNS messages. Domain names are not case-sensitive. |
| **Type** | Identifies the type of the resource in this record. There are numerous possible values, but some of the more common ones, along with the RFCs which define them, are listed in Table 12-2 on page 438. |
| **Class** | Identifies the protocol family. The only commonly used value is IN (the Internet system), though other values are defined by  RFC 1035 and include:   * CS (value 2): The CSNET class. This has been obsoleted. * CH (value 3): The CHAOS class. * HS (value 4): The Hesiod class. |
| **TTL** | The time-to-live (TTL) time in seconds for which this resource record will be valid in a name server cache. This is stored in the DNS as an unsigned 32-bit value. A typical value for records pointing to IP addresses is 86400 (one day). |
| **RDlength** | An unsigned 16-bit integer that specifies the length, in octets, of the RData field. |
| **RData** | A variable length string of octets that describes the resource. The format of this information varies according to the Type and Class of the resource record. |

*Table 12-2 Some of the possible resource record types*

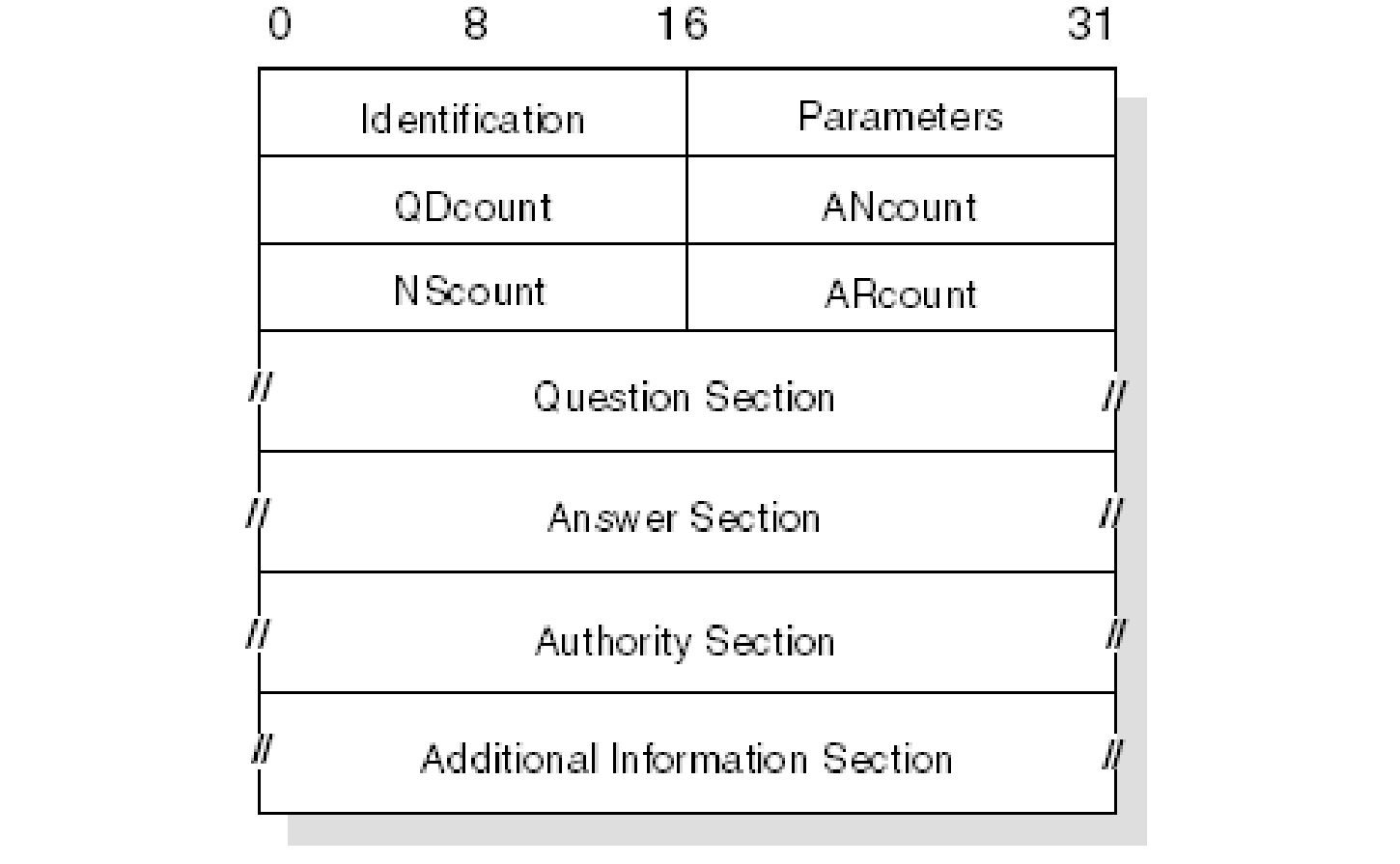
|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | **Value** | **Meaning** | **RFC def** |
| A | 1 | A host address | 1035 |
| NS | 2 | An authoritative name server | 1035 |
| CNAME | 5 | The canonical name for an alias | 1035 |
| SOA | 6 | Marks the start of a zone of authority | 1035 |
| MB | 7 | A mailbox domain name (experimental) | 1035 |
| MG | 8 | A mail group member (experimental) | 1035 |
| MR | 9 | A mail rename domain name (experimental) | 1035 |
| NULL | 10 | A NULL resource record (experimental) | 1035 |
| WKS | 11 | A well-known service description | 1035 |
| PTR | 12 | A domain name pointer | 1035 |
| HINFO | 13 | Host information | 1035 |
| MINFO | 14 | Mailbox or mail list information | 1035 |
| MX | 15 | Mail exchangea | 1035 |
| TXT | 16 | Text strings | 1035 |
| RP | 17 | Responsible person record | 1183 |
| AFSDB | 18 | Andrew File System database | 1183 |
| X25 | 19 | X.25 resource record | 1183 |
| ISDN | 20 | ISDN resource record | 1183 |
| RT | 21 | Route Through resource record | 1183 |
| NSAP | 22 | Network Service Access Protocol record | 1348 |
| **Type** | **Value** | **Meaning** | **RFC def** |
| NSAP-PTR | 23 | NSAP Pointer record | 1348 |
| KEY | 25 | The public key associated with a DNS name | 2535 |
| AAAA | 28 | An IPv6 address record | 3596 |
| LOC | 29 | GPS resource record | 1876 |
| SRV | 33 | Defines the services available in a zone | 2872 |
| CERT | 37 | Certificate resource records | 4398 |
| A6 | 38 | Forward mapping of an IPv6 address | 2874 |
| DNAME | 39 | Delegation of IPv6 reverse addresses | 2672 |
| DS | 39 | Delegated Signer record (DNS security) | 4034 |
| RRSIG | 46 | Resource record digital signature | 4034 |
| NSEC | 47 | Next Secure record (DNS security) | 4034 |
| DNSKEY | 48 | Public Key record (DNS security | 4034 |

a. The MX Type obsoletes Types MD (value 3, Mail destination) and MF (value 4, Mail forwarder).

#### 12.1.10 Domain Name System messages

All messages in the Domain Name System protocol use a single format. This format is shown in Figure 12-5 on page 440. This frame is sent by the resolver to the name server. Only the header and the question section are used to form the query. Replies and forwarding of the query use the same frame, but with more sections filled in (the answer/authority/additional sections).

*Figure 12-5 DNS message format*



##### Header format

The header section is always present and has a fixed length of 12 bytes. The other sections are of variable length.

**ID** A 16-bit identifier assigned by the program. This identifier is copied in the corresponding reply from the name server and can be used for differentiation of responses when multiple queries are outstanding at the same time.

**Parameters** A 16-bit value in the following format (Table 12-3).

*Table 12-3 Parameters*

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 10 | 11 | 12 13 | 14 | 15 |
| Q  R | Op code |  |  | A  A | T  C | R  D | R  A | Zero |  | Rcode |  |  |

Where:

|  |  |
| --- | --- |
| **QR** | Flag identifying a query (0) or a response(1). |
| **Op code** | 4-bit field specifying the kind of query: |

1. Standard query (QUERY)
2. Inverse query (IQUERY)
3. Server status request (STATUS)

Other values are reserved for future use:

|  |  |
| --- | --- |
| **AA** | Authoritative answer flag. If set in a response, this flag specifies that the responding name server is an authority for the domain name sent in the query. |
| **TC** | Truncation flag. Set if message was longer than permitted on the physical channel. |
| **RD** | Recursion desired flag. This bit signals to the name server that recursive resolution is asked for. The bit is copied to the response. |
| **RA** | Recursion available flag. Indicates whether the name server supports recursive resolution. |
| **Zero** | 3 bits reserved for future use. Must be zero. |
| **Rcode** | 4-bit response code. Possible values are:   1. No error. 2. Format error. The server was unable to interpret the message. 3. Server failure. The message was not processed because of a problem with the server. 4. Name error. The domain name in the query does not exist.   This is only valid if the AA bit is set in the response.   1. Not implemented. The requested type of query is not implemented by name server. 2. Refused. The server refuses to respond for policy reasons.   Other values are reserved for future use. |
| **QDcount** | An unsigned 16-bit integer specifying the number of entries in the question section. |
| **ANcount** | An unsigned 16-bit integer specifying the number of RRs in the answer section. |
| **NScount** | An unsigned 16-bit integer specifying the number of name server RRs in the authority section. |
| **ARcount** | An unsigned 16-bit integer specifying the number of RRs in the additional records section. |

##### Question section

The next section contains the queries for the name server. It contains QDcount (usually 1) entries, each in the format shown in Figure 12-6.

*Figure 12-6 DNS question format*

*2*



Where:

|  |  |
| --- | --- |
| **Length** | A single byte giving the length of the next label. |
| **Label** | One element of the domain name characters (for example, ibm from ral.ibm.com). The domain name referred to by the question is stored as a series of these variable length labels, each preceded by a 1-byte length. |
| **00** | X'00' indicates the end of the domain name and represents the null label of the root domain. |
| **Type** | 2 bytes specifying the type of query. It can have any value from the Type field in a resource record. |
| **Class** | 2 bytes specifying the class of the query. For Internet queries, this will be IN. |

2 Note that all of the fields are byte-aligned. The alignment of the Type field on a 4-byte boundary is for example purposes and is not required by the format.

For example, the domain name mydiv.mycorp.com is encoded with the following fields:

X'05'

"mydiv"

X'06'

"mycorp"

X'03'

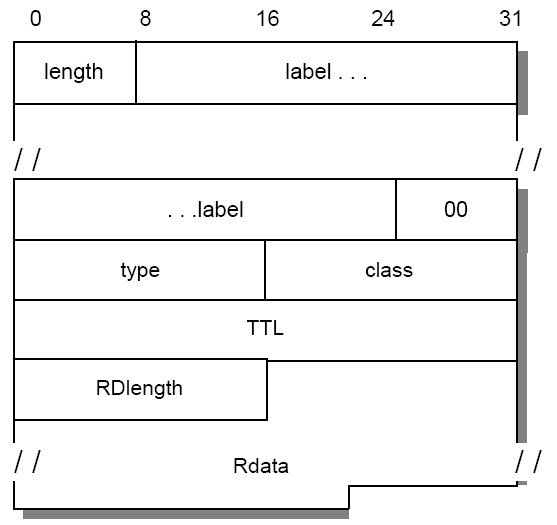
"com"

X'00'

Therefore, the entry in the question section for mydiv.mycorp.com requires 22 bytes: 18 to store the domain name and 2 each for the Qtype and Qclass fields.

##### Answer, authority, and additional resource sections

These three sections contain a variable number of resource records. The number is specified in the corresponding field of the header. The resource records are in the format shown in Figure 12-7.



*Figure 12-7 DNS: Answer Record Entry format [[4]](#footnote-4)*

Where the fields before the TTL field have the same meanings as for a question entry and:

|  |  |
| --- | --- |
| **TTL** | A 32-bit time-to-live value in seconds for the record. This defines how long it can be regarded as valid. |
| **RDlength** | A 16-bit length for the Rdata field. |
| **Rdata** | A variable length string whose interpretation depends on the Type field. |

##### Message compression

In order to reduce the message size, a compression scheme is used to eliminate the repetition of domain names in the various RRs. Any duplicate domain name or list of labels is replaced with a pointer to the previous occurrence. The pointer has the form of a 2-byte field as shown in Figure 12-8.



*Figure 12-8 DNS message compression*

Where:

The first 2 bits distinguish the pointer from a normal label, which is restricted to a 63-byte length plus the length byte ahead of it (which has a value of <64).

The offset field specifies an offset from the start of the message. A zero offset specifies the first byte of the ID field in the header.

If compression is used in an Rdata field of an answer, authority, or additional section of the message, the preceding RDlength field contains the real length after compression is done.

Refer to 12.2, “Dynamic Domain Name System” on page 453 for additional message formats.

##### Using the DNS Uniform Resource Identifiers (URI)

A DNS can also be queried using a Uniform Resource Identifier This is defined in RFC 4501. Strings are not case sensitive, and adhere to the following format:

“dns:” + [ “//” + dnsauthority + “:” + port + ”/” ] + dnsname +

[ “?” + dnsquery ]

|  |  |  |
| --- | --- | --- |
| Where: |  | |
| **dnsauthority** | The DNS server to which the query should be sent. If this is left blank, the query is sent to the default DNS server. | |
| **dnsname** | The name or IP address to be queried. |
| **dnsquery** | The type of the query to be performed. This can be any combination, separated by a semicolon (;), of: |

**CLASS** Usually IN for internet, the class of the query **TYPE** The type of resource record desired

For example, a request using the URI to resolve www.myCorp.com to an IP address might appear as follows: dns:www.mycorp.com

Additionally, the same request can be sent to the server at 10.1.2.3 on port 5353 using the following: dns://10.1.2.3:5353/www.mycorp.com

Finally, this same query can be made specifying a CLASS of IN and a TYPE of A:

dns://10.1.2.3:5353/www.mycorp.com?class=IN;type=A

#### 12.1.11 A simple scenario

Consider a stand-alone network (no outside connections), consisting of two physical networks:

One has an Internet network address of 129.112.

One has a network address of 194.33.7.

They are interconnected by an IP gateway (VM2). See Figure 12-9for more details.



*Figure 12-9 DNS: A simple configuration: Two networks connected by an IP gateway*

Assume the name server function has been assigned to VM1. Remember that the domain hierarchical tree forms a logical tree, completely independent of the physical configuration. In this simple scenario, there is only one level in the domain tree, which will be referred to as *test.example*.

The zone data for the name server appears as shown in Figure 12-10 and continued in Figure 12-11 on page 448.

;note: an SOA record has no TTL field

;

$origin test.example. ;note 1 @ IN SOA VM1.test.example. ADM.VM1.test.example.

(870611 ;serial number for data

1800 ;secondary refreshes every 30 mn

300 ;secondary reties every 5 mn

604800 ;data expire after 1 week

86400) ;minimum TTL for data is 1 week

;

@ 99999 IN NS VM1.test.example. ;note 2 ;

VM1 99999 IN A 129.112.1.1 ;note 3

99999 IN WKS 129.112.1.1 TCP (SMTP ;note 4

FTP

TELNET

NAMESRV)

;

RT1 99999 IN A 129.112.1.2

IN HINFO IBM RT/PC-AIX ;note 5

RT2 99999 IN A 129.112.1.3

IN HINFO IBM RT/PC-AIX

PC1 99999 IN A 129.112.1.11

PC2 99999 IN A 194.33.7.2

PC3 99999 IN A 194.33.7.3

;

;VM2 is an IP gateway and has 2 different IP addresses

;

VM2 99999 IN A 129.112.1.4

99999 IN A 194.33.7.1

99999 IN WKS 129.112.1.4 TCP (SMTP FTP) IN HINFO IBM-3090-VM/CMS

*Figure 12-10 Zone data for the name server, continued in Figure 12-11 on page 448*

|  |
| --- |
| ;  4.1.112.129.in-addr.arpa. IN PTR VM2 ;note 6  ;  ;Some mailboxes  ;  central 10 IN MX VM2.test.example. ;notes 7 and 8  ;  ;a second definition for the same mailbox, in case VM2 is down  ; central 20 IN MX VM1.test.example. waste 10 IN MX VM2.test.example. |

*Figure 12-11 Zone data for the name server, continued from Figure 12-10 on page 447*

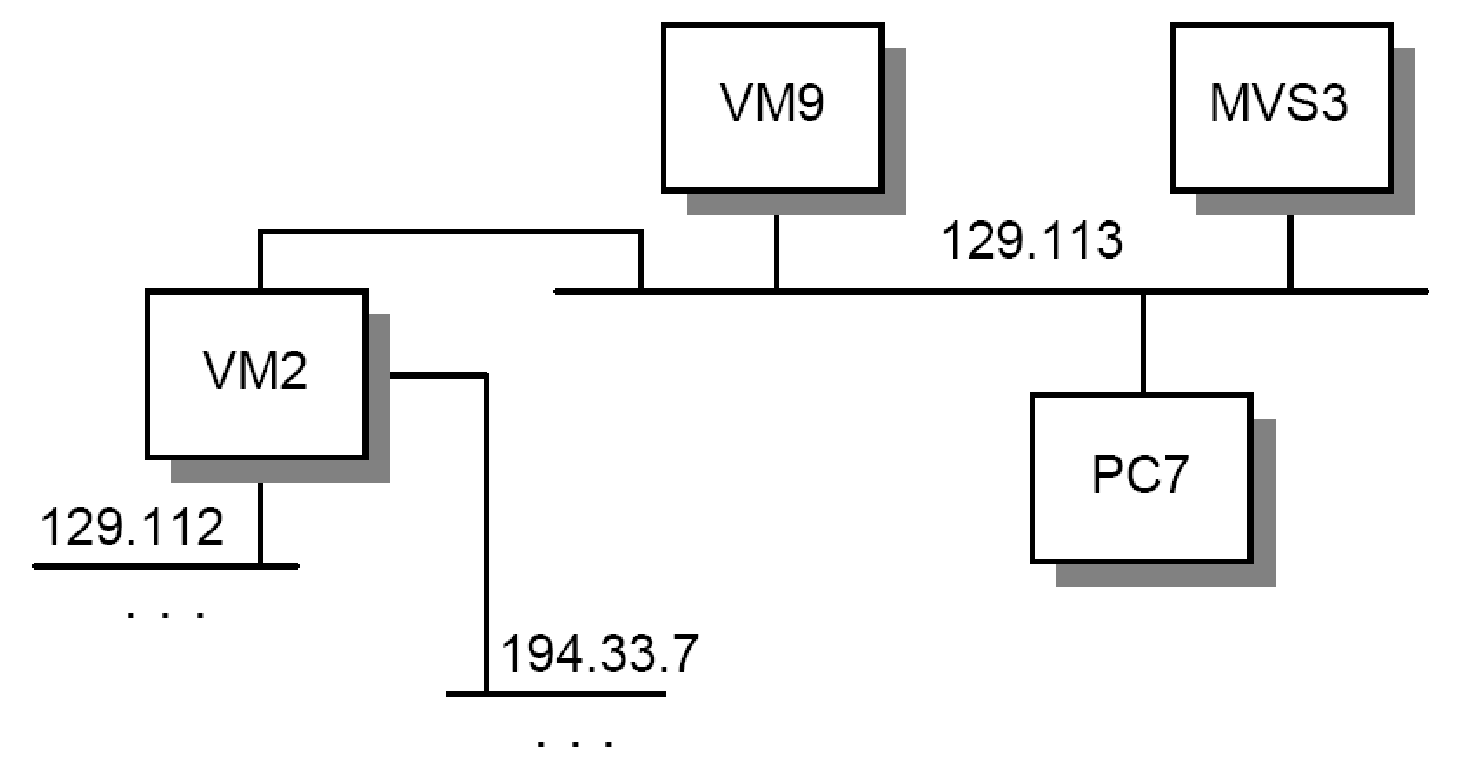
|  |
| --- |
| **Notes for Figure 12-10 on page 447 and Figure 12-11:**   1. The $origin statement sets the @ variable to the zone name   (test.example.). Domain names that do not end with a period are suffixed with the zone name. Fully qualified domain names (those ending with a period) are unaffected by the zone name.   1. Defines the name server for this zone. 2. Defines the Internet address of the name server for this zone. 3. Specifies well-known services for this host. These are expected to always be available. 4. Gives information about the host. 5. Used for inverse mapping queries (see 12.1.6, “Mapping IP addresses to domain names: Pointer queries” on page 430). 6. Will allow mail to be addressed to user@central.test.example. 7. See 15.1.2, “SMTP and the Domain Name System” on page 565 for the use of these definitions. |

#### 12.1.12 Extended scenario

Consider the case where a connection is made to a third network (129.113),

which has an existing name server with authority for that zone (see

Figure 12-12).



*Figure 12-12 DNS: Extended configuration - Third network connected to existing configuration*

Let us suppose that the domain name of the other network is tt.ibm.com and that its name server is located in VM9. All we have to do is add the address of this name server to our own name server database (in the named.ca initial cache file) and reference the other network by its own name server. The following two lines are all that is needed to do that:

tt.ibm.com. 99999 IN NS VM9.tt.ibm.com. VM9.tt.ibm.com. 99999 IN A 129.13.1.9

This simply indicates that VM9 is the authority for the new network and that all queries for that network will be directed to that name server.

#### 12.1.13 Transport

Domain Name System messages are transmitted either as datagrams (UDP) or through stream connection (TCP):

UDP usage: Server port 53 (decimal).

Messages carried by UDP are restricted to 512 bytes. Longer messages are truncated and the truncation (TC) bit is set in the header. Because UDP frames can be lost, a retransmission strategy is required.

TCP usage: Server port 53 (decimal).

In this case, the message is preceded by a 2-byte field indicating the total message frame length.

STD 3 – Host Requirements requires that:

* A Domain Name System resolver or server that is sending a non-zone-transfer query *must* send a UDP query first. If the answer section of the response is truncated and if the requester supports TCP, it tries the query again using TCP. UDP is preferred over TCP for queries because UDP queries have much lower overall processing cost, and the use of UDP is essential for a heavily loaded server. Truncation of messages is rarely a problem given the current contents of the Domain Name System database, because typically 15 response records can be accommodated in the datagram, but this might change as new record types continue to be added to the Domain Name System.
* TCP must be used for zone transfer activities because the 512-byte limit for a UDP datagram will always be inadequate for a zone transfer.
* Name servers must support both types of transport.

As IPv6 becomes more pervasive throughout the Internet community, some problems are forecasted as a result of mixed IPv4/IPv6 network segments. Primarily, if a resolver that can only use IPv4 is forwarded to across a network segment that supports only IPv6, the resolver and the name server will be unable to communicate. As a result, the hierarchical namespace becomes fragmented into two sets of segments: those that support IPv4 and IPv6, and those that support only IPv6. This impending issue has been named the Problem of Name Space Fragmentation, and documented in RFC 3901. In order to preserve namespace continuity, RFC 3901 recommends the following:

Every recursive name server should be either IPv4 only, or dual IPv4 and IPv6.

Every DNS zone should be served by at least one IPv4-reachable authoritative name server.

Additional suggestions about configuring IPv6 DNS servers are in RFC 4339.

##### Dynamic DNS (DDNS)

The Dynamic Domain Name System (DDNS) is a protocol that defines extensions to the Domain Name System to enable DNS servers to accept requests to add, update, and delete entries in the DNS database dynamically. Because DDNS offers a functional superset to existing DNS servers, a DDNS server can serve both static and dynamic domains at the same time, a welcome feature for migration and overall DNS design.

DDNS is currently available in a non-secure and a secure flavor, defined in RFC

2136 and RFC 3007, respectively. Rather than allowing any host to update its DNS records, the secure version of DDNS uses public key security and digital signatures to authenticate update requests from DDNS hosts.

Without client authentication, another host could impersonate an unsuspecting host by remapping the address entry for the unsuspecting host to that of its own. After the remapping occurs, important data, such as logon passwords and mail intended for the host would, unfortunately, be sent to the impersonating host instead.

See 12.2, “Dynamic Domain Name System” on page 453for more information about how DDNS works together with DHCP to perform seamless updates of reverse DNS mapping entries, and see 9.4, “DNS in IPv6” on page 367for more information about DNS with IPv6.

#### 12.1.14 DNS applications

Three common utilities for querying name servers are provided with many DNS implementations: **host**, **nslookup**, and **dig**. Though specifics details about each utility vary slightly by platform, most platforms provide a common set of options.

##### host

The **host** command obtains an IP address associated with a host name, or a host name associated with an IP address. The typical syntax for **host** command is: host [options] name [server]

Where:

**options** Valid options typically include:

**-c class** The query class. By default, this is IN (Internet), but other valid class names include CS (CSNET), CH (CHAOS), HS (Hesiod), and ANY (a wildcard encompassing all four classes).

**-r** Disables recursive processing.

|  |  |
| --- | --- |
|  | **-t type** The type of query required. This can be any of the standard resource record types (see Table 12-2 on page 438).  **-w** Instructs the **host** command to wait forever  for a reply. |
| **name** | The name of the host or the address to be resolved. |
| **server** | The name server to query. |

##### nslookup

The **nslookup** command enables you to locate information about network nodes, examine the contents of a name server database, and establish the accessibility of name servers. The typical syntax for the **nslookup** command is: nslookup [options] [host] [-nameserver] Where:

|  |  |
| --- | --- |
| **options** | These options vary widely by platform. Refer to the documentation for a specific implementation for information about what options are available. |
| **host** | The host name or IP address to be located. |
| **-nameserver** | The name server to which the query is to be directed. |

##### dig

**dig** stands for Domain Internet Groper, and enables you to exercise name servers, gather large volumes of domain name information, and execute simple domain name queries. The typical syntax for the **dig** command is: dig @server [options] [name] [type] [class] [queryopt]

Where:

|  |  |  |
| --- | --- | --- |
| **@server** | The DNS name server to be queried. | |
| **options** | Valid options typically include: | |
| **-b address** | The source IP address of the query-to address. |
|  | **-c class** | The query class. By default, this is IN  (Internet), but other valid class names |
|  | **-f filename** | include CS (CSNET), CH (CHAOS), and HS    (Hesiod).  Causes **dig** to operate in batch mode, and specifies the file from which the batch commands can be found. |

**-p port** Specifies that **dig** should send the query to a port other than well-known DNS port 53.

**-x address** Instructs **dig** to do a reverse lookup on the specified address.

**name** The name of the resource record to be looked up.

**type** The type of query required. This can be any of the standard resource record types (see Table 12-2 on page 438).

### 12.2 Dynamic Domain Name System

The Domain Name System described in 12.1, “Domain Name System (DNS)” on page 426 is a static implementation without recommendations with regard to security. In order to implement DNS dynamically, take advantage of DHCP, and still to be able to locate any specific host by means of a meaningful label (such as its host name), the following extensions to DNS are required:

A method for the host name to address a mapping entry for a client in the domain name server to be updated after the client has obtained an address from a DHCP server

A method for the reverse address to host name mapping to take place after the client obtains its address

Updates to the DNS to take effect immediately, without the need for intervention by an administrator

Updates to the DNS to be authenticated to prevent unauthorized hosts from accessing the network and to stop imposters from using an existing host name and remapping the address entry for the unsuspecting host to that of its own

A method for primary and secondary DNS servers to quickly forward and receive changes as entries are being updated dynamically by clients

However, implementation of a Dynamic Domain Name System (DDNS) can introduce problems if the environment is not secure. One method of security employed by DNS is the use of Secret Key Transaction Authentication (TSIG), defined in RFC 2845. This can be used to authenticate dynamic updates from clients, or authenticate responses coming from a recursive server. Additionally, these messages can now be protected for integrity and confidentiality through using TSIG over the Generic Security Service (GSS-TSIG). This extension, and the associated algorithms needed to implement GSS-TSIG, are defined in RFC 3645.

In addition to TSIG, and GSS-TSIG, several RFCs extended the functionality of DNS such that it incorporated additional security methods. These additions, defined in RFC 4033 and referred to as the DNS Security Extensions (DNSSEC), allow DNS to authenticate the origin of data as well as negative responses to DNS queries. However, they do not provide confidentiality, access control lists, or protection against denial-of-service-attacks. New resource records relating to security were added by RFCs 4034 and 4398, and include:

DNSKEY (public key)

DS (delegation signer)

RRSIG (resource record digital signature)

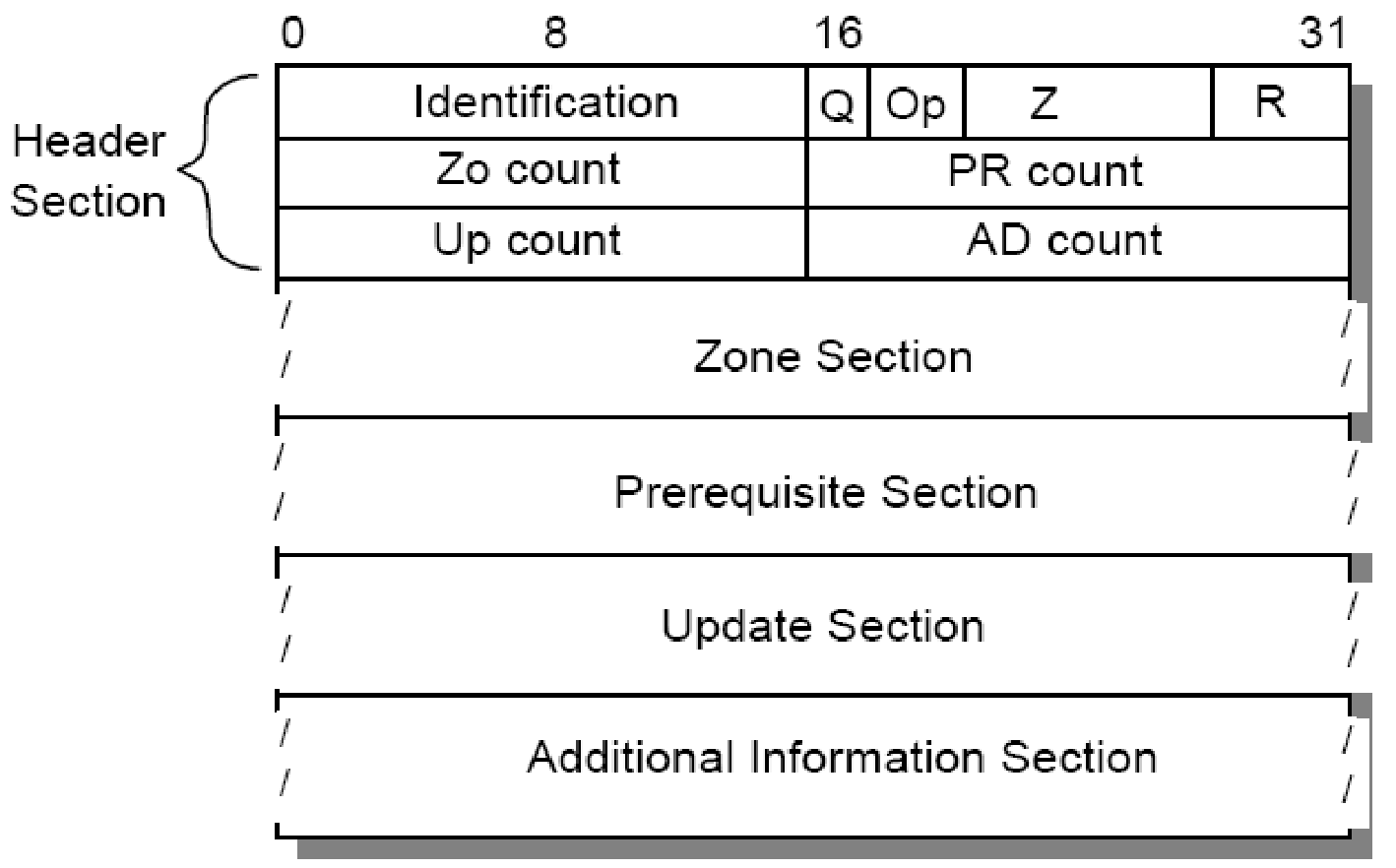
NSEC (authenticated denial of existence)

CERT (public key certificates)

Note that these RRs are also listed in Table 12-2 on page 438. Specific details about how the DNS protocol was modified to take advantage of these additions is in RFC 4035.

#### 12.2.1 Dynamic updates in the DDNS

The DNS message format (shown in Figure 12-5 on page 440) was designed for the querying of a static DNS database. RFC 2136 defines a modified DNS message for updates, called the UPDATE DNS message, illustrated in Figure 12-13 on page 455. This message adds or deletes resource records in the DNS, and allows updates to take effect without the DNS having to be reloaded.



*Figure 12-13 DDNS UPDATE message format*

The header section is always present and has a fixed length of 12 bytes. The other sections are of variable length. They are:

**Identification** A 16-bit identifier assigned by the program. This identifier is copied in the corresponding reply from the name server and can be used for differentiation when multiple queries/updates are outstanding at the same time.

1. Flag identifying an update request (0) or a response (1).

**Op** Opcode. The value 5 indicates an UPDATE message. **z** 7-bit field set to 0 and reserved for future use.

1. Response code (undefined in update requests). Possible

values are:

* 1. No error.
  2. Format error. The server was unable to interpret the message.
  3. Server failure. The message was not processed due to a problem with the server. **3** Name error. A name specified does not exist.

* + 1. Not implemented. The type of message specified in Opcode is not supported by this server.
    2. Refused. The server refuses to perform the UPDATE requested for security or policy reasons.
    3. Name error. A name exists when it should not.
    4. RRset error. A resource record set exists when it should not.
    5. RRset error. A resource record set specified does not exist.
    6. Zone Authority error. The server is not authoritative for the zone specified.
    7. Zone error. A name specified in the Prerequisite or Update sections is not in the zone specified.

|  |  |
| --- | --- |
| **ZO count** | The number of RRs in the Zone section. |
| **PR count** | The number of RRs in the Prerequisite section. |
| **UP count** | The number of RRs in the Update section. |
| **AD count** | The number of RRs in the Additional information section. |
| **Zone section** | This section is used to indicate the zone of the records that are to be updated. As all records to be updated must belong to the same zone, the zone section has a single entry specifying the zone name, zone type (which must be SOA), and zone class. |

##### Prerequisite section

This section contains RRs or RRsets that either must, or must not, exist, depending on the type of update.

**Update section** This section contains the RRs, RRsets, or both that are to be added to or deleted from the zone.

##### Additional information section

This section can be used to pass additional RRs that relate to the update operation in process.

For further information about the UPDATE message format, refer to RFC 2136.

#### 12.2.2 Incremental zone transfers in DDNS

RFC 1995 introduces the IXFR DNS message type, which allows incremental transfers of DNS zone data between primary and secondary DNS servers. In other words, when an update has been made to the zone data, only the change has to be copied to the other DNS servers that maintain a copy of the zone data, rather than the whole DNS database (as is the case with the AXFR DNS message type).

The format of an IXFR query is exactly that of a normal DNS query, but with a query type of IXFR. The response’s answer section, however, is made up of *difference sequences*.

Each list difference sequences is preceded by the server’s current version of the SOA and represents one update to the zone. Similarly, each difference sequence is preceded by an SOA version (indicating in which versions correspond to each change, and the difference sequences are ordered oldest to newest. Upon receiving this message, a server can update its zone by tracking the version history listed in the IXFR answer section.

For example, assume a server has the following zone:

|  |  |
| --- | --- |
| MYZONE.MYDIV.MYCORP | IN SOA MYHOST.MYDIV.MYCORP (  1 600 600 3600000 614800)  IN NS MYHOST.MYDIV.MYCORP |
| MYHOST.MYDIV.MYCORP | IN A 10.1.2.3 |
| OTHERHOST.MYDIV.MYCORP | IN A 10.2.3.4 |

Otherhost.mydiv.mycorp is removed, and in version 2, thishost.mydiv.mycorp is added, leaving the zone as:

MYZONE.MYDIV.MYCORP IN SOA MYHOST.MYDIV.MYCORP (

2 600 600 3600000 614800)

IN NS MYHOST.MYDIV.MYCORP

MYHOST.MYDIV.MYCORP IN A 10.1.2.3

THISHOST.MYDIV.MYCORP IN A 10.2.3.5

If the server receives an IXFR query, it sends back the following answer section:

|  |  |
| --- | --- |
| MYZONE.MYDIV.MYCORP | IN SOA serial=2 |
| MYZONE.MYDIV.MYCORP | IN SOA serial=1 |
| OTHERHOST.MYDIV.MYCORP | IN A 10.1.2.4 |
| MYZONE.MYDIV.MYCORP | IN SOA serial=2 |
| THISHOST.MYDIV.MYCORP | IN A 10.2.3.5 |
| MYZONE.MYDIV.MYCORP | IN SOA serial=2 |

**Note:** If a server received an IXFR query, but incremental zone transfers are not available, it will send back the entire zone in the reply.

#### 12.2.3 Prompt notification of zone transfer

RFC 1996 introduces the NOTIFY DNS message type, which is used by a master server to inform subordinate servers that an update has taken place and that they should initiate a query to discover the new data. The NOTIFY message uses the DNS message format, but only a subset of the available fields (unused

fields are filled with binary zeros). The message is similar to a QUERY message, and can contain the name of the RRs that have been updated. Upon receipt of a NOTIFY message, the subordinate returns a response. The response contains no useful information, and only serves to alert the master server of receipt of the NOTIFY. Based on the RRs contained in the notify, subordinate servers might then send an update query to the server to obtain the new changes.

### 12.3 Network Information System (NIS)

The Network Information System (NIS) is not an Internet standard. It was developed by Sun Microsystems, Inc. It was originally known as the Yellow Pages (YP) and many implementations continue to use this name.

NIS is a distributed database system that allows the sharing of system information in UNIX-based environment. Examples of system information that can be shared include the /etc/passwd, /etc/group, and /etc/hosts files. NIS has the following advantages:

Provides a consistent user ID and group ID name space across a large number of systems

Reduces the time and effort by users in managing their user IDs, group IDs, and NFS file system ownerships

Reduces the time and effort by system administrators in managing user IDs, group IDs, and NFS ownerships

NIS is built on the RPC, and employs the client/server model. Most NIS implementations use UDP. However, because it uses RPC, it is also possible for it to be implemented over TCP. A NIS domain is a collection of systems consisting of:

**NIS master server** Maintains *maps*, or databases, containing the

system information, such as passwords and host names. These are also referred to as Database Maps (DBMs).

**NIS subordinate server(s)** Can be defined to offload the processing from the master NIS server or when the NIS master server is unavailable.

**NIS client(s)** The remaining systems that are served by the

NIS servers.

The NIS clients do not maintain NIS maps; they query NIS servers for system information. Any changes to an NIS map is done only to the NIS master server (through RPC). The master server then propagates the changes to the NIS subordinate servers.

Note that the speed of a network determines the performance and availability of the NIS maps. When using NIS, the number of subordinate servers should be tuned in order to achieve these goals.

Because NIS is not standardized by the IETF, implementations vary by platform.

However, most platforms make available the following common NIS commands:

|  |  |
| --- | --- |
| **makedbm** | Generate a DBM file from an input file. |
| **ypcat** | Display the contents of a DBM file. |
| **ypinit** | Set up an NIS master or subordinate server. |
| **ypmake** | Performs the same function as **makedbm**, but provides the option to push the resulting DBMs to subordinate servers. |
| **ypmatch** | Prints the values associated with one or more keys in a DBM. |
| **yppasswd** | Change a login password stored in a DBM. |
| **yppush** | Pushes DBMs to subordinate servers. |
| **ypwhich** | Indicates what NIS server a client is using. |
| **ypxfr** | Pulls a DBM from the master server. |

### 12.4 Lightweight Directory Access Protocol (LDAP)

When implementing a Distributed Computing Environment (DCE), directory services are automatically included because they are an intrinsic part of the DCE architecture. However, though widely used, implementation of a DCE is not a practical solution for every company needing directory services because it is an “all-or-nothing” architecture. As such, if the other services provided by a DCE are not required, or if implementation of the DCE model is not feasible (for example, if it is not feasible to install the client software on every workstation within the network), other directory service alternatives must be identified.

One such alternative is the Lightweight Directory Access Protocol (LDAP), which is an open industry standard that has evolved to meet these needs. LDAP defines a standard method for accessing and updating information in a directory, and is gaining wide acceptance as the directory access method of the Internet. It is supported by a growing number of software vendors and is being incorporated into a growing number of applications.

For further information about LDAP, refer to the IBM Redbook *Understanding*  *LDAP - Design and Implementation*, SG24-4986.

#### 12.4.1 LDAP: Lightweight access to X.500

The OSI directory standard, X.500, specifies that communication between the directory client and the directory server uses the Directory Access Protocol

(DAP). However, as an application layer protocol, DAP requires the entire OSI protocol stack to operate, which requires more resources than are available in many small environments. Therefore, an interface to an X.500 directory server using a less resource-intensive or lightweight protocol was desired.

LDAP was developed as a *lightweight* alternative to DAP, because it requires the more popular TCP/IP protocol stack rather than the OSI protocol stack. LDAP also simplifies some X.500 operations and omits some esoteric features. Two precursors to LDAP appeared as RFCs issued by the IETF, RFC 1202 – Directory Assistance Service and RFC 1249 – DIXIE Protocol Specification.

These were both informational RFCs which were not proposed as standards. The directory assistance service (DAS) defined a method by which a directory client communicates to a proxy on an OSI-capable host, which issues X.500 requests on the client's behalf. DIXIE is similar to DAS, but provides a more direct translation of the DAP.

The first version of LDAP was defined in RFC 1487 – X.500 Lightweight Access, which was replaced by RFC 1777 – Lightweight Directory Access Protocol. Much of the work on DIXIE and LDAP was carried out at the University of Michigan, which provides reference implementations of LDAP and maintains LDAP-related Web pages and mailing lists. Since then, LDAPv2 has been replaced by LDAP Version 3. LDAPv3 is summarized in RFC 4510, but the technical specifications are divided into multiple subsequent RFCs listed in Table 12-4.

*Table 12-4 LDAP-related RFCs*

|  |  |
| --- | --- |
| **RFC number** | **Content** |
| 4510 | Technical Specification Road Map |
| 4511 | The Protocol |
| 4512 | Directory Information Models |
| 4513 | Authentication Methods and Security Mechanisms |
| 4514 | String Representation of Distinguished Names |
| 4515 | String Representation of Search Filters |
| 4516 | Uniform Resource Locator |
| 4517 | Syntaxes and Matching Rules |
| 4518 | Internationalized String Preparation |
| **RFC number** | **Content** |
| 4519 | Schema for User Applications |
| 4520 | Internet Assigned Numbers Authority (IANA) Considerations for  LDAP |
| 4521 | Considerations for LDAP |
| 4522 | The Binary Encoding Option |
| 4523 | Schema Definitions for X.509 Certificates |
| 4524 | COSINE/ LDAP X.500 Schema |
| 4525 | Modify-Increment Extension |
| 4526 | Absolute True and False Filters |
| 4527 | Read Entry Controls |
| 4528 | Assertion Control |
| 4529 | Requesting Attributes by Object Class in LDAP |
| 4530 | entryUUID Operational Attribute |
| 4531 | Turn Operation |
| 4532 | “Who Am I” Operation |
| 4533 | Content Synchronization Operation |

Though an application program interface (API) for previous versions of LDAP was limited to specifications in RFC 1823, the LDAPv3 provides both a C API and a Java™ Naming and Directory Interface (JNDI).

#### 12.4.2 The LDAP directory server

LDAP defines a communication protocol. That is, it defines the transport and format of messages used by a client to access data in an X.500-like directory. LDAP does not define the directory service itself. An application client program initiates an LDAP message by calling an LDAP API. But an X.500 directory server does not understand LDAP messages. In fact, the LDAP client and X.500 server even use different communication protocols (TCP/IP versus OSI). The LDAP client actually communicates with a gateway process (also called a proxy or front end) that forwards requests to the X.500 directory server (see Figure 12-14 on page 462), known as an LDAP server, which fulfils requests from the LDAP client. It does this by becoming a client of the X.500 server. The LDAP server must communicate using both TCP/IP (with the client) and OSI (with the X.500 server).

LDAP

Client

LDAP

Server

X.500

Server

Directory

TCP/IP

OSI

*Figure 12-14 LDAP server acting as a gateway to an X.500 directory server*

As the use of LDAP grew and its benefits became apparent, people who did not have X.500 servers or the environments to support them wanted to build directories that could be accessed by LDAP clients. This requires that the LDAP server store and access the directory itself instead of only acting as a gateway to X.500 servers (see Figure 12-15). This eliminates any need for the OSI protocol stack but, of course, makes the LDAP server much more complicated, because it must store and retrieve directory entries. These LDAP servers are often called stand-alone LDAP servers because they do not depend on an X.500 directory server. Because LDAP does not support all X.500 capabilities, a stand-alone LDAP server only needs to support the capabilities required by LDAP.

*Figure 12-15 Stand-alone LDAP server*

LDAP

Client

LDAP

Server

Directory

TCP/IP

The concept of the LDAP server being able to provide access to local directories supporting the X.500 model, rather than acting only as a gateway to an X.500 server, is discussed in RFC 4511 (see Table 12-4 on page 460). From the client's

point of view, any server that implements the LDAP protocol is an LDAP directory server, whether the server actually implements the directory or is a gateway to an X.500 server. The directory that is accessed can be called an LDAP directory, whether the directory is implemented by a stand-alone LDAP server or by an X.500 server.

#### 12.4.3 Overview of LDAP architecture

LDAP defines the content and format of messages exchanged between an LDAP client and an LDAP server. The messages specify the operations requested by the client (search, modify, delete, and so on), the responses from the server, and the format of data carried in the messages. LDAP messages are carried over TCP/IP, a connection-oriented protocol, so there are also operations to establish and disconnect a session between the client and server.

The general interaction between an LDAP client and an LDAP server takes the following form:

1. The client establishes a session with an LDAP server. This is known as *binding* to the server. The client specifies the host name or IP address and TCP/IP port number where the LDAP server is listening. The client can provide a user name and a password to properly authenticate with the server, or the client can establish an anonymous session with default access rights. The client and server can also establish a session that uses stronger security methods, such as encryption of data (see 12.4.5, “LDAP security” on page 471).
2. The client then performs operations on directory data. LDAP offers both read and update capabilities. This allows directory information to be managed as well as queried. LDAP supports searching the directory for data meeting arbitrary user-specified criteria. Searching is the most common operation in LDAP. A user can specify what part of the directory to search and what information to return. A search filter that uses Boolean conditions specifies which directory data matches the search.
3. When the client has finished making requests, it closes the session with the server. This is also known as *unbinding*.

Because LDAP was originally intended as a lightweight alternative to DAP for accessing X.500 directories, the LDAP server follows an X.500 model. The directory stores and organizes data structures known as entries. A directory entry usually describes an object such as a person, a printer, a server, and so on. Each entry has a name called a distinguished name (DN) that uniquely identifies it. The DN consists of a sequence of parts called relative distinguished names (RDNs), much like a file name can consist of a path of directory names. The entries can be arranged into a hierarchical tree-like structure based on their distinguished names. This tree of directory entries is called the directory information tree (DIT).

LDAP defines operations for accessing and modifying directory entries, such as:

Searching for entries meeting user-specified criteria

Adding an entry

Deleting an entry

Modifying an entry

Modifying the distinguished name or relative distinguished name of an entry (move)

Comparing an entry

#### 12.4.4 LDAP models

LDAP can be better understood by considering the four models upon which it is based:

|  |  |
| --- | --- |
| **Information** | Describes the structure of information stored in an LDAP directory. |
| **Naming** | Describes how information in an LDAP directory is organized and identified. |
| **Functional** | Describes the operations that can be performed on the information stored in an LDAP directory. |
| **Security** | Describes how the information in an LDAP directory can be protected from unauthorized access. |

The following sections discuss the first three LDAP models. We describe LDAP security in 12.4.5, “LDAP security” on page 471.

##### The information model

The basic unit of information stored in the directory is an entry, which represents an object of interest in the real world such as a person, server, or organization. Each entry contains one or more attributes that describe the entry. Each attribute has a type and one or more values. For example, the directory entry for a person might have an attribute called telephoneNumber. The syntax of the telephoneNumber attribute specifies that a telephone number must be a string of numbers that can contain spaces and hyphens. The value of the attribute is the person's telephone number, such as 123-456-7890 (a person might have multiple telephone numbers, in which case this attribute would have multiple values).

In addition to defining what data can be stored as the value of an attribute, an attribute syntax also defines how those values behave during searches and other directory operations. This is done using syntax and matching rules. The attribute telephoneNumber, for example, might have a syntax that specifies:

Lexicographic ordering.

Case, spaces, and dashes are ignored during the comparisons. Values must be character strings.

For example, using the correct definitions, the telephone numbers

123-456-7890, 123456-7890, and 1234567890 are considered to be the same. A few of the common syntaxes and matching rules, defined in RFC 4517, are listed in Table 12-5.

*Table 12-5 Examples of LDAP syntaxes*

|  |  |
| --- | --- |
| **Syntaxes and matching rules** | **Description** |
| Bit String | A sequence of binary digits |
| Postal Address | A sequence of strings that form an address in a physical mail system |
| caseExactMatch | A matching rule requiring that string comparisons are case-sensitive |
| caseIgnoreMatch | A matching rule that does not require case-sensitive comparisons |

Table 12-6 lists some common attributes defined by RFC 4519. Some attributes have alias names that can be used wherever the full attribute name is used.

*Table 12-6 Examples of LDAP syntaxes*

|  |  |  |  |
| --- | --- | --- | --- |
| **Attribute, alias** | **Syntax** | **Description** | **Example** |
| commonName, cn | cis | Common name of an entry | John Smith |
| surname, sn | cis | A person’s last name | Smith |
| initials | cis | A person’s initials | JS |
| telephoneNumber | tel | A person’s telephone number | 123-456-7890 |

An object class is a general description, sometimes called a template, of an object type, as opposed to the description of a specific object of that type. For example, the object class *person* has a surname attribute, while the object describing John Smith has a surname attribute with the value *Smith*. The object classes that a directory server can store and the attributes they contain are described by a *schema*. A schema defines where object classes are allowed in the directory, which attributes they must contain, which attributes are optional, and the syntax of each attribute. For example, a schema might define a *person* object class that requires that a person has a character-string surname attribute, can optionally have a number-string telephoneNumber attribute, and so on. Schema-checking ensures that all required attributes for an entry are present before an entry is stored. Schemas also define the inheritance and subclassing of objects, and where in the DIT structure (hierarchy) objects can appear.

Though an implementation can define any schema to meet its needs, RFC 4519 defines a few standard schemas. Table 12-7 lists a few of the common schema (object classes and their required attributes). In many cases, an entry can consist of more than one object class.

*Table 12-7 Examples of object classes and required attributes*

|  |  |  |
| --- | --- | --- |
| **Object class** | **Description** | **Attributes** |
| country | Defines a country | Required: countryCode Optional: searchGuide description |
| locality | Defines a place in the physical world | Required:  None  Optional: street seeAlso searchGuide description |
| person | Defines a person | Required:  surname commonName  Optional:  userPassword telephoneNumber seeAlso description |

Because servers can define their own schema, LDAP includes the functionality of allowing a client to query a server for the contents of the supported schema.

##### The naming model

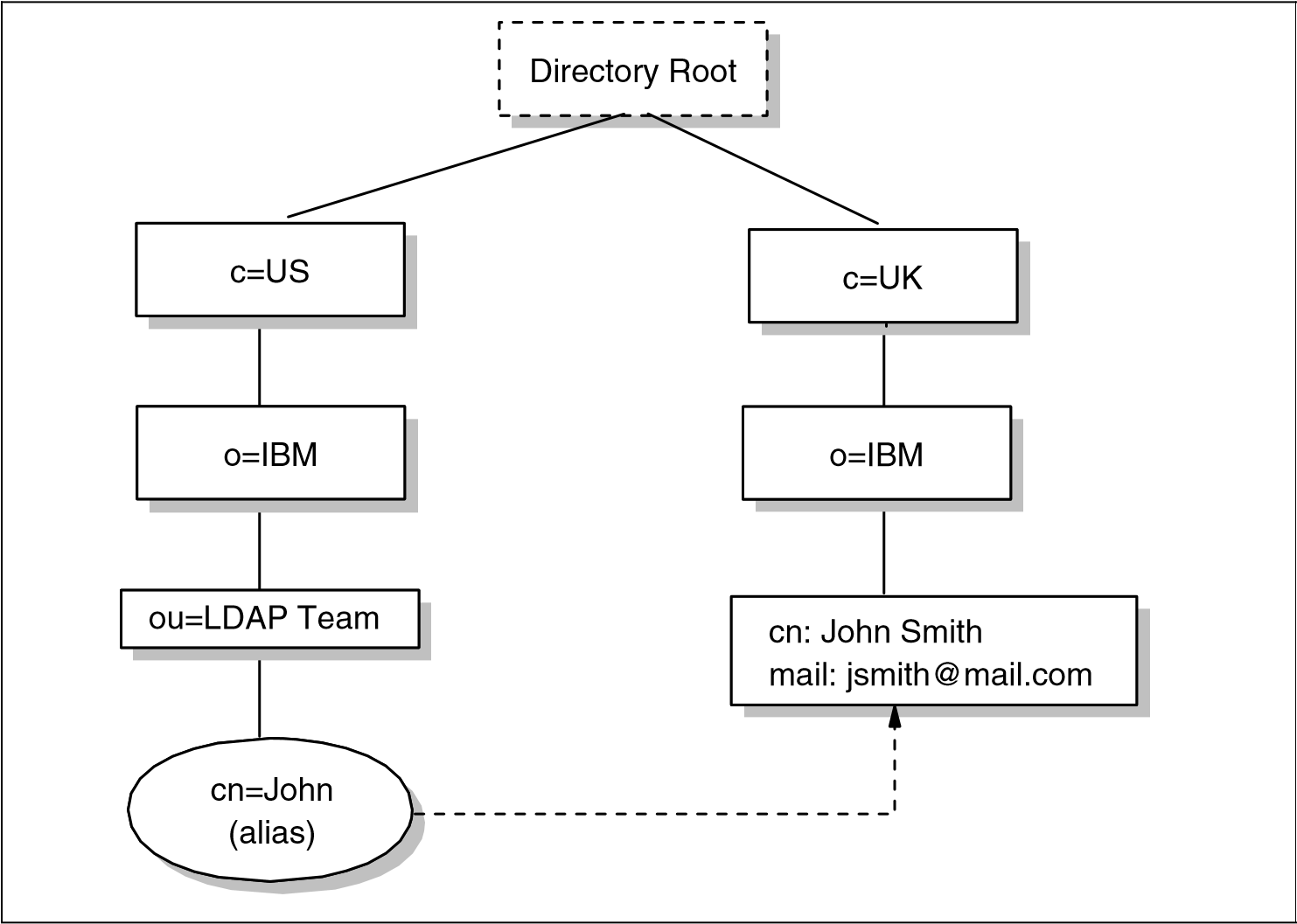
The LDAP naming model defines how entries are identified and organized.

Entries are organized in a tree-like structure called the directory information tree

(DIT). Entries are arranged within the DIT based on their distinguished name (DN). A DN is a unique name that unambiguously identifies a single entry. DNs are made up of a sequence of relative distinguished names (RDNs). Each RDN in a DN corresponds to a branch in the DIT leading from the root of the DIT to the directory entry.

Each RDN is derived from the attributes of the directory entry. In the simple and common case, an RDN has the form <attribute-name>=<value>. A DN is composed of a sequence of RDNs separated by commas. These relationships are defined in RFC 4514.

An example of a DIT is shown in Figure 12-16. The example is very simple, but can be used to illustrate some basic concepts. Each box represents a directory entry. The root directory entry is conceptual and does not actually exist. Attributes are listed inside each entry. The list of attributes shown is not complete. For example, the entry for the country UK (c=UK) could have an attribute called description with the value United Kingdom.



*Figure 12-16 Example of a directory information tree (DIT)*

It is usual to follow either a geographical or an organizational scheme to position entries in the DIT. For example, entries that represent countries would be at the top of the DIT. Below the countries would be national organizations, states, and provinces, and so on. Below this level, entries might represent people within those organizations or further subdivisions of the organization. The lowest layers of the DIT entries can represent any object, such as people, printers, application servers, and so on. The depth or breadth of the DIT is not restricted and can be designed to suit application requirements.

Entries are named according to their position in the DIT. The directory entry in the lower-right corner of Figure 12-16 on page 467 has the DN cn=John Smith,o=IBM,c=UK.

**Note:** DNs read from leaf-to-root, as opposed to names in a file system directory, which usually read from root-to-leaf.

The DN is made up of a sequence of RDNs. Each RDN is constructed from an attribute (or attributes) of the entry it names. For example, the DN cn=John Smith,o=IBM,c=UK is constructed by adding the RDN cn=John Smith to the DN of the ancestor entry o=IBM,c=UK.

The DIT is described as being tree-like, implying that it is not a tree. This is because of aliases. Aliases allow the tree structure to be circumvented. This can be useful if an entry belongs to more than one organization or if a commonly used DN is too complex. Another common use of aliases is when entries are moved within the DIT and you want access to continue to work as before. In Figure 12-16 on page 467, cn=John,ou=LDAP Team,o=IBM,c=US is an alias for cn=John Smith,o=IBM,c=UK.

Because an LDAP directory can be distributed, an individual LDAP server might not store the entire DIT. Instead, it might store the entries for a particular department but not the entries for the ancestors of the department. For example, a server might store the entries for the Accounting department at Yredbookscorp. The highest node in the DIT stored by the server would be ou=Accounting,o=Yredbookscorp,c=US. The server would store entries ou=Accounting,o=Yredbookscorp,c=US but not for c=US or for o=Yredbookscorp,c=US. The highest entry stored by a server is called a *suffix*. Each entry stored by the server ends with this suffix, so in this case, the suffix is the entire ou=Accounting,o=Yredbookscorp,c=US.

A single server can support multiple suffixes. For example, in addition to storing information about the Accounting department, the same server can store information about the Sales department at MyCorp. The server then has the suffixes ou=Accounting,o=Yredbookscorp,c=US and ou=Sales,o=MyCorp,c=US. Because a server might not store the entire DIT, servers need to be linked together in some way in order to form a distributed directory that contains the entire DIT. This is accomplished with *referrals*. A referral acts as a pointer to an entry on another LDAP server where requested information is stored. A referral is an entry of objectClass *referral*. It has an attribute, *ref*, whose value is the LDAP URL of the referred entry on another LDAP server. See 12.4.6, “LDAP URLs” on page 474 for further information. Referrals allow a DIT to be partitioned and distributed across multiple servers. Portions of the DIT can also be replicated. This can improve performance and availability.

**Note:** When an application uses LDAP to request directory information from a server, but the server only has a referral for that information, the LDAP URL for that information is passed to the client. It is then the responsibility of that client to contact the new server to obtain the information. This is unlike the standard mechanisms of both DCE and X.500, where a directory server, if it does not contain the requested information locally, will always obtain the information from another server and pass it back to the client.

##### The functional model

LDAP defines operations for accessing and modifying directory entries. LDAP operations can be divided into the following three categories:

**Query** Includes the search and compare operations used to

retrieve information from a directory.

**Update** Includes the add, delete, modify, modify RDN, and

unsolicited notification operations used to update stored information in a directory. These operations will normally be carried out by an administrator.

**Authentication** Includes the bind, unbind, abandon, and startTLS operations used to connect and disconnect to and from an LDAP server, establish access rights, and protect information. For further information, see 12.4.5, “LDAP security” on page 471.

###### The search operation

The most common operation is the search. This operation is very flexible and therefore has some of the most complex options. The search operation allows a client to request that an LDAP server search through some portion of the DIT for information meeting user-specified criteria in order to read and list the results.

The search can be very general or very specific. The search operation allows the specification of the starting point within the DIT, how deep within the DIT to search, the attributes an entry must have to be considered a match, and the attributes to return for matched entries.

Some example searches expressed informally are:

Find the postal address for cn=John Smith,o=IBM,c=UK.

Find all the entries that are children of the entry ou=ITSO,o=IBM,c=US.

Find the e-mail address and phone number of anyone in an organization whose last name contains the characters “miller” and who also has a fax number.

To perform a search, the following parameters must be specified:

**Base** A DN that defines the starting point, called the base

object, of the search. The base object is a node within the DIT.

**Scope** Specifies how deep within the DIT to search from the base object. There are three choices: **baseObject** Only the base object is examined.

**singleLevel** Only the immediate children of the base object are examined; the base object itself is not examined.

**wholeSubtree** The base object and all of its

descendants are examined.

**Alias dereferencing** Specifies if aliases are dereferenced. That is, the actual object of interest, pointed to by an alias entry, is examined. Not dereferencing aliases allows the alias entries themselves to be examined. This parameter must be one of the following:

**neverDerefAliases**

Do not deference aliases.

derefInSearching

Dereference aliases only when searching subordinates of the base object.

derefFindingBaseObj

Dereference aliases only when searching for the base object, but not when searching subordinates of the base object.

**derefAlways** Always dereference aliases.

**Size Limit** The maximum number of entries that should be returned as a result of the search.

**Time Limit** The maximum number of seconds allowed to perform the

search. Specifying zero indicates that there is no time limit.

**Types Only** This parameter has two possible values:

|  |  |
| --- | --- |
| **TRUE** | Only attribute descriptions are returned. |
| **FALSE** | Attribute descriptions and values are returned. |

**Search filter** Specifies the criteria an entry must match to be returned from a search. The search filter is a Boolean combination of attribute value assertions. An attribute value assertion tests the value of an attribute for equality, less than or equal, and so on.

**Attributes to return** Specifies which attributes to retrieve from entries that match the search criteria. Because an entry can have many attributes, this allows the user to only see the attributes in which they are interested.

#### 12.4.5 LDAP security

Security is of great importance in the networked world of computers, and this is true for LDAP as well. When sending data over insecure networks, internally or externally, sensitive information might need to be protected during transportation. There is also a need to know who is requesting the information and who is sending it. This is especially important when it comes to the update operations on a directory. RFC 4513 discusses the authentication methods and security mechanisms available in LDAPv3, which can be divided into the following sections:

|  |  |
| --- | --- |
| **Authentication** | Assurance that the opposite party (machine or person) really is who he/she/it claims to be. |
| **Integrity** | Assurance that the information that arrives is really the same as what was sent. |
| **Confidentiality** | Protection against information disclosure, by means of data encryption, to those who are not intended to receive it. |
| **Authorization** | Assurance that a party is really allowed to do what it is requesting to do, usually checked after user  authentication. Authorization is achieved by assigning access controls, such as read, write, or delete, for user IDs or common names to the resources being accessed. Because these attributes are usually platform-specific,  LDAP does not provide specific controls. Instead, it has |

built-in mechanisms to allow the use of the platform-specific controls.

Because the use of authorization controls is platform-specific, the following sections describe only the authentication, integrity, and confidentiality. There are several mechanisms that can be used for this purpose; the most important ones are discussed here. These are:

No authentication

Basic authentication

Simple Authentication and Security Layer (SASL)

Transport Layer Security (TLS)

The security mechanism to be used in LDAP is negotiated when the connection between the client and the server is established.

##### No authentication

No authentication should only be used when data security is not an issue and when no special access control permissions are involved. This might be the case, for example, when your directory is an address book browsable by anybody. No authentication is assumed when you leave the password and DN field empty in the bind API call. The LDAP server then automatically assumes an anonymous user session and grants access with the appropriate access controls defined for this kind of access (not to be confused with the SASL anonymous user discussed in “Simple Authentication and Security Layer (SASL)”).

##### Basic authentication

Basic authentication is also used in several other Web-related protocols, such as HTTP. When using basic authentication with LDAP, the client identifies itself to the server by means of a DN and a password, which are sent in the clear over the network (some implementations might use Base64 encoding instead). The server considers the client authenticated if the DN and password sent by the client matches the password for that DN stored in the directory. Base64 encoding is defined in the Multipurpose Internet Mail Extensions, or MIME (see 15.3, “Multipurpose Internet Mail Extensions (MIME)” on page 571). Base64 is a relatively simple encryption, and it is not hard to break after the data has been captured in the network.

##### Simple Authentication and Security Layer (SASL)

SASL is a framework for adding additional authentication mechanisms to connection-oriented protocols, and is defined in RFC 4422. It has been added to LDAPv3 to overcome the authentication shortcomings of Version 2. SASL was originally devised to add stronger authentication to the IMAP protocol (see 15.5, “Internet Message Access Protocol (IMAP4)” on page 591), but has since evolved into a more general system for mediating between protocols and authentication systems.

In SASL, connection protocols, such as LDAP, IMAP, and so on, are represented by profiles; each profile is considered a protocol extension that allows the protocol and SASL to work together. A complete list of SASL profiles can be obtained from the Information Sciences Institute (ISI). Among these are IMAP, SMTP, POP, and LDAP. Each protocol that intends to use SASL needs to be extended with a command to identify an authentication mechanism and to carry out an authentication exchange. Optionally, a security layer can be negotiated to encrypt the data after authentication and ensure confidentiality. LDAPv3 includes such a command (**ldap\_sasl\_bind()** or **ldap\_sasl\_bind\_s()**). The key parameters that influence the security method used are:

|  |  |
| --- | --- |
| **dn** | This is the distinguished name of the entry which is to bind. This can be thought of as the user ID in a normal user ID and password authentication. |
| **mechanism** | This is the name of the security method to use. Valid security mechanisms are, currently:  **OTP** The One Time Password mechanism  (defined in RFC 2444).  **GSSAPI** The Generic Security Services Application Program Interface (defined in RFC 2743).  **CRAM-MD5** The Challenge/Response Authentication Mechanism (defined in RFC 2195), based on the HMAC-MD5 MAC algorithm.  **DIGEST-MD5** An HTTP Digest-compatible CRAM based on the HMAC -MD5 MAC algorithm.  **EXTERNAL** An external mechanism. Usually this is TLS, discussed in “Transport Layer Security (TLS)” on page 474.  **ANONYMOUS** Unauthenticated access. |
| **credentials** | This contains the arbitrary data that identifies the DN. The format and content of the parameter depends on the mechanism chosen. If it is, for example, the ANONYMOUS  mechanism, it can be an arbitrary string or an e-mail address that identifies the user. |

SASL provides a high-level framework that lets the involved parties decide on the particular security mechanism to use. The SASL security mechanism negotiation between client and server is done in the clear. After the client and the server agree on a common mechanism, the connection is secure against modifying the authentication identities. However, an attacker might try to eavesdrop the mechanism negotiation and cause a party to use the least secure mechanism. In order to prevent this from happening, configure clients and servers to use a minimum security mechanism, provided they support such a configuration option. As stated earlier, SSL and its successor, TLS, are the mechanisms commonly used in SASL for LDAP. For details about these protocols, refer to 22.7, “Secure Sockets Layer (SSL)” on page 854.

Because no data encryption method was specified in LDAPv2, some vendors added their own SSL calls to the LDAP API. A potential drawback of such an approach is that the API calls might not be compatible among different vendor implementations. The use of SASL, as specified in LDAPv3, assures compatibility, although it is likely that vendor products will support only a subset of the possible range of mechanisms (possibly only SSL).

##### Transport Layer Security (TLS)

Transport Layer Security (TLS) is available through the SASL EXTERNAL method, described earlier. An LDAP client can opt to secure a session using TLS at any point during a transaction with an LDAP server, except when:

The session is already TLS protected.

A multi-stage SASL negotiation is in progress.

The client is awaiting a response from an operation request.

To request that TLS be set up on the session, the client sends a *StartTLS* message to the server. This enables the client and server to exchange certificates. RFC 4513 requires that, in addition to this, the client verifies the server’s identity using the DNS or IP address presented in the server’s certificate. This prevents a client’s attempt to connect to a server from being intercepted by malicious user, who might then stage a *man-in-the-middle* attack. After this has occurred, the client and server can negotiate a ciphersuite.

#### 12.4.6 LDAP URLs

Because LDAP has become an important protocol on the Internet, a URL format for LDAP resources has been defined in RFC 4516. LDAP URLs begin with ldap:// or ldaps://, if the LDAP server communicates using SSL. LDAP URLs can simply name an LDAP server, or can specify a complex directory search.

Some examples help make the format of LDAP URLs clear. The following example refers to the LDAP server on the host ldpserv.mydiv.mycorp.com (using the well-known port 389):

ldap://ldpserv.mydiv.mycorp.com/

Additionally, search options can be specified in the URL. The following example retrieves all the attributes for the DN ou=Accounting,c=US from the LDAP server on host ldpserv.mydiv.mycorp.com. In this case, nonstandard port 4389 is explicitly specified here as an example. ldap://ldpserv.mydiv.mycorp.com:4389/ou=Accounting,c=US

The following example retrieves all the attributes for the DN cn=JohnSmith,ou=Sales,o=myCorp,c=US. Note that some characters are considered unsafe in URLs because they can be removed or treated as delimiters by some programs. Unsafe characters such as space, comma, brackets, and so forth need to be represented by their hexadecimal value preceded by the percent sign: ldap://ldpserv.mydiv.mycorp.com/cn=John%20Smith,o=myCorp,c=US

In this example, %20 is a space. More information about unsafe characters and URLs in general are in RFC 4516.

In addition to options, the URL can specify what values attributes are to be returned using the ? symbol. For example, assume we want to find the U.S. address of myCorp. We use the following URL: ldap://ldpserv.mydiv.mycorp.com:4389/o=myCorp,c=US?postalAddress

#### 12.4.7 LDAP and DCE

DCE has its own Cell Directory Service, or CDS (see 13.3.1, “DCE directory service” on page 498). If applications never access resources outside of their DCE cell, only CDS is required. However, if an application needs to communicate with resources in other DCE cells, the Global Directory Agent (GDA) is required. The GDA accesses a global (that is, non-CDS) directory where the names of

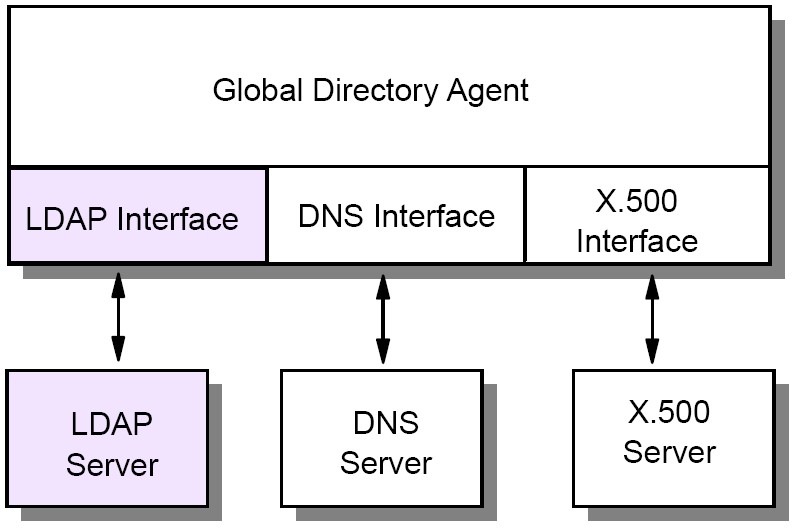
DCE cells can be registered. This global directory (GDS) can be either a Domain Name System (DNS) directory or an X.500 directory. The GDA retrieves the address of a CDS server in the remote cell. The remote CDS can then be contacted to find DCE resources in that cell. Using the GDA enables an organization to link multiple DCE cells together using either a private directory on an intranet or a public directory on the Internet.

In view of LDAP's strong presence in the Internet, two LDAP projects have been sponsored by The Open Group to investigate LDAP integration with DCE technology.

##### LDAP interface for the GDA

One way LDAP is being integrated into DCE is to allow DCE cells to be registered in LDAP directories. The GDA in a cell that wants to connect to remote cells is configured to enable access to the LDAP directory (see Figure 12-17).

*Figure 12-17 The LDAP interface for GDA*



DCE originally only supported X.500 and DNS name syntax for cell names. LDAP and X.500 names both follow the same hierarchical naming model, but their syntax is slightly different. X.500 names are written in reverse order and use a slash (/) rather than a comma (,) to separated relative distinguished names. When the GDA is configured to use LDAP, it converts cell names in X.500 format into the LDAP format.

##### LDAP interface for the CDS

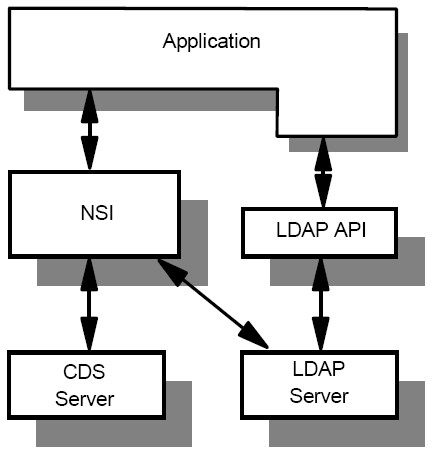
DCE provides two programming interfaces to the Directory Service; Name

Service Interface (NSI) and the X/Open Directory Service (XDS). XDS is an X.500-compatible interface used to access information in the GDS, and it can also be used to access information in the CDS. However, the use of NSI is much more common in DCE applications. The NSI API provides functionality that is

specifically tailored for use with DCE client and server programs that use RPC. NSI allows servers to register their address and the type of RPC interface they support. This address/interface information is called an RPC binding, and is needed by clients that want to contact the server. NSI allows clients to search the CDS for RPC binding information.

NSI was designed to be independent of the directory where the RPC bindings are stored. However, the only supported directory to date has been CDS. NSI will be extended to also support adding and retrieving RPC bindings from an LDAP directory. This will allow servers to advertise their RPC binding information in either CDS or an LDAP directory. Application programs can use either the NSI or the LDAP API when an LDAP directory is used (see Figure 12-18).

*Figure 12-18 The LDAP interface for NSI*



#### 12.4.8 The Directory-Enabled Networks (DEN) initiative

In September 1997, Cisco Systems Inc. and Microsoft® Corp. announced the so-called Directory-Enabled Networks (DEN) initiative as a result of a collaborative work. Many companies, such as IBM, either support this initiative or

actively participate in ad hoc working groups (ADWGs). DEN represents an information model specification for an integrated directory that stores information about people, network devices, and applications. The DEN schema defines the object classes and their related attributes for those objects. As such, DEN is a key piece to building intelligent networks, where products from multiple vendors can store and retrieve topology and configuration-related data.

Of special interest is that the DEN specification defines LDAPv3 as the core protocol for accessing DEN information, which makes information available to LDAP-enabled clients or network devices, or both.

DEN makes use of the Common information Model (CIM). CIM details a way of integrating different management models such as SNMP MIBs and DMTF MIFs. At the time of writing, the most current CIM schema was version 2.12, released in April of 2006.

More information about the DEN initiative can be found on the founder’s Web at:

<http://www.dmtf.org/standards/wbem/den/><http://www.dmtf.org/standards/cim/>

#### 12.4.9 Web-Based Enterprise Management (WBEM)

WBEM is a set of standards designed to deliver an integrated set of management tools for the enterprise. By making use of XML and CIM, it becomes possible to manage network devices, desktop systems, telecom systems and application systems, all from a Web browser. For further information, see: <http://www.dmtf.org/standards/wbem/>

### 12.5 RFCs relevant to this chapter

The following RFCs provide detailed information about the directory and naming protocols and architectures presented throughout this chapter:

[RFC 1032 – Domain administrators guide (November 1987)](http://www.ietf.org/rfc/rfc1032.txt)

[RFC 1033 – Domain administrators operations guide (November 1987)](http://www.ietf.org/rfc/rfc1033.txt)

[RFC 1034 – Domain names - concepts and facilities (November 1987)](http://www.ietf.org/rfc/rfc1034.txt)

[RFC 1035 – Domain names - implementation and specifications](http://www.ietf.org/rfc/rfc1035.txt)

[(November](http://www.ietf.org/rfc/rfc1035.txt) [1987)](http://www.ietf.org/rfc/rfc1035.txt)

[RFC 1101 – DNS encoding of network names and other types (April 1989)](http://www.ietf.org/rfc/rfc1101.txt)

[RFC 1183 – New DNS RR Definitions (October 1990)](http://www.ietf.org/rfc/rfc1183.txt)

[RFC 1202 – Directory Assistance service (February 1991)](http://www.ietf.org/rfc/rfc1202.txt)

[RFC 1249 – DIXIE Protocol Specification (August 1991)](http://www.ietf.org/rfc/rfc1249.txt)

[RFC 1348 – DNS NSAP RRs (July 1992)](http://www.ietf.org/rfc/rfc1348.txt)

[RFC 1480 – The US Domain (June 1993)](http://www.ietf.org/rfc/rfc1480.txt)

[RFC 1706 – DNS NSAP Resource Records (October 1994)](http://www.ietf.org/rfc/rfc1706.txt)

[RFC 1823 – The LDAP Application Programming Interface (August 1995)](http://www.ietf.org/rfc/rfc1823.txt)

[RFC 1876 – A Means for Expressing Location Information in the Domain](http://www.ietf.org/rfc/rfc1876.txt)

[Name System (January 1996)](http://www.ietf.org/rfc/rfc1876.txt)

[RFC 1995 – Incremental Zone Transfer in DNS (August 1996)](http://www.ietf.org/rfc/rfc1995.txt)

[RFC 1996 – A Mechanism for Prompt Notification of Zone Changes (DNS](http://www.ietf.org/rfc/rfc1996.txt)

[NOTIFY) (August 1996)](http://www.ietf.org/rfc/rfc1996.txt)

[RFC 2136 – Dynamic Updates in the Domain Name System (DNS UPDATE) (April 1997)](http://www.ietf.org/rfc/rfc2136.txt)

[RFC 2444 – The One-time-Password SASL Mechanism (October 1998)](http://www.ietf.org/rfc/rfc2444.txt)

RFC 4592 – The Role of Wildcards in the Domain Name System (July 2006)

[RFC 2743 – Generic Security Service Application Program Interface Version](http://www.ietf.org/rfc/rfc2743.txt)

[2, Update 1 (January 2000)](http://www.ietf.org/rfc/rfc2743.txt)

[RFC 2874 – DNS Extensions to Support IPv6 Address Aggregation and](http://www.ietf.org/rfc/rfc2874.txt)

[Renumbering (July 2000)](http://www.ietf.org/rfc/rfc2874.txt)

[RFC 3007 – Secure Domain Name Systems (DNS) Dynamic Update](http://www.ietf.org/rfc/rfc3007.txt)

[(November 2000)](http://www.ietf.org/rfc/rfc3007.txt)

[RFC 3494 – Lightweight Directory Access protocol version 2 (LDAPv2) (March 2003)](http://www.ietf.org/rfc/rfc3494.txt)

[RFC 3596 – DNS Extensions to Support IP Version 6 (October 2003)](http://www.ietf.org/rfc/rfc3596.txt)

[RFC 3645 – Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG) (October 2003)](http://www.ietf.org/rfc/rfc3645.txt)

[RFC 3901 – DNS IPv6 Transport Operational Guidelines (September 2004)](http://www.ietf.org/rfc/rfc3901.txt)

[RFC 4033 – DNS Security Introduction and Requirements (March 2005)](http://www.ietf.org/rfc/rfc4033.txt)

[RFC 4034 – Resource Records for the DNS Security Extensions](http://www.ietf.org/rfc/rfc4034.txt)

[(March](http://www.ietf.org/rfc/rfc4034.txt) [2005)](http://www.ietf.org/rfc/rfc4034.txt)

[RFC 4035 – Protocol Modifications for the DNS Security Extensions](http://www.ietf.org/rfc/rfc4035.txt)

[(March](http://www.ietf.org/rfc/rfc4035.txt) [2005)](http://www.ietf.org/rfc/rfc4035.txt)

[RFC 4339 – IPv6 Host Configuration of DNS Server Information Approaches (February 2006)](http://www.ietf.org/rfc/rfc4339.txt)

[RFC 4398 – Storing Certificates in the Domain Name System (DNS)](http://www.ietf.org/rfc/rfc4398.txt)

[(March](http://www.ietf.org/rfc/rfc4398.txt) [2006)](http://www.ietf.org/rfc/rfc4398.txt)

[RFC 4422 – Simple Authentication and Security Layer (SASL) (June 2006)](http://www.ietf.org/rfc/rfc4422.txt)

[RFC 4501 – Domain Name System Uniform Resource Identifiers (May 2006)](http://www.ietf.org/rfc/rfc4501.txt) [RFC 4505 – Anonymous Simple Authentication and Security Layer (SASL) (June 2006)](http://www.ietf.org/rfc/rfc4505.txt)

[RFC 4510 – Lightweight Directory Access Protocol (LDAP): Technical](http://www.ietf.org/rfc/rfc4510.txt)

[Specification Road Map (June 2006)](http://www.ietf.org/rfc/rfc4510.txt)

[RFC 4511 – Lightweight Directory Access Protocol (LDAP): The Protocol (June 2006)](http://www.ietf.org/rfc/rfc4511.txt)

[RFC 4512 – Lightweight Directory Access Protocol (LDAP): Directory](http://www.ietf.org/rfc/rfc4512.txt)

[Information Models (June 2006)](http://www.ietf.org/rfc/rfc4512.txt)

[RFC 4513 – Lightweight Directory Access Protocol (LDAP): Authentication](http://www.ietf.org/rfc/rfc4513.txt)

[Methods and Security Mechanisms (June 2006)](http://www.ietf.org/rfc/rfc4513.txt)

[RFC 4514 – Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names (June 2006)](http://www.ietf.org/rfc/rfc4514.txt)

[RFC 4515 – Lightweight Directory Access Protocol (LDAP): String](http://www.ietf.org/rfc/rfc4515.txt)

[Representation of Search Filters (June 2006)](http://www.ietf.org/rfc/rfc4515.txt)

[RFC 4516 – Lightweight Directory Access Protocol (LDAP): Uniform](http://www.ietf.org/rfc/rfc4516.txt)

[Resource Locator (June 2006)](http://www.ietf.org/rfc/rfc4516.txt)

[RFC 4517 – Lightweight Directory Access Protocol (LDAP): Syntaxes and](http://www.ietf.org/rfc/rfc4517.txt)

[Matching Rules (June 2006)](http://www.ietf.org/rfc/rfc4517.txt)

[RFC 4518 – Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation (June 2006)](http://www.ietf.org/rfc/rfc4518.txt)

[RFC 4519 – Lightweight Directory Access Protocol (LDAP): Schema for User Applications (June 2006)](http://www.ietf.org/rfc/rfc4519.txt)

[RFC 4520 – Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP) (June 2006)](http://www.ietf.org/rfc/rfc4520.txt)

[RFC 4521 – Considerations for Lightweight Directory Access Protocol](http://www.ietf.org/rfc/rfc4521.txt)

[(LDAP) (June 2006)](http://www.ietf.org/rfc/rfc4521.txt)

[RFC 4522 – Lightweight Directory Access Protocol (LDAP): The Binary](http://www.ietf.org/rfc/rfc4522.txt)

[Encoding Option (June 2006)](http://www.ietf.org/rfc/rfc4522.txt)

[RFC 4523 – Lightweight Directory Access Protocol (LDAP): Schema](http://www.ietf.org/rfc/rfc4523.txt)

[Definitions for X.509 Certificates (June 2006)](http://www.ietf.org/rfc/rfc4523.txt)

[RFC 4524 – Lightweight Directory Access Protocol (LDAP): COSINE/LDAP X.500 Schema (June 2006)](http://www.ietf.org/rfc/rfc4524.txt)

[RFC 4525 – Lightweight Directory Access Protocol (LDAP): Modify-Increment](http://www.ietf.org/rfc/rfc4525.txt)

[Extension (June 2006)](http://www.ietf.org/rfc/rfc4525.txt)

[RFC 4526 – Lightweight Directory Access Protocol (LDAP): Absolute True and False Filters (June 2006)](http://www.ietf.org/rfc/rfc4526.txt)

[RFC 4527 – Lightweight Directory Access Protocol (LDAP): Read Entry Controls (June 2006)](http://www.ietf.org/rfc/rfc4527.txt)

[RFC 4528 – Lightweight Directory Access Protocol (LDAP): Assertion Control (June 2006)](http://www.ietf.org/rfc/rfc4528.txt)

[RFC 4529 – Requesting Attributes by Object Class in the Lightweight](http://www.ietf.org/rfc/rfc4529.txt)

[Directory Access Protocol (LDAP) (June 2006)](http://www.ietf.org/rfc/rfc4529.txt)

[RFC 4530 – Lightweight Directory Access Protocol (LDAP): entryUUID](http://www.ietf.org/rfc/rfc4530.txt)

[Operational Attribute (June 2006)](http://www.ietf.org/rfc/rfc4530.txt)

[RFC 4531 – Lightweight Directory Access Protocol (LDAP): Turn Operation (June 2006)](http://www.ietf.org/rfc/rfc4531.txt)

[RFC 4532 – Lightweight Directory Access Protocol (LDAP): “Who Am I?”](http://www.ietf.org/rfc/rfc4532.txt)

[Operation (June 2006)](http://www.ietf.org/rfc/rfc4532.txt)

[RFC 4533 – Lightweight Directory Access Protocol (LDAP): Content](http://www.ietf.org/rfc/rfc4533.txt)

[Synchronization Operation (June 2006)](http://www.ietf.org/rfc/rfc4533.txt)

|  |  |  |
| --- | --- | --- |
|  | |  | | --- | | **17** | |

## Chapter 17. Network management

With the growth in size and complexity of the TCP/IP-based internetworks the need for network management became very important. To address this, in 1988

the Internet Architecture Board (IAB) issued RFC 1052 detailing its recommendation to achieve this management. The suggestion adopted two different approaches:

The Simple Network Management Protocol (SNMP)

ISO Common Management Information Services/Common Management

Information Protocol (CMIS/CMIP)

The original plan detailed by RFC 1052 involved using SNMP as a short-term solution to the network management problem. The development of SNMP was to be kept simple, facilitating rapid deployment of the protocol throughout the Internet community. After the immediate management needs were met, albeit temporarily, by SNMP, thorough research and development could be performed on CMIS/CMIP. Ultimately, this protocol would then be deployed as a permanent solution, replacing SNMP.

However, this plan allowed SNMP to gain widespread usage throughout the

Internet community. As a result, CMIS/CMIP was never fully deployed. In fact, only two RFCs describing CMIS/CMIP were released. RFC 1095, which described the CMIS protocol over TCP/IP (CMOT) was released in 1989. It was ultimately obsoleted by RFC 1189, released in 1990, which proposed the standard for CMOT and CMIP. The status of RFC 1189 is currently historic, and is not widely used in today’s networks.

© Copyright IBM Corp. 1989-2006. All rights reserved.

Given these circumstances, this chapter discusses the SNMP model and implementation. Also included is a discussion on the NETSTAT utility. Though this command is not RFC defined, it is available on most platforms and is useful in both monitoring and managing local connections on a system.

### 17.1 The Simple Network Management Protocol (SNMP)

The fundamental use of the Simple Network Management Protocol (SNMP) is to manage all aspects of a network, as well as applications related to that network. To do this, SNMP has been architected to perform two services:

Monitor: SNMP implementations allow network administrators to monitor their networks in order to--among other things--ensure the health of the network, forecast usage and capacity, and in problem determination. Aspects which can be monitored vary in granularity, and can be something as global as the total amount of IP traffic experienced on a single host, or can be as minute as the current status of a single TCP connection.

Additionally, the SNMP architecture allows components of the SNMP model to notify network administrators should a problem occur on a network. For example, if a link were to break or an interface to deactivate for some reason, SNMP can send a message to alert network administrators that this has occurred.

Manage: In addition to monitoring a network, SNMP provides the capability for network administrators to affect aspects with the network. Values which regulate network operation can be altered, allowing administrators to quickly respond to network problems, dynamically implement new network changes, and to perform real-time testing on how changes may affect their network.

SNMP implements a manager/agent/subagent model, which conforms very closely to the client/server model (11.1.1, “The client/server model” on page 408). RFC 1157 defines the components and interactions involved in an SNMP community, which include:

A Management Information Base (MIB, discussed in 17.1.1, “The

Management Information Base (MIB)” on page 625)

An SNMP agent (discussed in 17.1.2, “The SNMP agent” on page 630)

An manager (discussed in 17.1.3, “The SNMP manager” on page 631) SNMP subagents (discussed in 17.1.4, “The SNMP subagent” on page 632)

#### 17.1.1 The Management Information Base (MIB)

The management information base defines a set of objects which can be monitored or managed using an SNMP implementation. The current MIB, MIB-II, is defined in RFC 1213 and replaces the MIB-I definition outlined in RFC 1156. It

is updated by RFCs 4022, 4113, and 4293. MIB-II defines the groups of information which should be made available in any SNMP implementation in a TCP/IP based network. These groups are as shown in Table 17-1.

*Table 17-1 Group names and descriptions available in an SNMP implementation*

|  |  |  |
| --- | --- | --- |
| **Group name** | **Description of objects within the group** | **RFC defining**  **the group’s MIB** |
| System | Basic system information, such as the system’s name, description, and how much time has passed since the last time the system was restarted. | RFC 3418 |
| Interfaces | Information about network interfaces, including a list of interfaces, and statistics specific to these interfaces. | RFC 2863 |
| IP | Information and statistics on IP traffic. | RFC 4293 |
| ICMP | Statistics on ICMP input and output. | RFC 4293 |
| TCP | General information about the TCP layer (such as timeout values and the total number of TCP connections) as well as information about specific TCP connections (such as the connection’s state, addresses, and ports). | RFC 4022 |
| UDP | General information about the UDP layer (such as the number of UDP packets sent and delivered) as well as information about specific UDP usage (such as addresses and ports). | RFC 4113 |
| EGP | Statistics on external gateway protocol traffic. | RFC 1156  RFC 1213 |
| Transmission | This group is not yet implemented, but was created as a placeholder for when Internet-standard definitions for managing transmission media emerge. | RFC 1213 |

|  |  |  |
| --- | --- | --- |
| **Group name** | **Description of objects within the group** | **RFC defining**  **the group’s MIB** |
| SNMP | Information and statistics related to the SNMP environment. | RFC 3411  RFC 3412  RFC 3413  RFC 3414  RFC 3415  RFC 3418 |

Note that these constitute only the minimum implementation. An implementation can also create it’s own groups and objects which are application or platform-specific. In such cases, the MIB must be built into the SNMP agent itself, or be made available to the agent using the distributed programming interface (DPI, see 11.2.3, “The SNMP distributed programming interface (SNMP DPI)” on page 419). Additionally, each managed node supports only those groups that are appropriate. For example, if there is no gateway, the EGP group need not be supported. If a group is appropriate, all objects in that group must be supported.

Objects within a MIB are defined using the Structure of Management Information Version 2 (SMIv2), defined in RFC 2578.

##### Structure of Management Information Version 2 (SMIv2)

SMIv2 defines the rules for how managed objects are described and how management protocols can access these objects. The description of managed objects is made using a subset of the Abstract Syntax Notation One (ASN.1, ISO standard 8824), a data description language. The object type definition uses the following syntax:

|  |  |
| --- | --- |
| objectName | OBJECT-TYPE |
| SYNTAX | *syntax* |
| UNITS | “*units*” |
| MAX-ACCESS | *access* |
| STATUS | *status* |
| DESCRIPTION | “*descriptiveText*” |
| REFERENCE | “*referenceText*” |
| INDEX | {*indexTypes*} |
| DEFVAL | {*defaultValue*} |

::= { *group #* }

These fields are defined as follows:

|  |  |
| --- | --- |
| **OBJECT-TYPE** | A textual name, called the *object descriptor*, for the object type along with its corresponding *object identifier* defined later. |
| **SYNTAX** | The abstract syntax for the object type. It can be a choice of SimpleSyntax (Integer, Octet String, Object Identifier, Null) or an ApplicationSyntax (NetworkAddress, Counter, Gauge, TimeTicks, Opaque) or other application-wide types (see RFC 2578 for more details). |
| **UNITS** | This field is optional and applies only when the object maintains a value that is unit specific. For example, an object that monitors time might specify UNIT “seconds” or UNIT “minutes”. |
| **MAX-ACCESS** | Defines the access that a user has to this object. Valid values include accessible-for-notify, read-only, read-write, read\_create, and not-accessible. |
| **STATUS** | Defines the status of the object. Valid values include current, deprecated, and obsolete. |
| **DESCRIPTION** | A textual description of the semantics of the object type. |
| **REFERENCE** | This field is optional and can be used to include a text string referencing some other document. |
| **INDEX** | This field is optional and is only used when the object is part of a conceptual row of objects. |
| **DEFVAL** | This field is optional and is only used when the object should have a default value. |
| **group** | The RFC 1213-defined group to which the object belongs. |
| **#** | The object’s position within the RFC 1213-defined group. |

As an example, consider the object ifType, defined by RFC 2863. ifType is part of the Interface group defined by RFC 1213. Its SMIv2 definitions is illustrated in Figure 17-1.

|  |
| --- |
| ifType OBJECT-TYPE  SYNTAX IANAifType  MAX-ACCESS read-only  STATUS current  DESCRIPTION  “The type of interface. Additional values for ifType are assigned by the Internet Assigned Numbers Authority  (IANA), through updating the syntax of the IANAifType textual convention.”  ::= { ifEntry 3 } |

*Figure 17-1 SMIv2 definition of sysUpTime*

##### Object identifiers (OIDs)

A managed object not only has to be described but identified, too. This is done using the ASN.1 object identifier (OID). The object identifier reserves a set of numbers for different groups. Each object is identified by a string of numbers indicating the hierarchy to which it belongs. Referring back to the example of ifType, this object has an OID of 1.3.6.1.2.1.2.2.1.3. This can initially be broken into two parts:

**ifEntry** 1.3.6.1.2.1.2.2.1

###### ifType 3

Note that the terms ifType, 1.3.6.1.2.1.2.2.1.3, and ifEntry.3 are functionally interchangeable. However, ifType’s OID can be further broken down as follows:

|  |  |
| --- | --- |
| **ifTable** | 1.3.6.1.2.1.2.2 |
| **ifEntry** | 1 |
| **ifType** | 3 |

Again, the terms ifType, 1.3.6.1.2.1.2.2.1.3, ifTable.1.3, and ifEntry.3 are all functionally interchangeable. The OID can continue to be broken down because each digit has a specific meaning. The significance of each digit adheres to the following rules:

The first digit defines the node administrator:

* 1 for ISO
* 2 for CCITT
* 3 for the joint ISO-CCITT

The possible values for the second digit are determined by the first digit. In this case, the ISO node administrator defines *3* for use by other organizations.

The third digit’s potential values again depend on the first and second digits.

But if the first two digits are 1.3, *6* is defined for the use of the U.S. Department of Defense.

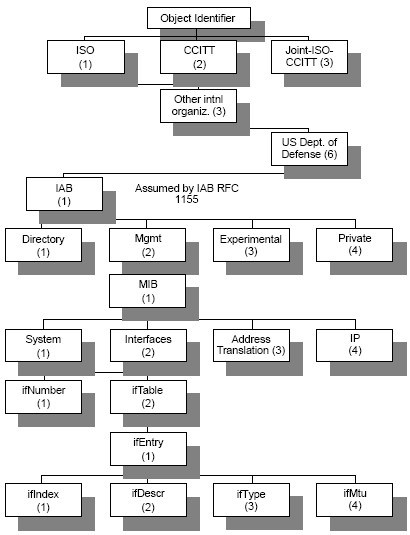
In the fourth group, the Department of Defense has not indicated how it will manage its group, so the Internet community assumed *1* for its own.

The fifth group was approved by IAB to be:

* 1 for the use of OSI directory in the Internet
* 2 for object identification for management purposes
* 3 for object identification for experimental purposes
* 4 for object identification for private use

This if further illustrated in Figure 17-2, which shows a mapping of how the OID number for ifType is determined.

*Figure 17-2 Finding ifType’s OID number*



#### 17.1.2 The SNMP agent

The SNMP agent acts as a server in the client/server model and listens on well-known UDP port 161 for requests from SNMP managers (we discuss managers in 17.1.3, “The SNMP manager” on page 631). Additionally, the SNMP agent is typically responsible for supporting both the system and the SNMP groups defined by RFC 1213.

Upon receiving a request from a manager, the agent determines if the requesting management station has the authority to access the SNMP community. If so, the agent obtains the value of the requested objects and returns them to the manager.

Finally, the agent can accept connections from subagents (discussed in the next section) to make MIBs available to SNMP managers. Upon receiving a request from a manager for an object supported by a subagent, the agent forwards the request to the appropriate subagent. This is illustrated later in Figure 17-5 on page 636.

#### 17.1.3 The SNMP manager

The SNMP manager, also referred to as a Network Management Station (NMS), provides a user interface through which network administrators can monitor and manage their network. The manager fulfills the role of a client in the client/server model and is available in a variety of formats including command-line interfaces, graphical user interface (GUI) applications, and fully automated applications.

The SNMP manager is responsible for issuing requests to the SNMP agent. These requests can be queries to obtain the value of a MIB object, or they can be requests to set the value of a MIB object. SNMP managers also can listen for notifications or alerts, called traps, generated by components in the SNMP community. For additional information about traps, see 17.1.6, “SNMP traps” on page 638.

**Note:** Communication between an SNMP manager and the SNMP agent occurs using the communication structure outlined by the Simple Network Management Protocol. SNMP usually employs UDP as a transport.

An SNMP manager can make the following types of requests to the SNMP agent:

|  |  |
| --- | --- |
| **getRequest** | Requests that the agent return the value of the specified object. |
| **getNextRequest** | Requests that the agent return the first valid value following the specified object. For example, assume a  **getNext** is executed for ifType (1.3.6.1.2.1.2.2.1.3). Assuming the first valid instance of ifType is ifType.1 (1.3.6.1.2.1.2.2.1.3.1), this is the value that the SNMP agent will return. |
| **getBulkRequest** | Performs the same function as the **get** request, but allows the manager to query more than one object per request. This is only valid using the SNMPv2c security model (see “The GetBulkRequest” on page 642). | |
| **setRequest** | Requests that the SNMP agent set the value of the specified object. | |
| **walk** | Implements a series of **getNext** requests such that an entire sequence of objects is returned to the manager. In each iteration of the **getNext** series, the last object returned becomes the next object on which a **getNext** is executed. The **walk** ends when an object is returned that is beyond the scope of the request. An example of this is provided in Figure 17-6 on page 637. | |

Note that the **walk** request is not architected in the SNMP communication that occurs between the SNMP manager and SNMP agent. Instead, it is a convention widely used by most SNMP managers.

#### 17.1.4 The SNMP subagent

An SNMP subagent supports its own MIB, which might be an RFC-architected MIB, or might be a proprietary (referred to as enterprise-specific) MIB. For example, a TCP/IP subagent would most likely support the IP, ICMP, TCP, UDP, and Interface groups defined in RFC 1213. However, an individual software company might want use SNMP to make available information specific to their software. To do this, they can create a subagent that supports their enterprise-specific MIB.

The subagent, upon initializing, opens a DPI connection to the SNMP agent. This occurs by first querying the agent, as though the subagent were a manager, for information about the agent’s DPI ports. Note that this information is maintained by the SNMP agent in the following two objects: dpiPortForTCP.0 1.3.6.1.4.1.2.2.1.1.1.0 dpiPortForUDP.0 1.3.6.1.4.1.2.2.1.1.2.0

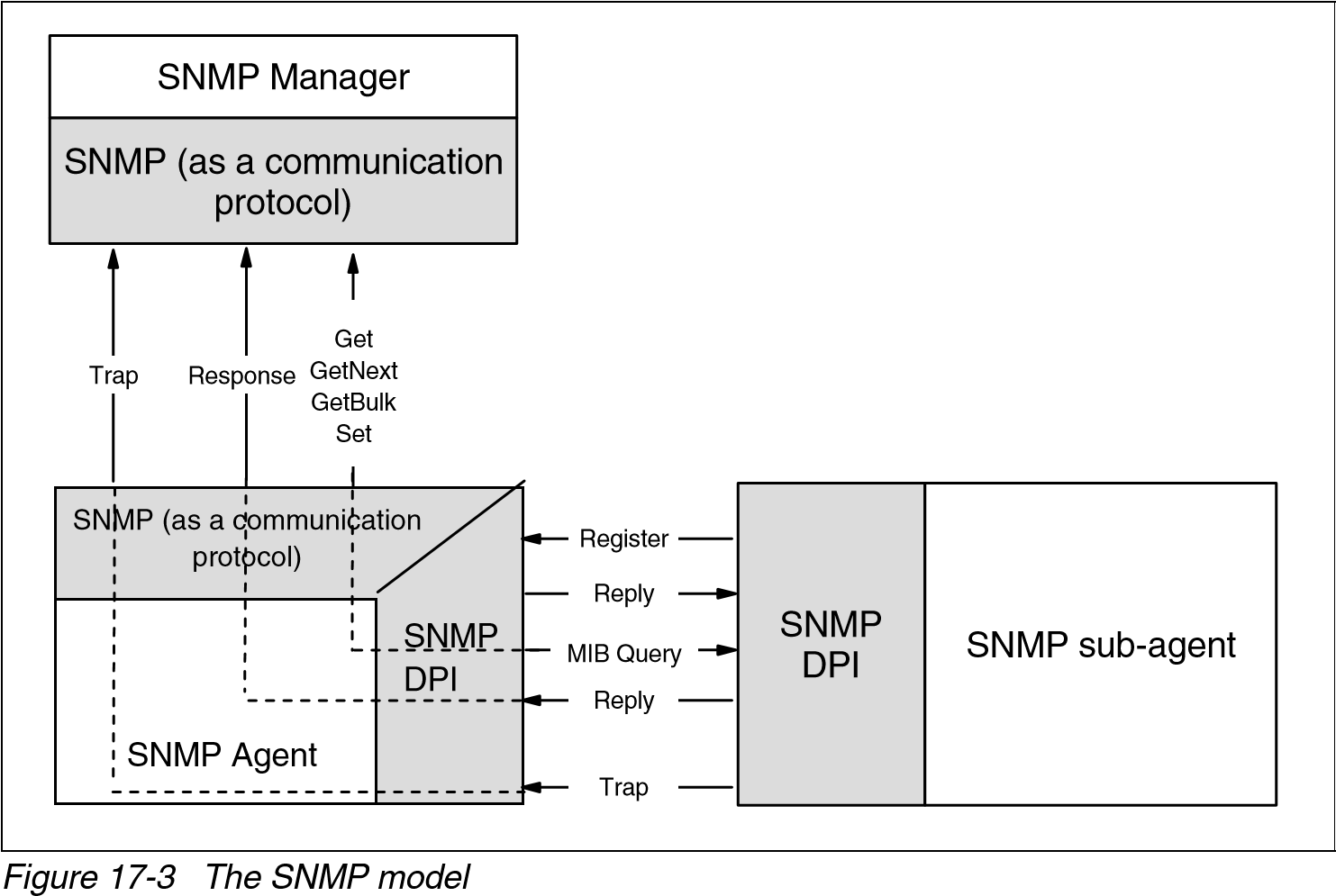
The agent’s response directs the subagent to the correct port over which a DPI connection can be opened. With this information, the subagent can interact with the agent, as described in 11.2.3, “The SNMP distributed programming interface (SNMP DPI)” on page 419.

#### 17.1.5 The SNMP model

The interaction between SNMP components is agent-restrictive: A manager can communicate only with an agent, and a subagent can communicate only with an agent. In no aspects of the model will a subagent communicate with a manager. If a manager needs to obtain or set the value of an object supported by a subagent, the request is delivered to the agent.

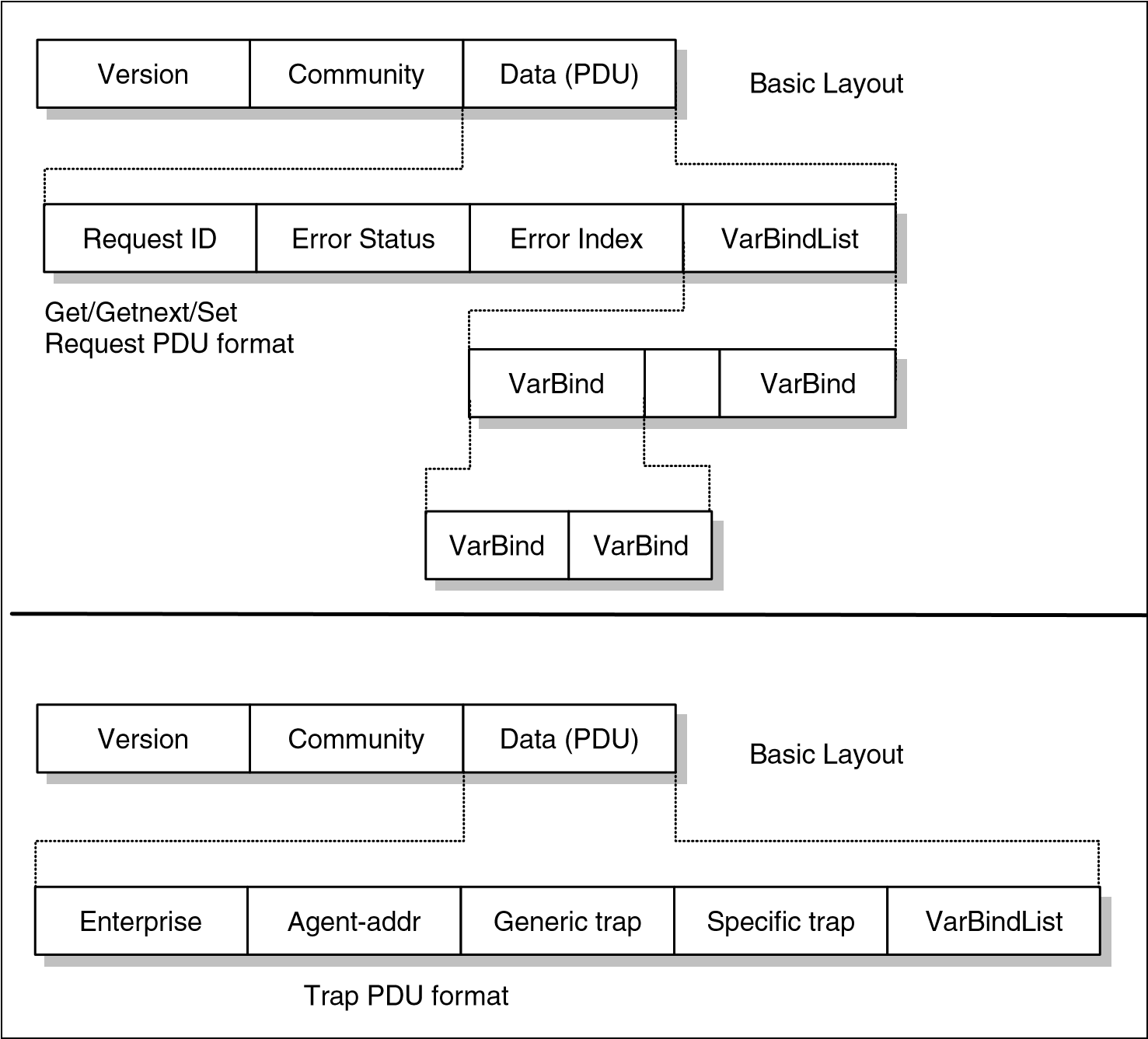
The agent, upon realizing that the request is for an object in a MIB other than one it supports, attempts to find the object in one of the MIBs registered by a subagent. Upon finding the correct MIB, the agent passes the request to the subagent.

The subagent then locates the correct value and passes it back to the SNMP agent. The agent then forwards this value back to the manager. This process, as well as the relationship that exists between manager, agents, and subagents, is illustrated in Figure 17-5 on page 636.



Messages sent between SNMP agents and managers use a Protocol Data Unit

(PDU) preceded by the SNMP header. The header specifies the version of SNMP being used, as well as authentication credentials. The PDU contains information regarding the type of request or response contained in the PDU, and in the case of a response, the actual value of the queried objects. The SNMP message format is illustrated in Figure 17-4.



*Figure 17-4 The SNMP message format*

This format is defined in RFC 1157, and the fields are defined as follows:

|  |  |
| --- | --- |
| **Version** | Indicates the version of SNMP being used (valid values are 1, 2, and 3). |
| **Community** | The SNMP community to which the request is directed, or from which the response originated. |
| **Request ID** | Serializes request/response iterations. A manager uses this to determine which responses correspond to a specific request. |
| **Error Status** | Specified on responses to inform the manager of any errors encountered with the request. On request PDUs, this value is set to 0. Valid values are: **noError** No error was encountered.  **tooBig** The response was too large to deliver in a PDU.  **noSuchName** The requested object does not exist.  **badValue** The returned value does not adhere to ASN.1 encoding standards.  **readOnly** A set request was executed for an object which is read-only.  **genErr** An error not covered by the other types occurred. |
| **Error Index** | An integer indicating which object in a list of objects caused the error reported by the errorStatus. |
| **VarBind** | The list of objects requested and, for a response, their values. |
| **Enterprise** | The entity (defined by the sysObjectID MIB object) generating an enterprise-specific trap. |
| **Agent-addr** | The address of the SNMP agent from which the trap was generated. |
| **Generic trap** | The generic trap type that indicates the type of trap sent. If this is an enterprise-specific trap, this is set to 6 (see 17.1.6, “SNMP traps” on page 638). |
| **Specific trap** | The value of an enterprise-specific trap (see 17.1.6, “SNMP traps” on page 638). |

To illustrate the process of querying an object using SNMP, refer back to the example of the ifType object. Figure 17-5 illustrates the sequence of events occurring when executing a **getNext** request for the ifType object.

getNext ifType

161)

UDP,Port

(

SNMP

Manager

SNMP

Agent

ifType belongs to the

Interface Group,

which was registered

by the TCP/IP

sub-agent

Forward this value

to the requesting

manager

TCPIP

Sub-agent

Retrieve from the

Interface Group MIB

ifType.1 = 6

ifType.1 = 6

UDP, manager's

(

ephemeral port)

getNext ifType

(

DPI socket

)

IPGroup MIB

UDP Group MIB

TCP Group MIB

ifType.1 = 6

)

DPI socket

(

SNMP Group

MIB

System Group

MIB

MIBs registered

by sub-agents

Interface Group

MIB

ifType.1 = 6

ICMP Group MIB

*Figure 17-5 An example of SNMP manager, agent, and subagent interaction*

The sequence of events is as follows:

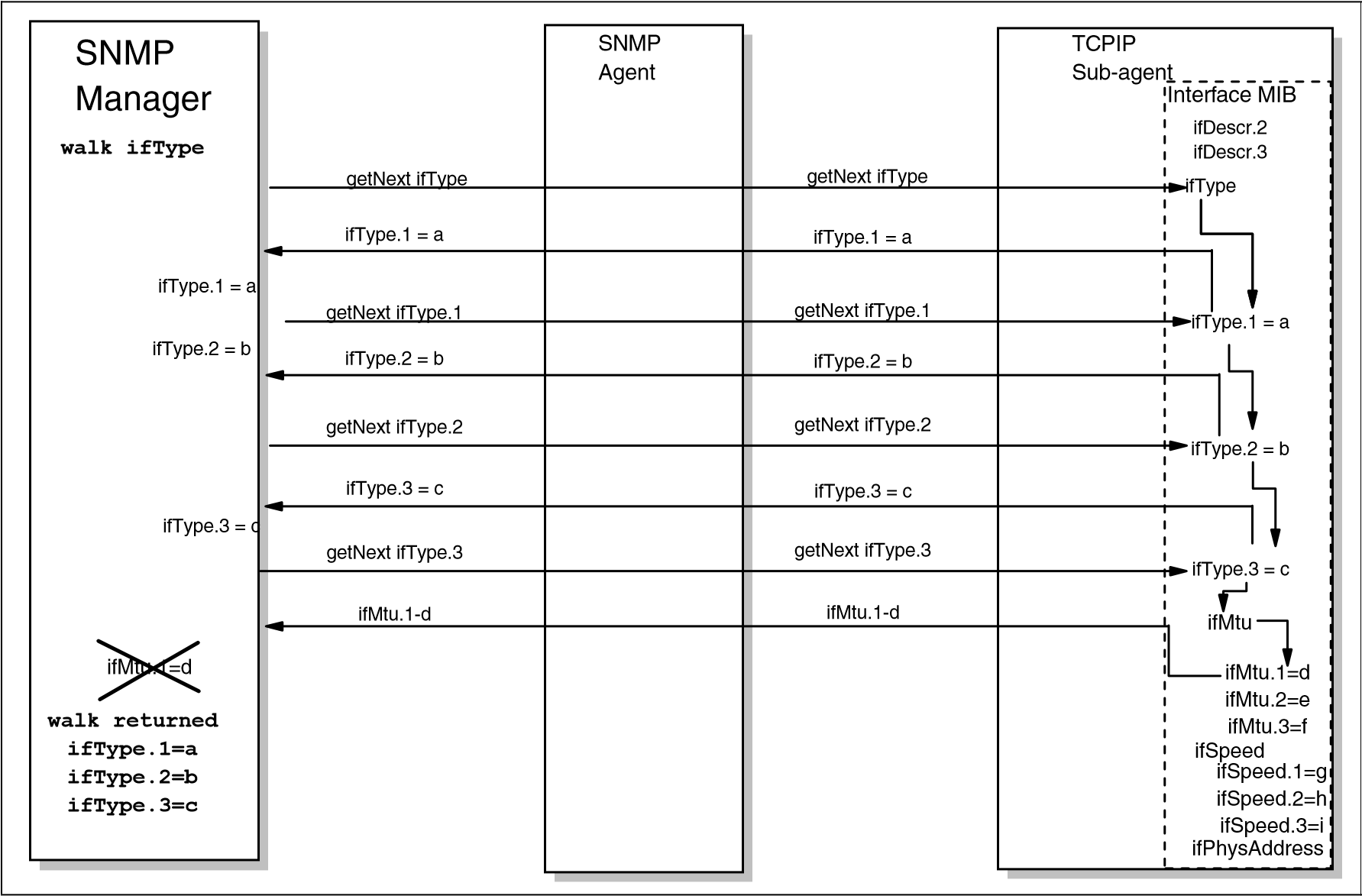
1. In this example, a **getNext** request is executed by the SNMP manager for ifType.
2. The SNMP agent does not recognize ifType as an object from the System Group or SNMP Group MIBs. It does, however, recognize ifType as an object from a MIB registered by a subagent. In this case, the MIB is the Interface Group MIB, and was registered by the TCP/IP subagent.
3. The SNMP agent passes the **getNext** over the DPI socket to the TCP/IP subagent.
4. The subagent recognizes ifType as an object in the Interface MIB and obtains the next object with a valid value: ifType.1.
5. The subagent sends a response back to the agent with the object ifType.1

and the value 6 (which, by RFC definition, is Ethernet).

1. The agent then replies back to the manager, again indicating that the object is ifType.1 and the value is 6.

Note that, had the **getNext** request been for an object in the System Group or SNMP Group MIBs, the SNMP agent would have recognized the object and responded directly to the manager. No subagent would have been involved in this circumstance.

While the concept of the **get**, **getNext**, **getBulk**, and **set** processes are somewhat simple, the process of executing a **walk** warrants additional discussion. As noted previously, a **walk** request is never actually sent to the SNMP agent. Instead, the walk is a manager convention, and is implemented as a series of **getNext** requests. In each iteration of the series, the object returned previously by the agent becomes the next object specified on the **getNext** request. The first time the agent returns a value outside of the range specified on the **walk** request, the **walk** ends. To demonstrate this, assume that there are three instances of ifType at the time a **walk** is issued for the ifType object: ifType.1 through ifType.3. The processing of the walk proceeds as illustrated in Figure 17-6.



*Figure 17-6 An example of a walk on ifType*

In this illustration, we see the following progression:

1. The user executes a **walk** on ifType, which the manager implements by first executing a **getNext** on ifType. This is forwarded to the TCP/IP subagent by the SNMP agent.
2. The subagent obtains the next valid value following ifType, ifType.1, and returns this value to the agent. The agent passes this information back to the manager.
3. The manager takes the ifType.1 response and executes a **getNext** for it.
4. The subagent locates ifType.1 and returns the next valid value: ifType.2.
5. The manager executes a **getNext** for ifType.2 6. The subagent returns ifType.3
6. The manager executes a **getNext** for ifType.3
7. The subagent returns ifMtu.1
8. The manager recognizes that ifMtu.1 is outside the scope of ifType, and assumes that the **walk** is complete.

#### 17.1.6 SNMP traps

Traps are asynchronous notifications of events occurring within an SNMP community. They can be generated both by SNMP agents and SNMP subagents. Additionally, they can be RFC architected (called a generic trap type) or they can be proprietary (called enterprise-specific). Architected traps, defined in RFC 1215, are as follows:

|  |  |
| --- | --- |
| **coldStartEvent** | Notifies managers that the SNMP agent is reinitializing and that the configuration might have been altered. This trap belongs to the RFC 1213-architected System group, and is therefore supported by the SNMP agent. |
| **warmStartEvent** | Notifies managers that the SNMP agent is reinitializing, but there has been no alteration of the configuration. This trap belongs to the RFC 1213-architected System group, and is therefore supported by the SNMP agent. |
| **linkDownEvent** | Notifies managers that an interface has been deactivated. Information identifying the interface is included in the trap. This trap belongs to the RFC 1213-architected Interface group and is usually supported by a TCP/IP specific  subagent. |

**linkUpEvent** Notifies managers that an interface has been activated. Information identifying the interface is included in the trap. This trap belongs to the RFC 1213-architected Interface group and is usually supported by a TCP/IP-specific subagent, or by an SNMP agent that manages its own TCP/IP MIBs.

##### snmpAuthenFailureEvent

Notifies managers that a user attempting to access the SNMP community did not provide the credentials needed to gain authorization by the SNMP agent. This trap belongs to the RFC 1213-architected SNMP group, and therefore is supported by the SNMP agent.

##### egpNeighborLossEvent

Notifies manages that a relationship with an EGP neighbor no longer exists. Information identifying the EGP neighbor is included in the trap. This trap belongs to the RFC 1213-architected EGP group, and therefore is usually supported by an EGP-specific subagent or a TCP/IP specific-subagent.

**entSpecificEvent** This trap is a placeholder that allows SNMP agent or subagent implementations to create enterprise-specific traps.

Traps generated by an SNMP agent are usually delivered to managers using well-known UDP port 162. However, SNMP implementations might provide a configuration option to allow traps to be sent to other user-determined ports. If a subagent generates a trap, the trap is not sent directly from the subagent to a manager. Instead, the trap is passed over the DPI connection to the agent, who then sends out the trap to the managers (see Figure 17-3 on page 633).

#### 17.1.7 SNMP versions

There are three versions of SNMP available, usually referred as SNMPv1 (RFC 1157), SNMPv2 (RFC 1901), and SNMPv3 (RFC 3414). Additionally, RFC 3584 was created to specify how all three versions can coexist with a single SNMP community. The security functions provided by the SNMP protocols are categorized into the following two models:

Community-based Security Model, whose data is protected by nothing more than a password, referred to as the community name (see Figure 17-4 on page 634). Community-based security allows the SNMP agent to authenticate a request based on the community name used and the IP address from which the request originated. This level of security is provided by the SNMPv1 and SNMPv2 Community-based Security Models.

User-based Security Model (USM), which provides different levels of security, based on the user accessing the managed information. To support this security level, the SNMPv3 framework defines several security functions, such as USM for authentication and privacy and vIew-based Access Control Model (VACM, defined in RFC 3415), which provides the ability to limit access to different MIB objects on a per-user basis and the use of authentication and data encryption for privacy.

##### SNMPv1

Version 1 of SNMP incorporates the basics of SNMP already covered in this chapter. Therefore, there is no need for additional discussion except to note that SNMPv1 does not allow **getBulk** requests. Such requests executed in an

SNMPv1 community, depending on the SNMP manager implementation, will result either in an error or in downgrading the request to a series of **get** requests.

##### SNMPv2

The framework of Version 2 of the Simple Network Management Protocol (SNMPv2) was published in April 1993 and consists of 12 RFCs, including the first, RFC 1441, which is an introduction. In August 1993, all 12 RFCs became a proposed standard with the status elective.

This framework consists of the following disciplines:

Structure of Management Information (SMI)

Definition of the OSI ASN.1 subset for creating MIB modules. See RFC 2578 for a description.

Textual conventions

Definition of the initial set of textual conventions available to all MIB modules. See RFC 2579 for a description.

Protocol operations

Definition of protocol operations with respect to the sending and receiving of PDUs. See RFC 3416 for a description.

Transport mappings

Definition of mapping SNMPv2 onto an initial set of transport domains because it can be used over a variety of protocol suites. The mapping onto UDP is the preferred mapping. The RFC also defines OSI, DDP, IPX, and so on. See RFC 3417 for a description.

Protocol instrumentation

Definition of the MIB for SNMPv2. See RFC 3418 for a description.

Administrative framework

Definition of the administrative infrastructure for SNMPv2, the User-based Security Model for SNMPv2 and the Community-based SNMPv2. See RFCs 1901, 1909, and 1910 for descriptions.

Conformance statements

Definition of the notation compliance or capability of agents. See RFC 2580 for a description.

The following sections describe the major differences and improvements from SNMPv1 to SNMPv2.

###### SNMPv2 entity

An SNMPv2 entity is an actual process that performs network management operations by generating or responding, or both, to SNMPv2 protocol messages by using the SNMPv2 protocol operations. All possible operations of an entity can be restricted to a subset of all possible operations that belong to a particular administratively defined party (refer to “SNMPv2 party”). An SNMPv2 entity can be member of multiple SNMPv2 parties. The following local databases are maintained by an SNMPv2 entity:

One database for all parties known by the SNMPv2 entity that can be:

* Operation realized locally
* Operation realized by proxy interactions with remote parties or devices
* Operation realized by other SNMPv2 entities

Another database that represents all managed object resources that are known to that SNMPv2 entity.

And at least a database that represents an access control policy that defines the access privileges accorded to known SNMPv2 parties.

An SNMPv2 entity can act as an SNMPv2 agent or manager.

###### SNMPv2 party

An SNMPv2 party is a conceptual, virtual execution environment whose operation is restricted, for security or other purposes, to an administratively defined subset of all possible operations of a particular SNMPv2 entity (refer to “SNMPv2 entity”). Architecturally, each SNMPv2 party consists of: A single, unique party identity.

A logical network location at which the party executes, characterized by a transport protocol domain and transport addressing information.

A single authentication protocol and associated parameters by which all protocol messages originated by the party are authenticated as to origin and integrity.

A single privacy protocol and associated parameters by which all protocol messages received by the party are protected from disclosure.

###### The GetBulkRequest

The **GetBulkRequest** is defined in RFC 3416 and is thus part of the protocol operations. A **GetBulkRequest** is generated and transmitted as a request of an SNMPv2 application. The purpose of the **GetBulkRequest** is to request the transfer of a potentially large amount of data, including, but not limited to, the efficient and rapid retrieval of large tables. The **GetBulkRequest** is more efficient than the **GetNext** request in case of retrieval of large MIB object tables. The syntax of the **GetBulkRequest** is:

GetBulkRequest [ non-repeaters = N, max-repetitions = M ]

( RequestedObjectName1,

RequestedObjectName2, RequestedObjectName3 )

Where:

**RequestedObjectName1, 2, 3**

MIB object identifier, such as sysUpTime. The objects are in a lexicographically ordered list. Each object identifier has a binding to at least one variable. For example, the object identifier ipNetToMediaPhysAddress has a variable binding for each IP address in the ARP table and the content is the associated MAC address.

**N** Specifies the non-repeaters value, which means that you request

only the contents of the variable next to the object specified in your request of the first N objects named between the parentheses. This is the same function as provided by the **GetNextRequest**.

**M** Specifies the max-repetitions value, which means that you request from the remaining (number of requested objects - N) objects the contents of the M variables next to your object specified in the request. Similar to an iterated **GetNextRequest** but transmitted in only one request.

With the **GetBulkRequest**, you can efficiently get the contents of the next variable or the next M variables in only one request.

Assume the following ARP table in a host that runs an SNMPv2 agent:

Interface-Number Network-Address Physical-Address Type

1 10.0.0.51 00:00:10:01:23:45 static

1. 9.2.3.4 00:00:10:54:32:10 dynamic
2. 10.0.0.15 00:00:10:98:76:54 dynamic

An SNMPv2 manager sends the following request to retrieve the sysUpTime and the complete ARP table:

GetBulkRequest [ non-repeaters = 1, max-repetitions = 2 ]

( sysUpTime, ipNetToMediaPhysAddress, ipNetToMediaType )

The SNMPv2 agent responds with a response PDU:

Response (( sysUpTime.0 = "123456" ),

( ipNetToMediaPhysAddress.1.9.2.3.4 =

"000010543210" ),

( ipNetToMediaType.1.9.2.3.4 = "dynamic" ),

( ipNetToMediaPhysAddress.1.10.0.0.51 =

"000010012345" ),

( ipNetToMediaType.1.10.0.0.51 = "static" ))

The SNMPv2 manager continues with:

GetBulkRequest [ non-repeaters = 1, max-repetitions = 2 ]

( sysUpTime, ipNetToMediaPhysAddress.1.10.0.0.51, ipNetToMediaType.1.10.0.0.51 )

The SNMPv2 agent responds with:

Response (( sysUpTime.0 = "123466" ),

( ipNetToMediaPhysAddress.2.10.0.0.15 =

"000010987654" ), ( ipNetToMediaType.2.10.0.0.15 =

"dynamic" ), ( ipNetToMediaNetAddress.1.9.2.3.4 =

"9.2.3.4" ),

( ipRoutingDiscards.0 = "2" ))

This response signals the end of the table to the SNMPv2 manager. Using the **getNextRequest**, this same result requires four iterations of queries.

###### InformRequest

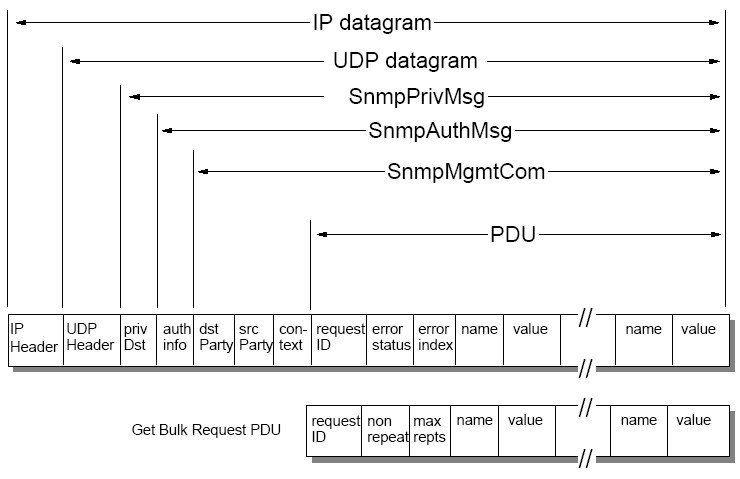
An **InformRequest** is generated and transmitted as a request from an application in an SNMPv2 manager entity that wants to notify another application, acting also in an SNMPv2 manager entity, of information in the MIB view[[5]](#footnote-5) of a party local to the sending application. The packet is used as an indicative assertion to the manager of another party about information accessible to the originating party (manager-to-manager communication across party boundaries). The first two variables in the variable binding list of an **InformRequest** are sysUpTime.0 and snmpEventID.i[[6]](#footnote-6), respectively. Other variables can follow.

###### The new administrative model

It is the purpose of the administrative model for SNMPv2 to define how the administrative framework is applied to realize effective network management in a variety of configurations and environments.

The model entails the use of distinct identities for peers that exchange SNMPv2 messages. Therefore, it represents a departure from the community-based administrative model of the original SNMPv1. By unambiguously identifying the source and intended recipient of each SNMPv2 message, this new strategy improves on the historical community scheme both by supporting a more convenient access control model and allowing for effective use of asymmetric (public key) security protocols in the future. Figure 17-7 on page 645 illustrates the new message format.

*Figure 17-7 The SNMPv2 message format*



In this figure, the fields are defined as follows:

**PDU** Includes one of the following protocol data units:

* GetNextRequest
* GetRequest
* Inform
* Report
* Response
* SNMPv2-Trap
* SetRequest

The **GetBulkRequest** has a different PDU format, as shown earlier (refer to “The GetBulkRequest” on page 642).

SnmpMgmtCom (SNMP Management Communication)

Adds the source party ID (srcParty), the destination party ID (dstParty), and the context to the PDU. The context specifies the SNMPv2 context containing the management information referenced by the communication.

**SnmpAuthMsg** This field is used as authentication information from the authentication protocol used by that party. The SnmpAuthMsg is serialized according to ASN.1 BER[[7]](#footnote-7) and can then be encrypted.

SnmpPrivMsg SNMP Private Message

An SNMPv2 private message is an SNMPv2 authenticated management communication that is (possibly) protected from disclosure. A private destination (privDst) is added to address the destination party.

The message is then encapsulated in a normal UDP/IP datagram and sent to the destination across the network.

For further information, refer to the previously mentioned RFCs.

##### SNMPv3

SNMPv3 is described in RFCs 3410 through 3415. SNMPv3 is not a replacement of SNMPv1 or SNMPv2, but rather is an extension to the existing SNMP architecture.

SNMPv3 supports the following:

A new SNMP message format

Authentication for messages

Security for messages

Access control

Continued support for SNMPv2

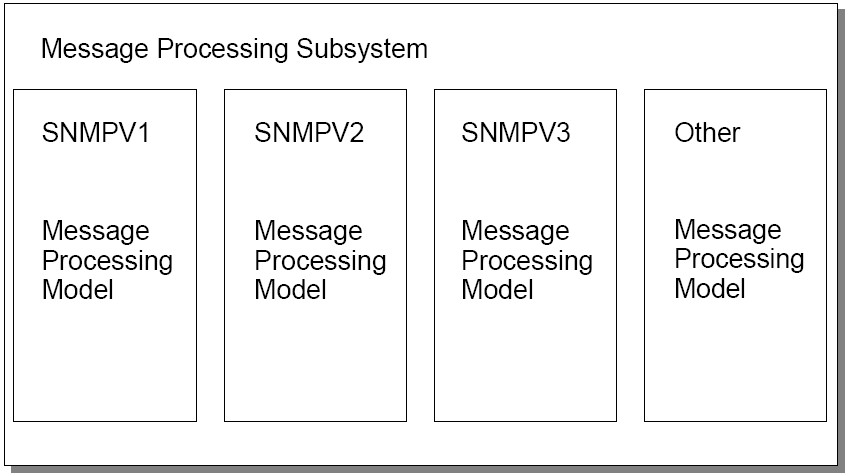
The User-based Security Model (USM), described in RFC 3414, specifies using MD5 and hashing algorithms. This provides data integrity, security, and privacy. There is support for the authentication protocols HMAC-MD5-96,

HMAC-SHA-96, and optional support for the encryption protocol CBC-DES.

The View-based Access Control Model (VACM), defined in RFC 3415, shows how to define views that are subsets of the full MIB tree. Access control on a per-user basis can then be implemented for these views.

Because SNMP has a modular structure, changes to individual modules do not impact the other modules directly. This allows you to easily define SNMPv3 over the existing model. For example, to add a new SNMP message format, it is

sufficient to upgrade the message processing model. Furthermore, because it is needed to support SNMPv1 and SNMPv2 messages as well, it can be achieved by adding the new SNMPv3 message module into the message processing subsystem. Figure 17-8 illustrates this structure.



*Figure 17-8 The SNMP message processing subsystem*

#### 17.1.8 Single authentication and privacy protocol

The authentication protocol provides a mechanism by which SNMPv3 management communications, transmitted by a party, can be reliably identified as having originated from that party.

The privacy protocol provides a mechanism by which SNMPv3 management communications transmitted to a party are protected from disclosure.

Principal threats against which the SNMPv3 security protocol provides protection are:

Modification of information

Masquerade

Message stream modification

Disclosure

The following security services provide protection against these threats:

**Data integrity** Provided by the MD5 message digest algorithm. A 128-bit digest is calculated over the designated portion of a SNMPv3 message and included as part of the message sent to the recipient.

|  |  |
| --- | --- |
| **Data origin authentication** | Provided by prefixing each message with a secret value shared by the originator of that message and its intended recipient before digesting. |
| **Message delay or replay** | Provided by including a time stamp value in each message. |
| **Data confidentiality** | Provided by the symmetric privacy protocol that encrypts an appropriate portion of the message according to a secret key known only to the originator and recipient of the message. This protocol is used in conjunction with the symmetric encryption algorithm, in the cipher block chaining mode, which is part of the Data Encryption Standard (DES). The designated portion of an SNMPv3 message is encrypted and included as part of the message sent to the recipient. |

### 17.2 The NETSTAT utility

The NETSTAT utility is a command available on most platforms that enables a user to list the sockets in use on a system. The information returned by the command is only for the local host, and there is no provision for monitoring remote hosts using this utility.

The most common uses for NETSTAT are:

Determining how many sockets are currently open on a system

Determining what application owns a particular socket

Diagnosing TCP/IP problems

Diagnosing routing problems

The NETSTAT command can be issued with or without parameters. Without parameters, the output generated by the command typically lists all of the active UDP and TCP connections in the system’s connection table. Options can be added to filter the output, or to request additional information. Because NETSTAT is not RFC defined, the specific options employed by different implementations vary. However, there is a common set of options that remain constant among most NETSTAT implementations.

#### 17.2.1 Common NETSTAT options

Common NETSTAT options include:

|  |  |
| --- | --- |
| **-r** / **-route** | Displays the routing table currently used by the TCP/IP |
| **-i** / **-interface**  **-l** / **-listening**  **-a** / **-all**   1. / **-statistics** 2. / **-timer**   **-v** / **-verbose**  **-f** / **-family** | application.  Displays a list of interfaces, and their states.  Displays only sockets on which an application is listening.  Displays all connections (typically, this is the default).  Displays the statistics for each protocol.  Displays timer information.  Displays the output in verbose mode.  Displays the address family of the connections. |

#### 17.2.2 Sample NETSTAT report output

Example 17-1 is a sample of a NETSTAT -all command and illustrates what is usually output by the default implementation of the utility.

*Example 17-1 NETSTAT -all command output*

:\> NETSTAT -a

|  |  |
| --- | --- |
| TCPIP Name: TCPIP | 13:11:51 |
| User Id Conn Local Socket Foreign Socket | State |
| ------- ---- ------------ --------------  FTPD1 00064A00  10.44.36.163..21 10.76.141.227..1780 Establsh | ----- |
| FTPD1 00000039 0.0.0.0..21 0.0.0.0..0 | Listen |
| PSF06A 00064B75 10.44.36.163..1384 10.27.172.17..9100 | SynSent |
| SMTP 00000037 0.0.0.0..25 0.0.0.0..0 | Listen |
| SNMPD 00000031 0.0.0.0..1026 0.0.0.0..0  TCPIP 0006421F  10.44.36.163..23 10.27.204.195..1055 Establsh | Listen |
| SMTP 00000038 0.0.0.0..1028 \*..\* | UDP |
| SNMPD 00000030 0.0.0.0..161 \*..\* | UDP |

The columns of the output, as well as in most implementations, are defined as

|  |  |
| --- | --- |
| follows: |  |
| **User Id** | The application or user that is using the socket. |
| **Conn** | The connection identification number. |
| **Local Socket** | The local IP address and port over which the connection is active. | |
| **Foreign Socket** | The remote IP address and port over which the connection is active. | |
| **State** | The state of the connection. Most implementations use some form of the following values for state: | |

* CloseWait
* Closed
* Established
* FinWait\_1
* FinWait\_2
* LastAck
* Listen
* SynReceived
* SynSent
* TimeWait
* UDP

(Because UDP is a connectionless protocol, they cannot be listed in a particular state. As such, NETSTAT simply indicates that they are UDP sockets.)

Additional information about these states can be found in RFC 0793.

Additionally, Example 17-2 is a sample routing table generated by NETSTAT.

*Example 17-2 Sample routing table*

:\> NETSTAT -r

TCPIP Name: TCPIP 13:25:04

Destination Gateway Flags Refcnt Interface

----------- ------- ----- ------ ---------

Default 10.44.36.129 UGS 001504 INTRF1 Default 10.44.36.129 UGS 000006 INTRF2

10.44.36.128 0.0.0.0 US 000003 INTRF1 10.44.36.128 0.0.0.0 US 000000 INTRF2

10.44.36.129 0.0.0.0 UHS 000000 INTRF1

10.44.36.129 0.0.0.0 UHS 000000 INTRF2

10.44.36.163 0.0.0.0 UH 000000 VIPAL1

10.44.36.164 0.0.0.0 UH 000000 INTRF1

10.44.36.165 0.0.0.0 UH 000000 INTRF2

127.0.0.1 0.0.0.0 UH 000002 LOOPBACK

Again, the columns above are defined as follows:

|  |  |
| --- | --- |
| **Destination** | The route described by the report. |
| **Gateway** | The gateway (if any) used to reach this route. |
| **Flags** | Attributes of the route. Possible values include:   * G: The route uses a gateway. * U: The interface over which the route travels is up. * H: Only a single host can be reached through this route. * D: The route was dynamically created. * M: The route’s table entry was modified by an ICMP redirect message. * !: The route is a reject route; datagrams will be dropped. |
| **Refcnt** | The number of connections using this route. |
| **Interface** | The interface used by the route. |

### 17.3 RFCs relevant to this chapter

The following RFCs provide detailed information about the management protocols and architectures presented throughout this chapter:

[RFC 0793 – Transmission Control Protocol (September 1981)](http://www.ietf.org/rfc/rfc0793.txt)

[RFC 1028 – Simple Gateway Monitoring Protocol (November 1987) Historic](http://www.ietf.org/rfc/rfc1028.txt)

[RFC 1052 – IAB recommendations for the development of Internet network management standards (April 1988)](http://www.ietf.org/rfc/rfc1052.txt)

[RFC 1085 – ISO presentation services on top of TCP/IP based internets (December 1988)](http://www.ietf.org/rfc/rfc1085.txt)

[RFC 1095 – Common Management Information Services and Protocol over TCP/IP (CMOT) (April 1989)](http://www.ietf.org/rfc/rfc1095.txt)

[RFC 1155 – Structure and identification of management information for](http://www.ietf.org/rfc/rfc1155.txt)

[TCP/IP-based internets (May 1990)](http://www.ietf.org/rfc/rfc1155.txt)

[RFC 1156 – Management Information Base for network management of TCP/IP-based internets (May 1990)](http://www.ietf.org/rfc/rfc1156.txt)  [RFC 1157 – Simple Network Management Protocol (SNMP) (May 1990)](http://www.ietf.org/rfc/rfc1157.txt)

[RFC 1189 – Common Management Information Services and Protocol for the](http://www.ietf.org/rfc/rfc1189.txt)

[Internet (CMOT and CMIP) (October 1990)](http://www.ietf.org/rfc/rfc1189.txt)

[RFC 1213 – Management Information Base for Network Management of](http://www.ietf.org/rfc/rfc1213.txt)

[TCP/IP-based internets: MIB-II (March 1991)](http://www.ietf.org/rfc/rfc1213.txt)

[RFC 1215 – Convention for defining traps for use with the SNMP](http://www.ietf.org/rfc/rfc1215.txt)

[(March1991)](http://www.ietf.org/rfc/rfc1215.txt)

[RFC 1239 – Reassignment of experimental MIBs to standard MIBs](http://www.ietf.org/rfc/rfc1239.txt)

[(June](http://www.ietf.org/rfc/rfc1239.txt) [1991)](http://www.ietf.org/rfc/rfc1239.txt)

[RFC 1351 – SNMP Administrative Model (July 1992)](http://www.ietf.org/rfc/rfc1351.txt)

[RFC 1352 – SNMP Security Protocols (July 1992)](http://www.ietf.org/rfc/rfc1352.txt)

[RFC 1441 – Introduction to version 2 of the Internet-standard Network](http://www.ietf.org/rfc/rfc1441.txt)

[Management Framework (April 1993)](http://www.ietf.org/rfc/rfc1441.txt)

[RFC 1592 – Simple Network Management Protocol Distributed Protocol](http://www.ietf.org/rfc/rfc1592.txt)

[Interface Version 2.0 (March 1994)](http://www.ietf.org/rfc/rfc1592.txt)

[RFC 1748 – IEEE 802.5 MIB using SMIv2 (December 1994)](http://www.ietf.org/rfc/rfc1748.txt)

[RFC 1901 – Introduction to Community-based SNMPv2 (January 1996)](http://www.ietf.org/rfc/rfc1901.txt)

[RFC 1909 – An Administrative Infrastructure for SNMPv2 (February 1996)](http://www.ietf.org/rfc/rfc1909.txt)

[RFC 1910 – User-based Security Model for SNMPv2 (February 1996)](http://www.ietf.org/rfc/rfc1910.txt)

[RFC 2578 – Structure of Management Information Version 2 (SMIv2) (April](http://www.ietf.org/rfc/rfc2578.txt) [1999)](http://www.ietf.org/rfc/rfc2578.txt)

[RFC 2579 – Textual Conventions for SMIv2 (April 1999)](http://www.ietf.org/rfc/rfc2579.txt)

[RFC 2580 – Conformance Statements for SMIv2 (April 1999)](http://www.ietf.org/rfc/rfc2580.txt)

[RFC 2742 – Definitions of Managed Objects for Extensible SNMP Agents (January 2000)](http://www.ietf.org/rfc/rfc2742.txt)

[RFC 2863 – The Interfaces Group MIB (June 2000)](http://www.ietf.org/rfc/rfc2863.txt)

[RFC 3410 – Introduction and Applicability Statements for Internet-Standard](http://www.ietf.org/rfc/rfc3410.txt)

[Management Framework (December 2002)](http://www.ietf.org/rfc/rfc3410.txt)

[RFC 3411 – An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks (December 2002)](http://www.ietf.org/rfc/rfc3411.txt)

[RFC 3412 – Message Processing and Dispatching for the Simple Network](http://www.ietf.org/rfc/rfc3412.txt)

[Management Protocol (SNMP) (December 2002)](http://www.ietf.org/rfc/rfc3412.txt)

[RFC 3413 – Simple Network Management Protocol (SNMP) Applications](http://www.ietf.org/rfc/rfc3413.txt)

[(December 2002)](http://www.ietf.org/rfc/rfc3413.txt)

[RFC 3414 – User-based Security Model (USM) for version 3 of the Simple](http://www.ietf.org/rfc/rfc3414.txt)

[Network Management Protocol (SNMPv3) (December 2002)](http://www.ietf.org/rfc/rfc3414.txt)

[RFC 3415 – View-based Access Control Model (VACM) for the Simple](http://www.ietf.org/rfc/rfc3415.txt)

[Network Management Protocol (SNMP) (December 2002)](http://www.ietf.org/rfc/rfc3415.txt)

[RFC 3416 – Version 2 of the Protocol Operations for the Simple Network](http://www.ietf.org/rfc/rfc3416.txt)

[Management Protocol (SNMP) (December 2002)](http://www.ietf.org/rfc/rfc3416.txt)

[RFC 3417 – Transport Mappings for the Simple Network Management](http://www.ietf.org/rfc/rfc3417.txt)

[Protocol (SNMP) (December 2002)](http://www.ietf.org/rfc/rfc3417.txt)

[RFC 3418 – Management Information Base (MIB) for the Simple Network](http://www.ietf.org/rfc/rfc3418.txt)

[Management Protocol (SNMP) (December 2002)](http://www.ietf.org/rfc/rfc3418.txt)

[RFC 3584 – Coexistence between Version 1, Version 2, and Version 3 of the](http://www.ietf.org/rfc/rfc3584.txt)

[Internet-standard Network Management Framework (August 2003)](http://www.ietf.org/rfc/rfc3584.txt)

[RFC 4022 – Management Information Base for the Transmission Control](http://www.ietf.org/rfc/rfc4022.txt)

[Protocol (TCP) (March 2005)](http://www.ietf.org/rfc/rfc4022.txt)

[RFC 4113 – Management Information Base for the User Datagram Protocol (UDP) (June 2005)](http://www.ietf.org/rfc/rfc4113.txt)

[RFC 4293 – Management Information Base for the Internet Protocol (IP) (April 2006)](http://www.ietf.org/rfc/rfc4293.txt)

|  |  |  |
| --- | --- | --- |
|  | |  | | --- | | **22** | |

## Chapter 22. TCP/IP security

This chapter discusses security issues regarding TCP/IP networks and provides an overview of solutions to prevent security exposures or problems before they occur. The field of network security in general and of TCP/IP security in particular is too wide to be dealt within an all encompassing way in this book, so the focus of this chapter is on the most common security exposures and measures to counteract them. Because many, if not all, security solutions are based on cryptographic algorithms, we also provide a brief overview of this topic for the better understanding of concepts presented throughout this chapter.

© Copyright IBM Corp. 1989-2006. All rights reserved.

### 22.1 Security exposures and solutions

This section gives an overview of some of the most common attacks on computer security, and it presents viable solutions to those exposures and lists actual implementations thereof.

#### 22.1.1 Common attacks against security

For thousands of years, people have been guarding the gates to where they store their treasures and assets. Failure to do so usually resulted in being robbed, victimized by society, or even killed. Though things are usually not as dramatic anymore, they can still become very bad. Modern day IT managers have realized that it is equally important to protect their communications networks against intruders and saboteurs from both inside and outside. One does not have to be overly paranoid to find some good reasons as to why this is the case:

Packet sniffing: To gain access to cleartext network data and passwords

Impersonation: To gain unauthorized access to data or to create unauthorized e-mails by impersonating an authorized entity

Denial-of-service: To render network resources non-functional

Replay of messages: To gain access to information and change it in transit

Password cracking: To gain access to information and services that would normally be denied (dictionary attack)

Guessing of keys: To gain access to encrypted data and passwords (brute-force attack)

Viruses: To destroy data

Port scanning: To discover potential available attack points

Though these attacks are not exclusively specific to TCP/IP networks, they must be considered potential threats to anyone who is going to base their network on TCP/IP, which is the most prevalent protocol used. TCP/IP is an open protocol, and therefore, hackers find easy prey by exploiting vulnerabilities using the previous methods.

#### 22.1.2 Solutions to network security problems

Network owners need to try to protect themselves with the same zealousness that intruders use to search for a way to get into the network. To that end, we provide some solutions to effectively defend a network from an attack, specifically against the attacks mentioned earlier. It has to be noted that any of these solutions only solve a single (or a very limited number) of security problems. Therefore, consider a combination of several such solutions to guarantee a certain level of safety and security. These solutions include:

Encryption: To protect data and passwords

Authentication by digital signatures and certificates: To verify who is sending data over the network

Authorization: To prevent improper access

Integrity checking and message authentication codes: To protect against improper alteration of messages

Non-repudiation: To make sure that an action cannot be denied by the person who performed it

One-time passwords and two-way random number handshakes: To mutually authenticate parties of a conversation

Frequent key refresh, strong keys, and prevention of deriving future keys: To protect against breaking of keys (cryptanalysis)

Address concealment: To protect against denial-of-service attacks

Disable unnecessary services: To minimize the number of attack points

Table 22-1 matches common problems and security exposures to the previous solutions.

*Table 22-1 Security exposures and protections*

|  |  |
| --- | --- |
| **Problem/exposure** | **Remedy** |
| How to prevent a packet sniffer from reading messages? | Encrypt messages, typically using a shared secret key (secret keys offer a tremendous performance advantage over public/private keys). |
| How to distribute the keys in a secure way? | Use a different encryption technique, typically public/private key. |
| How to prevent keys from becoming stale, and how to protect against guessing of future keys by cracking current keys? | Refresh keys frequently and do not derive new keys from old ones (use perfect forward secrecy). |
| How to prevent retransmission of messages by an impostor (replay attack)? | Use sequence numbers (time stamps are usually unreliable for security purposes). |
| How to ensure that a message has not been altered in transit? | Use message digests (hash or one-way functions). |
| How to ensure that the message digest has not also been compromised? | Use digital signatures by encrypting the message  digest with a secret or private key (origin authentication, non-repudiation). |
| **Problem/exposure** | **Remedy** |
| How to ensure that the message and signature    originated from the desired partner? | Use two-way handshakes involving encrypted random numbers (mutual authentication). |
| How to ensure that handshakes are exchanged with the right partners (man-in-the-middle attack)? | Use digital certificates (binding of public keys to permanent identities). |
| How to prevent improper use of services by otherwise properly authenticated users? | Use a multilayer access control model. |
| How to protect against viruses? | Restrict access to outside resources; run anti-virus software on every server and workstation that has contact to outside data, and update that software frequently. |
| How to protect against unwanted or malicious messages (denial of service attacks)? | Restrict access to internal network using filters, firewalls, proxies, packet authentication, conceal internal address and name structure, and so on. |
| How to minimize the number of attack points? | Close all unnecessary services. Use encryption and encapsulation to run many services over a smaller number of ports. |

In general, keep your network tight toward the outside, but also keep a watchful eye on the inside because most attacks are mounted from inside a corporate network.

#### 22.1.3 Implementations of security solutions

The following protocols and systems are commonly used to provide various degrees of security services in a computer network. They are discussed at length throughout the rest of this chapter.

IP filtering

Network Address Translation (NAT)

IP Security Architecture (IPSec)

SOCKS

Secure Shell (SSH)

Secure Sockets Layer (SSL)

Application proxies

Firewalls

Kerberos and other authentication systems (AAA servers)

Secure Electronic Transactions (SET)

Figure 22-1 illustrates where these security solutions fit within the TCP/IP layers.

*Figure 22-1 Security solutions in the TCP/IP layers*

Applications

TCP/UDP

)

Transport

(

IP

)

(

Internetwork

Network Interface

(

Data Link

)

-

S-MIME

-

Kerberos

Proxies

-

SET

-

)

IPSec (ISAKMP

-

-

SOCKS

SSL, TLS

-

-

IPSec (AH, ESP

)

Packet filtering

-

-

Tunneling protocols

-

CHAP, PAP, MS-CHAP

Table 22-2 summarizes the characteristics of some of the security solutions mentioned earlier and compares them to each other. This should help anyone who needs to devise a security strategy to determine what combination of solutions achieves a desired level of protection.

*Table 22-2 Security solution implementations: A comparison*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Access control** | **Encryption** | **Authentication** | **Integrity checking** | **Perfect forward security** | **Address concealment** | **Session monitoring** |
| IP filtering | Y | N | N | N | N | N | N |
| NAT | Y | N | N | N | N | Y | Y  (connection) |
| IPSec | Y | Y (packet) | Y (packet) | Y (packet) | Y | Y | N |
| SOCKS | Y | N | Y (client/ user) | N | N | Y | Y  (connection) |
| SSL | Y | Y (data) | Y (system/ user) | y |  | n | y |
|  | **Access control** | **Encryption** | **Authentication** | **Integrity checking** | **Perfect forward security** | **Address concealment** | **Session monitoring** |
| Application proxy | Y | Normally no | Y (user) | Y | Normally no | Y | Y  (connection and data) |
| AAA servers | y (user) | N | Y (user) | N | N | N | N |

An overall security solution can, in most cases, only be provided by a combination of the listed options. Your particular security requirements need to be specified in a security policy and should be, for example, enforced by using firewalls and validated by using security health checking tools and vulnerability scanners.

#### 22.1.4 Network security policy

An organization's overall security policy must be determined according to security and business needs analysis and based on security best practices. Because a firewall relates to network security only, a firewall has little value unless the overall security policy is properly defined.

A network security policy defines those services that will be explicitly allowed or denied, how these services will be used, and the exceptions to these rules. Every rule in the network security policy should be implemented on a firewall, remote access server (RAS), or both. Generally, a firewall uses one of the following methods.

##### Everything not specifically permitted is denied

This approach blocks all traffic between two networks except for those services and applications that are permitted. Therefore, each desired service and application is implemented one by one. No service or application that might be a potential hole on the firewall is permitted. This is the most secure method, denying services and applications unless explicitly allowed by the administrator. However, from the point of users, it might be more restrictive and less convenient.

##### Everything not specifically denied is permitted

This approach allows all traffic between two networks except for those services and applications that are denied. Therefore, each untrusted or potentially harmful service or application is denied one by one. Although this is a flexible and convenient method for the users, it can potentially cause some serious security problems, especially as new applications are introduced into the environment.

Remote access servers should provide authentication of users and should ideally also provide for limiting certain users to certain systems and networks within the corporate intranet (authorization). Remote access servers must also determine if a user is considered roaming (can connect from multiple remote locations) or stationary (can connect only from a single remote location), and if the server should use callback for particular users after they are properly authenticated.

Generally, anonymous access should at best, be granted to servers in a demilitarized zone (DMZ, see “Screened subnet firewall (demilitarized zone)” on page 808). All services within a corporate intranet should require at least password authentication and appropriate access control. Direct access from the outside should always be authenticated and accounted.

### 22.2 A short introduction to cryptography

The purpose of this chapter is to introduce the terminology and give a brief overview of the major cryptographic concepts that relate to TCP/IP security implementations. The information presented here only scratches the surface. Some issues are left open or not mentioned at all.

#### 22.2.1 Terminology

Let us start with defining some very basic concepts.

##### Cryptography

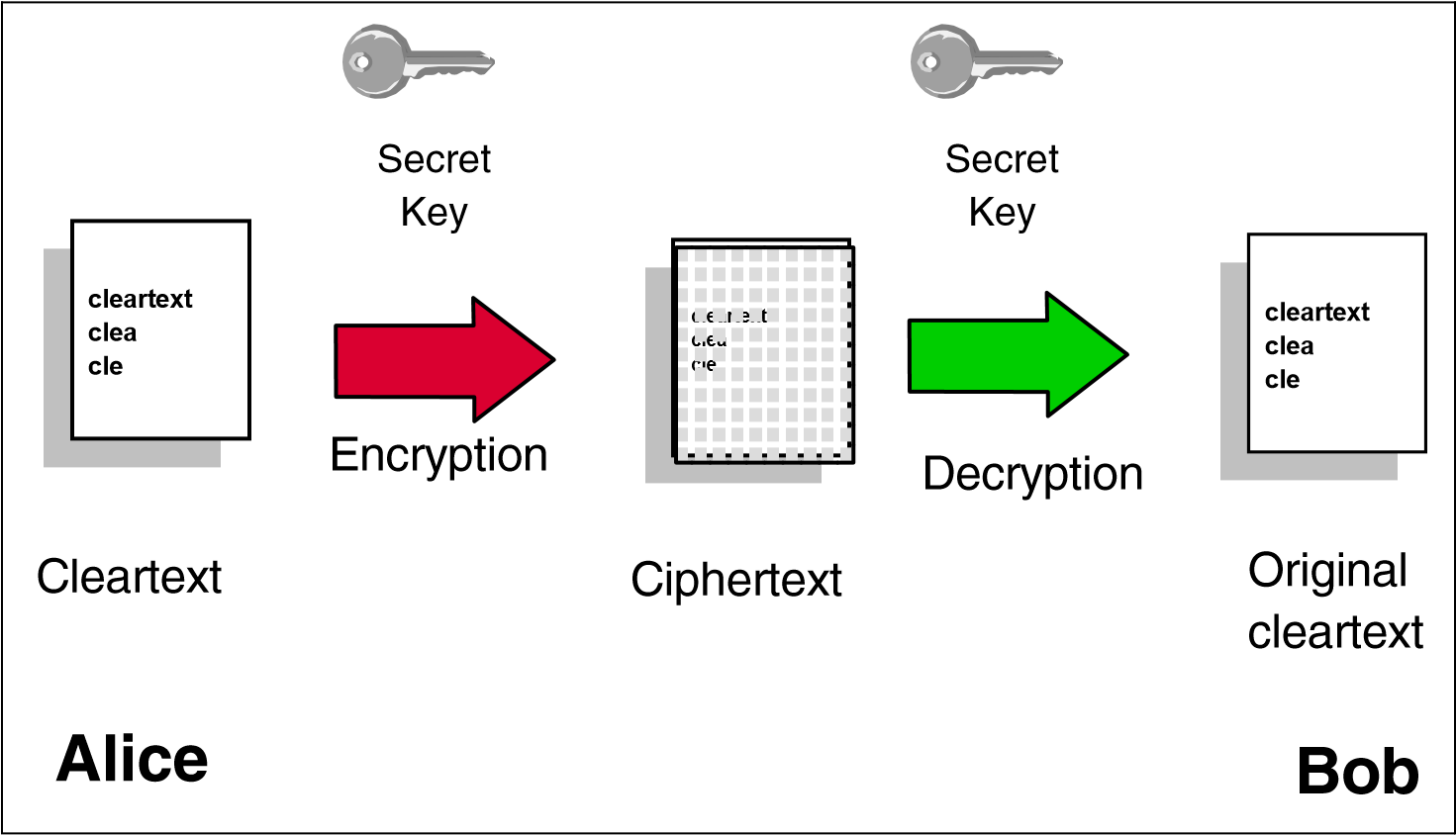
Put simply, *cryptography* is the science of altering the appearance of data in an effort to keep data and data communications secure. To achieve this goal, techniques such as *encryption*, *decryption*, and *authentication* are used. With the recent advances in this field, the frontiers of cryptography have become blurred. Every procedure consisting of transforming data based on methods that are difficult to reverse can be considered cryptography. The key factor to strong cryptography is the difficulty of reverse engineering. You might be amazed to know that simple methods, such as password-scrambled word processor documents or compressed archives, can be broken in a matter of minutes by a hacker using an ordinary PC. *Strong* cryptography means that the computational effort needed to retrieve your cleartext messages without knowing the proper keys makes the retrieval infeasible. In this context, infeasible means something like this: If all the computers in the world were assigned to the problem, they would have to work tens of thousands of years until the solution was found. The process of retrieval is called *cryptanalysis*. An attempted cryptanalysis is an *attack*.

###### Encryption and decryption: Cryptographic algorithms

*Encryption* is the transformation of a cleartext message into an unreadable form in order to hide its meaning. The opposite transformation, which retrieves the original cleartext, is the *decryption*. The mathematical function used for encryption and decryption is the *cryptographic algorithm* or *cipher*.

The security of a cipher might be based entirely on keeping its functionality a secret, in which case it is a *restricted cipher*. There are many drawbacks to restricted ciphers. It is very difficult to keep an algorithm a secret when it is used by many people. If it is incorporated in a commercial product, it is only a matter of time and money before it is reverse engineered. For these reasons, the currently used algorithms are *keyed*, that is, the encryption and decryption makes use of a parameter, known as the *key*. The key can be chosen from a set of possible values, called the *keyspace*. The keyspace usually is huge, the bigger the better. The security of these algorithms rely entirely on the key, not on their internal secrets. In fact, the algorithms themselves are usually public and are extensively analyzed for possible weaknesses. The principle of keyed ciphers is shown in Figure 22-2.

**Note:** Do not trust new, unknown, or unpublished algorithms.



*Figure 22-2 Keyed encryption and decryption*

**Note:** It is common in cryptographic literature to denote the first participant in a protocol as Alice and the second one as Bob. They are the “crypto couple.”

###### Authentication, integrity, and non-repudiation

Encryption provides confidentiality to messages. When communicating over an untrusted medium, such as the Internet, you might also need, in addition to confidentiality:

Authentication: A method for verifying that the sender of a message is really who he or she claims to be. Any intruder masquerading as someone else is detected by authentication.

Integrity checking: A method for verifying that a message has not been altered along the communication path. Any tampered message sent by an intruder is detected by an integrity check. As a side effect, communication errors are also detected.

Non-repudiation: The possibility to prove that the sender has really sent the message. When algorithms providing non-repudiation are used, the sender is not able to later deny the fact that he or she sent the message in question.

#### 22.2.2 Symmetric or secret-key algorithms

Symmetric algorithms are keyed algorithms where the decryption key is the same as the encryption key. These are conventional cryptographic algorithms where the sender and the receiver must agree on the key *before* any secured communication can take place between them. Figure 22-2 on page 778 illustrates a symmetric algorithm. There are two types of symmetric algorithms: *block algorithms*, which operate on the cleartext in blocks of bits, and *stream algorithms*, which operate on a single bit (or byte) of cleartext at a time.

Block ciphers are used in several modes. Electronic Codebook Mode (ECB) is the simplest; each block of cleartext is encrypted independently. Given a block length of 64 bits, there are 264 possible input cleartext blocks, each of them corresponding to exactly one out of 264 possible ciphertext blocks. An intruder might construct a codebook with known cleartext-ciphertext pairs and mount an attack. Because of this vulnerability, the Cipher Block Chaining (CBC) mode is often used, where the result of the encryption of the previous block is used in the encryption of the current block, thus each ciphertext block is dependent not just on the corresponding plaintext block, but on all previous plaintext blocks.

The algorithms often make use of initialization vectors (IVs). These are variables independent of the keys and are good for setting up the initial state of the algorithms.

A well-known block algorithm is the Data Encryption Standard (DES), which was a worldwide standard cipher developed by IBM. DES operates on 64-bit blocks and has a key length of 56 bits, often expressed as a 64-bit number, with every eighth bit serving as parity bit. From this key, 16 subkeys are derived, which are used in the 16 rounds of the algorithm.

DES produces ciphertexts the same length as the cleartext and the decryption algorithm is exactly the same as the encryption, the only difference being the subkey schedule. These properties make it very suitable for hardware implementations.

DES is becoming obsolete (its origins date back to the early 1970s) and is no longer sufficient as a standard. The most practical attack against it is *brute-force* decryption, with all possible keys, looking for a meaningful result. The problem with DES is the key length. Given enough time and computers, a brute-force attack against the 56-bit key might be feasible. That is why newer modes of DES, called triple-DES, or 3DES, have become popular. With triple-DES, the original DES algorithm is applied in three rounds, with two or three different keys.

Today, DES is still widely used in many forms but has been replaced as a standard by the Advanced Encryption Standard (AES), which is based on a block cipher named Rijndael. The Rijndael cipher is based on a block cipher Square. The Rijndael key length and block size are both variable and can be set to 128, 192, or 256 bits, but the official block size is 128 bits.

Another, block algorithm is the International Data Encryption Algorithm (IDEA).

This cipher uses 64-bit blocks and 128-bit keys. It was developed in the early

1990s and aimed to replace DES. It is cryptographically strong and faster than DES. The most significant use of IDEA is in the freeware secure e-mail package Pretty Good Privacy (PGP).

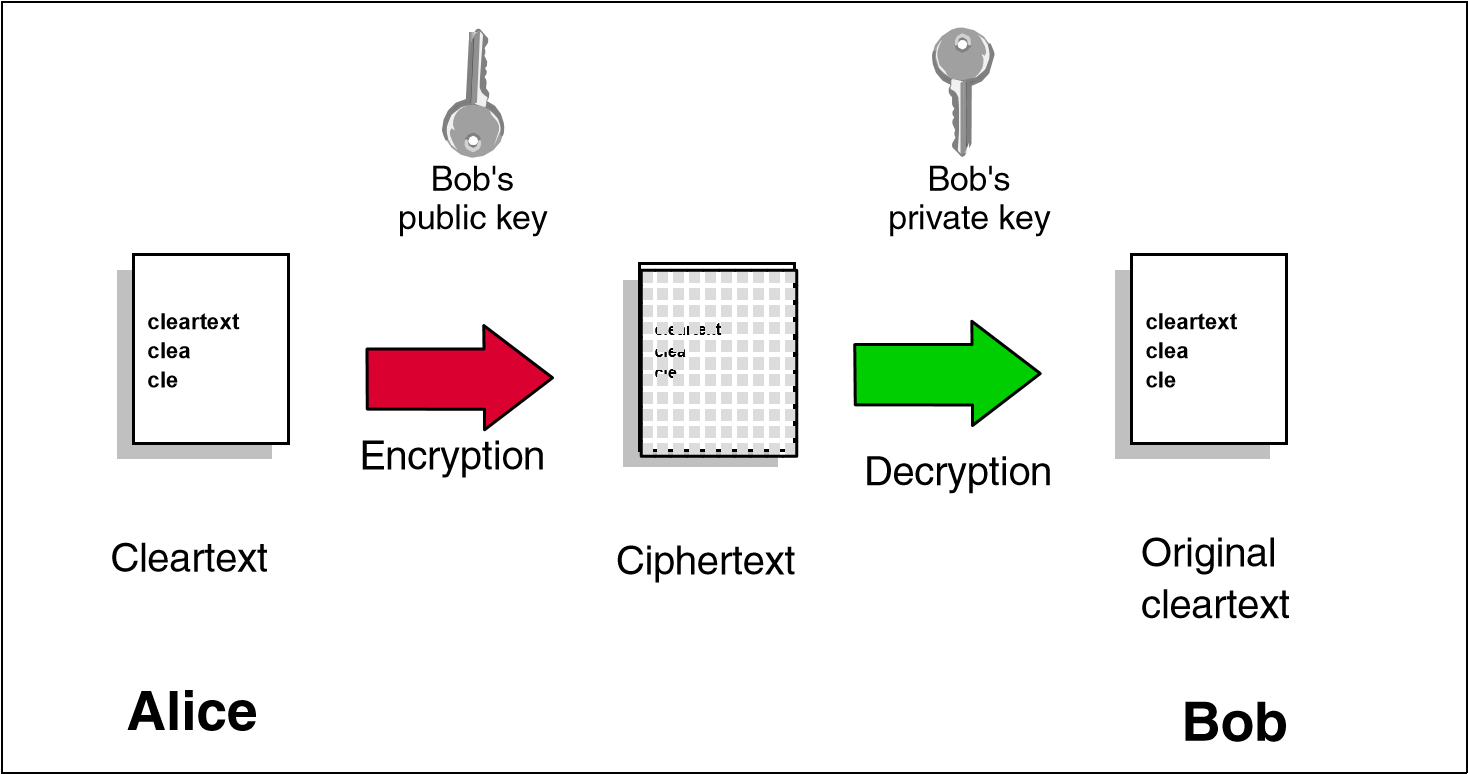
An example of a stream algorithm is A5, which is used to encrypt digital cellular telephony traffic in the GSM standard, widely used in Europe.

The advantage of the symmetric algorithms is their efficiency. They can be easily implemented in hardware. A major disadvantage is the difficulty of key management. A secure way of exchanging the keys must exist, which is often very hard to implement.

#### 22.2.3 Asymmetric or public key algorithms

These algorithms address the major drawback of symmetric ciphers, the requirement of the secure key-exchange channel. The idea is that two different keys should be used: a public key, which, as the name implies, is known to

everyone, and a private key, which is to be kept in tight security by the owner. The private key cannot be determined from the public key. A cleartext encrypted with the public key can only be decrypted with the corresponding private key. A cleartext encrypted with the private key can only be decrypted with the corresponding public key. Therefore, if someone sends a message encrypted with the recipient's public key, it can be read by the intended recipient only. The process is shown in Figure 22-3, where Alice sends an encrypted message to Bob.

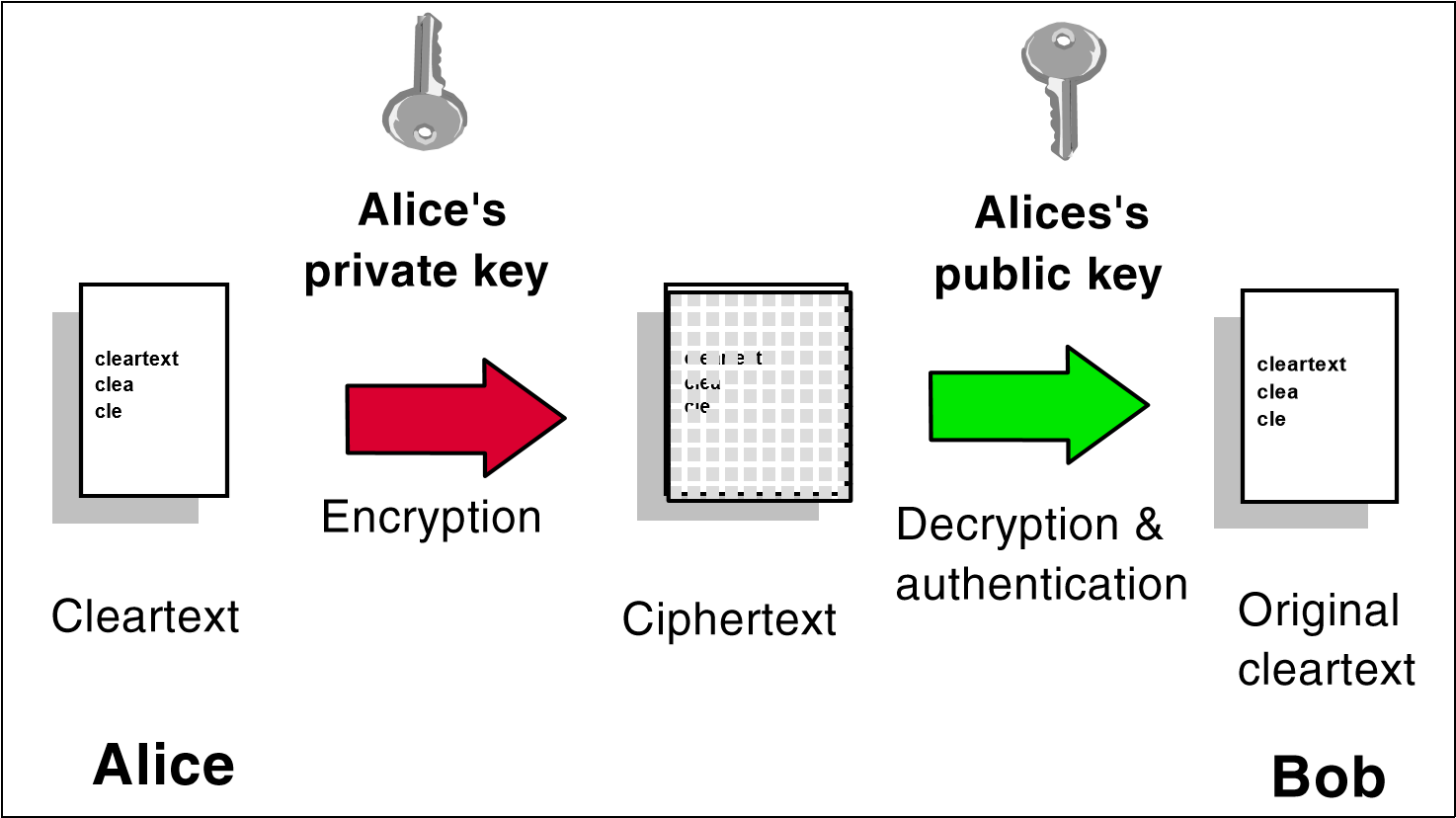


*Figure 22-3 Encryption using the recipient's public key*

As the public key is available to anyone, privacy is assured without the need for a secure key-exchange channel. Parties that want to communicate retrieve each other's public key.

##### Authentication and non-repudiation

An interesting property of the public key algorithms is that they can provide authentication. The private key is used for encryption. Because anyone has access to the corresponding public key and can decrypt the message, this provides no privacy. However, it authenticates the message. If you can successfully decrypt it with the claimed sender's public key, the message has been encrypted with the corresponding private key, which is known by the real sender only. Therefore, the sender's identity is verified. Encryption with the private key is used in *digital signatures*. The principle is shown in Figure 22-4 on page 782. Alice encrypts her message with her private key (“signs” it), in order to enable Bob to verify the authenticity of the message.



*Figure 22-4 Authentication by encrypting with a private key*

Going a step further, encrypting with the private key gives non-repudiation, too. The mere existence of such an encrypted message testifies that the originator has really sent it, because only he or she could have used the private key to generate the message. Additionally, if a time stamp is included, the exact date and time can also be proven. There are protocols involving trusted third parties that prevent the sender from using phony time stamps.

##### Examples of public key algorithms

Algorithms based on public keys can be used for a variety of purposes. Two common applications are:

Encryption (see “RSA public key algorithm” on page 783).

Generation of shared keys for use with symmetric key algorithms (see “Diffie-Hellman key exchange” on page 784).

The most popular public key algorithm is the *de facto* standard RSA, named after its three inventors: Ron Rivest, Adi Shamir, and Leonard Adleman. The security of RSA relies on the difficult problem of factoring large numbers. The public and private keys are functions of two very large (200 digits or even more) prime numbers. Given the public key and the ciphertext, an attack is successful if it can factor the product of the two primes. RSA has resisted many years of extensive attacks. As computing power grows, keeping RSA secure is a matter of increasing the key length (unlike DES, where the key length is fixed).

Another public key algorithm, the very first ever invented, is *Diffie-Hellman*. This is a key exchange algorithm; that is, it is used for securely establishing a shared secret over an insecure channel. The communicating parties exchange public information from which they derive a key. An eavesdropper cannot reconstruct the key from the information that went through the insecure channel. More precisely, the reconstruction is computationally infeasible. The security of Diffie-Hellman relies on the difficulty of calculating discrete logarithms in finite fields. After the shared secret has been established, it can then be used to derive keys for use with symmetric key algorithms such as DES.

Diffie-Hellman makes the secure derivation of a shared secret key possible, but it does not authenticate the parties. For authentication, another public key algorithm must be used, such as RSA.

Unfortunately, public key algorithms, while providing for easier key management, privacy, authentication, and non-repudiation, also have some disadvantages. The most important one is that they are slow and difficult to implement in hardware. For example, RSA is 100 to 10,000 times slower than DES, depending on implementation. Because of this, public key algorithms generally are not used for bulk encryption. Their most important use is key exchange and authentication. Another notable disadvantage is that they are susceptible to certain cryptanalytic attacks to which symmetric algorithms are resistant.

Therefore, a good cryptographic system (*cryptosystem*) makes use of both worlds. It uses public key algorithms in the session establishment phase for authentication and key exchange, and then a symmetric one for encrypting the consequent messages.

For the interested reader, we give more detailed information of the two most important asymmetric algorithms, which involve modular arithmetic. An arithmetic operation modulo m means that the result of that operation is divided by m and the remainder is taken. For example: 3 \* 6 mod 4 = 2, since 3 \* 6 = 18 and dividing 18 by 4 gives us 2 as the remainder.

###### RSA public key algorithm

RSA is used in the ISAKMP/Oakley framework as one of the possible authentication methods. The principle of the RSA algorithm is as follows:

1. Take two large primes, p and q.
2. Find their product n = pq; n is called the modulus.
3. Choose a number, e, less than n and relatively prime to (p-1)(q-1), which means that e and (p-1)(q-1) have no common factor other than 1.
4. Find its inverse, d mod (p-1)(q-1), which means that ed = 1 mod (p-1)(q-1).

e and d are called the public and private exponents, respectively. The public key is the pair (n,e); the private key is d. The factors p and q must be kept secret or destroyed.

A simplified example of RSA encryption is:

1. Suppose Alice wants to send a private message, m, to Bob. Alice creates the ciphertext c by exponentiating:

c = me mod n

Where e and n are Bob's public key.

1. Alice sends c to Bob.
2. To decrypt, Bob exponentiates:

m = cd mod n

And recovers the original message; the relationship between e and d ensures that Bob correctly recovers m. Because only Bob knows d, only Bob can decrypt the ciphertext.

A simplified example of RSA authentication is:

1. Suppose Alice wants to send a signed message, m, to Bob. Alice creates a digital signature s by exponentiating:

s = md mod n

Where d and n belong to Alice's private key.

1. She sends s and m to Bob.
2. To verify the signature, Bob exponentiates and checks if the result, compares to m:

m = se mod n

Where e and n belong to Alice's public key.

###### Diffie-Hellman key exchange

The Diffie-Hellman key exchange is a crucial component of the ISAKMP/Oakley framework. In the earliest phase of a key negotiation session, there is no secure channel in place. The parties derive shared secret keys using the Diffie-Hellman algorithm. These keys will be used in the next steps of the key negotiation protocol. The following steps outline the algorithm:

1. The parties (Alice and Bob) share two public values, a modulus m and an integer g. m is a large prime number.
2. Alice generates a large random number a and computes: X = ga mod m
3. Bob generates a large random number b and computes: Y = gbmod m
4. Alice sends X to Bob.
5. Bob computes:

K1 = Xb mod m

1. Bob sends Y to Alice.
2. Alice computes: K2 = Ya mod m

Both K1 and K2 are equal to gab mod m. This is the shared secret key. No one is able to generate this value without knowing a or b. The security of the exchange is based on the fact that is extremely difficult to inverse the exponentiation performed by the parties. (In other words, to calculate discrete logarithms in finite fields of size m.) Similar to RSA, advances in adversary computing power can be countered by choosing larger initial values, in this case a larger modulus m.

See 22.4.5, “Internet Key Exchange (IKE) protocol” on page 829 for more details about how ISAKMP/Oakley uses Diffie-Hellman exchanges.

#### 22.2.4 Hash functions

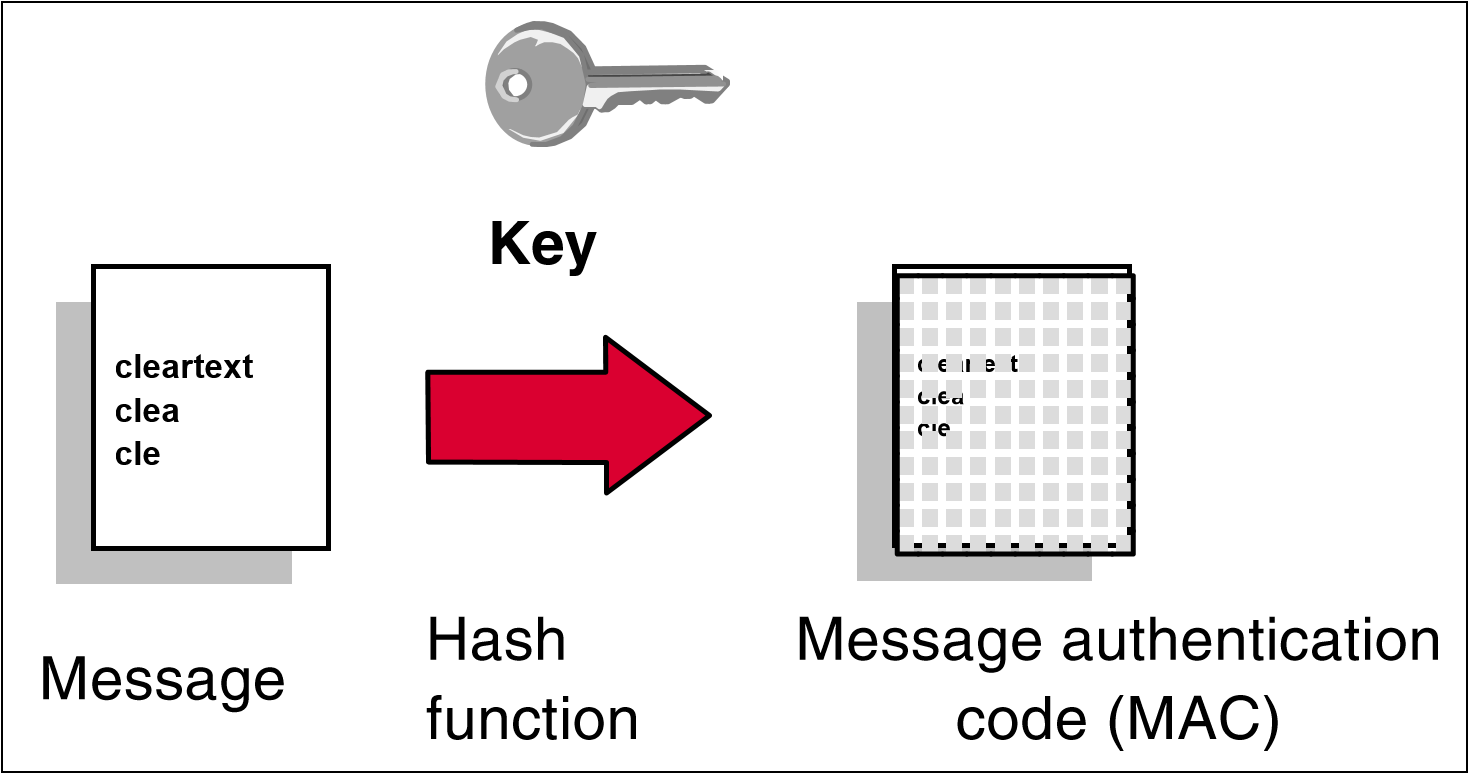
Hash functions (also called message digests) are fundamental to cryptography. A hash function is a function that takes variable-length input data and produces fixed length output data (the hash value), which can be regarded as the “fingerprint” of the input. That is, if the hashes of two messages match, it is highly probable that the messages are the same.

Cryptographically useful hash functions must be *one-way*, which means that they should be easy to compute, but infeasible to reverse. An everyday example of a one-way function is mashing a potato; it is easy to do, but once mashed, reconstructing the original potato is rather difficult.

A good hash function must also be *collision-resistant*. It must be hard to find two different inputs that hash to the same value. Because any hash function maps an input set to a smaller output set, theoretically it is possible to find collisions. The

point is to provide a unique digital “fingerprint” of the message that identifies it with high confidence, much like a real fingerprint identifying a person.

A hash function that takes a key as a second input parameter and its output depends on both the message and the key is called a *message authentication code (MAC)*, as shown in Figure 22-5.



*Figure 22-5 Generating a message authentication code (MAC)*

Put simply, if you encrypt a hash, it becomes a MAC. If you add a secret key to a message, and then hash the concatenation, the result is a MAC. Both symmetric and asymmetric algorithms can be used to generate MACs.

Hash functions are primarily used to assure integrity and authentication:

The sender calculates the hash of the message and appends it to the message.

The recipient calculates the hash of the received message and then compares the result with the transmitted hash.

If the hashes match, the message was not tampered with.

If the encryption key (symmetric or asymmetric) is only known by a trusted sender, a successful MAC decryption indicates that the claimed and actual senders are identical.

See Figure 22-6 for an illustration of the procedure. The Message\* and MAC\* notations reflect the fact that the message might have been altered while crossing the untrusted channel.

**Key**

Message

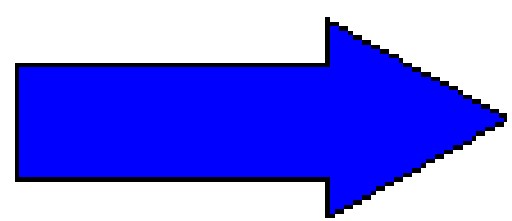
MAC

+



Hash

function



Message\*



Original

MAC



MAC\*

**Untrusted**

**channel**

**Alice**

Match?

Compare

Accept

Reject

NO

YES

**Bob**



*Figure 22-6 Checking integrity and authenticity with MAC*

You might argue that the same result can be obtained with any kind of encryption, because if an intruder modifies an encrypted message, the decryption will result in nonsense, thus tampering can be detected. The answer is that many times only integrity, authentication, or both are needed, maybe with encryption on some of the fields of the message. Also encryption is very processor-intensive. Examples include the personal banking machine networks, where only the PINs are encrypted. However, MACs are widely used. Encrypting all the messages in their entirety would not yield noticeable benefits and performance would dramatically decrease.

The encryption of a hash with the private key is called a *digital signature*. It can be thought of as a special MAC. Using digital signatures instead of encrypting the whole message with the private key leads to considerable performance gains and a remarkable new property. The authentication part can be decoupled from the document itself. This property is used, for example, in the Secure Electronic

Transactions (SET) protocol.

The encryption of a secret key with a public key is called a *digital envelope*. This is a common technique used to distribute secret keys for symmetric algorithms.

##### Examples of hash functions

The most widely used hash functions are MD5 and Secure Hash Algorithm 1 (SHA-1). MD5 was designed by Ron Rivest (co-inventor of RSA). SHA-1 is largely inspired from MD5 and was designed by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) for use with the Digital Signature Standard (DSS). MD5 produces a 128-bit hash, while SHA-1 produces a 160-bit hash. Both functions encode the message length in their output. SHA-1 is regarded as more secure, because of the larger hashes it produces.

Neither MD5 nor SHA-1 takes a key as an input parameter. Therefore, in their original implementation, they cannot be used for MAC calculation. However, for this purpose, it is easy to concatenate a key with the input data and apply the function to the result.

**Note:** In practice, for example, in IPSec, more sophisticated schemes are often used.

###### Keyed MD5 and keyed SHA-1

Using MD5 and SHA-1 in keyed mode is simple. The shared secret key and the data to be protected are both input to the hash algorithm. In the following IPSec example, the datagram is combined with the key, and the output hash value is placed in the Authentication Data field of the AH header, as shown in Figure 22-7.

*Figure 22-7 Keyed MD5 processing*

IP Hdr

AH

Payload

(

Pad

)

MD5

Shared key

(128

bits

)

(128)

Keyed SHA-1 operates in the same way, the only difference being the larger 160-bit hash value.

###### HMAC-MD5-96 and HMAC-SHA-1-96

A stronger method is the Hashed Message Authentication Code (HMAC), proposed by IBM. HMAC itself is not a hash function, rather a cryptographically strong way to use a specific hash function for MAC calculation.

To show how HMAC works, consider MD5 as an example. The base function is applied twice in succession. In the first round, the input to MD5 is the shared secret key and the datagram. The 128-bit output hash value and the key are input again to the hash function in the second round. The left-most 96 bits of the resulting hash value are used as the MAC for the datagram. See Figure 22-8 for an illustration.

*Figure 22-8 HMAC-MD5-96 processing*

IP Hdr

AH

Payload

)

(

Pad

MD5

Shared key

(128

)

bits

(128)

MD5

(128)

(96)

HMAC-SHA-1-96 operates in the same way, except that the intermediary results are 160 bits long.

###### Digital Signature Standard (DSS)

As mentioned previously, a hash value encrypted with the private key is called a *digital signature* and is illustrated in Figure 22-9.



**Private key**

Message



Encryption



Message

digest

(

hash

)

Hash

function

Digital

signature

*Figure 22-9 Generating a digital signature*

One authentication method that can be used with ISAKMP/Oakley is DSS, which was selected by NIST and NSA to be the digital authentication standard of the U.S. government. The standard describes the Digital Signature Algorithm (DSA) used to sign and verify signatures of message digests produced with SHA-1.

The following steps provide a brief description of DSA:

1. Choose a large prime number, p, usually between 512 and 1024 bits long.
2. Find a prime factor q of (p-1), 160 bits long.
3. Compute:

g=h(p-1)/q mod p

Where h is a number less than (p-1) and the following is true:

h(p-1)/q>1

1. Choose another number x, less than q, as the sender's private key.
2. Compute: y=gx mod p

And use that as the sender's public key. The pair (x,y) is sometimes referred to as the long-term key pair.

1. The sender signs the message as follows:
   1. Generate a random number, k, less than q.
   2. Compute:

r=(gk mod p) mod q s=(k-1(SHA1(m)+xr)) mod q

The pair (k,r) is sometimes referred to as the per-session key pair, and the signature is represented by the pair (r,s).

1. The sender sends (m,r,s).
2. The receiver verifies the signature as follows:

Compute:

w=s-1 mod q u1=(SHA1(m)\*w) mod q u2=(rw) mod q v=((gu1yu2) mod p) mod q

1. If v=r, the signature is verified.

#### 22.2.5 Digital certificates and certification authorities

As mentioned in “Authentication and non-repudiation” on page 781, with public key cryptography, the parties retrieve each other's public key. However, there are security exposures here. An intruder can replace some real public keys with his or her own public key, and then mount a so-called *man-in-the-middle attack*.

For example, the intruder places himself between Alice and Bob. He can trick Bob by sending him one of his own public keys as though it were Alice's. The same applies to Alice. She thinks she uses Bob's public key, but she actually uses the intruder's. So, the clever intruder can decrypt the confidential traffic between the two and remain undetected. For example, a message sent by Alice and encrypted with “Bob's” public key arrives at the intruder, who decrypts it, learns its content, then re-encrypts it with Bob's real public key. Bob has no way to realize that Alice is using a phony public key.

An intruder can also use impersonation, claiming to be somebody else, for example, an online shopping mall, fooling innocent shoppers.

The solution to these serious threats is the *digital certificate*. A digital certificate is a file that binds an identity to the associated public key. This binding is validated by a trusted third party, the *certification authority (CA)*. A digital certificate is signed with the private key of the certification authority, so it can be authenticated. It is only issued after a verification of the applicant. Apart from the public key and identification, a digital certificate usually contains other information too, such as:

Date of issue

Expiration date

Miscellaneous information from the issuing CA (for example, serial number)

**Note:** There is an international standard in place for digital certificates: The ISO X.509 protocols.

The parties retrieve each other's digital certificate and authenticate it using the public key of the issuing certification authority. They have confidence that the public keys are real, because a trusted third party vouches for them. This helps protect against both man-in-the-middle and impersonation attacks.

It is easy to imagine that one CA cannot cover all needs. What happens when Bob's certificate is issued by a CA unknown to Alice? Can she trust that unknown authority? Well, this is entirely her decision, but to make life easier, CAs can form a hierarchy, often referred to as the *trust chain*. Each member in the chain has a certificate signed by its superior authority. The higher the CA is in the chain, the tighter security procedures are in place. The root CA is trusted by everyone and its private key is top secret.

Alice can traverse the chain upward until she finds a CA that she trusts. The traversal consists of verifying the subordinate CA's public key and identity using the certificate issued to it by the superior CA.

When a trusted CA is found in the chain, Alice is assured that Bob's issuing CA is trustworthy. This is all about delegation of trust. We trust your identity card if somebody who we trust signs it. And if the signer is unknown to us, we can go upward and see who signs for the signer, and so on.

An implementation of this concept is in the SET protocol, where the major credit card brands operate their own CA hierarchies that converge to a common root. Lotus® Notes® authentication, as another example, is also based on certificates, and it can be implemented using hierarchical trust chains. PGP also uses a similar approach, but its trust chain is based on persons and it is a distributed Web rather than a strict hierarchical tree.

#### 22.2.6 Random-number generators

An important component of a cryptosystem is the random-number generator. Many times random session keys and random initialization variables (often referred to as initialization vectors) are generated. For example, DES requires an explicit initialization vector and Diffie-Hellman relies on picking random numbers which serve as input for the key derivation.

The quality, that is the randomness of these generators, is more important than you might think. The ordinary random function provided with most programming language libraries is good enough for games, but not for cryptography. Those random-number generators are rather predictable; if you rely on them, be prepared for happy cryptanalysts finding interesting correlations in your encrypted output.

The fundamental problem faced by the random-number generators is that the computers are ultimately deterministic machines, so real random sequences cannot be produced. As John von Neumann ironically said: “Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin.” That's why the term *pseudorandom generator* is more appropriate.

Cryptographically strong pseudorandom generators must be unpredictable. It must be computationally infeasible to determine the next random bit, even with total knowledge of the generator.

A common practical solution for pseudorandom generators is to use hash functions. This approach provides sufficient randomness and it can be efficiently implemented. Military-grade generators use specialized devices that exploit the inherent randomness in physical phenomena. An interesting solution can be found in the PGP software. The initial seed of the pseudorandom generator is derived from measuring the time elapsed between the keystrokes of the user.

#### 22.2.7 Export/import restrictions on cryptography

U.S. export regulations changed on January 14, 2000 with the publication of new regulations in the Federal Register. These regulations make it easier for United States companies and individuals to export strong encryption. Some of the changes include:

“Retail” encryption products are widely exportable to all but certain “terrorist” nations though still subject to a government review and reporting requirements.

Non-retail products are also exportable, subject to similar requirements, to most non-government users. Encryption products with less than 64-bits are freely exportable.

Some non-proprietary source code is exportable to most countries after notice to the government.

In September 1998, the White House announced further liberalization of U.S. export restrictions on cryptographic material and key recovery requirements, which can be summarized as follows:

The key recovery requirement for export of 56-bit DES and equivalent products is eliminated. This includes products that use 1024-bit asymmetric key exchanges together with 56-bit symmetric key algorithms.

Export of unlimited strength encryption (for example, 3DES) under license exceptions (with or without key recovery) is now broadened to include others besides the financial industry for 45 countries. This includes subsidiaries of U.S firms, insurance, health and medical (excluding biochemical and pharmaceutical manufacturers), and online merchants for the purpose of securing online transactions (excluding distributors of items considered munitions).

For the latter, recoverable products will be granted exceptions world wide (excluding terrorist countries) without requiring a review of foreign key recovery agents.

Export of recoverable products will be granted to most commercial firms, for a broad range of countries, in the major commercial markets (excluding items on the U.S. munitions list).

Export licenses to end users may be granted on a case-by-case basis.

More information can be obtained from the U.S. Department of Commerce: <http://www.bis.doc.gov/Encryption/Default.htm>

According to the law in France, any product capable of enciphering/deciphering user data must be granted a license from the French government before being marketed. Clients need to be authorized to use such products on a case-by-case basis. In reality, two major and useful exceptions exist:

Routinely, licenses are granted that allow banks to use DES products on a global basis (no case-by-case authorization required).

Routinely, global licenses are granted that allow anybody to use weak encryption (RC2/RC4 with 40-bit keys).

### 22.3 Firewalls

Firewalls have significant functions in an organization's security policy. Therefore, it is important to understand these functions and apply them to the network properly. This chapter explains the firewall concept, network security, firewall components, and firewall examples.

#### 22.3.1 Firewall concept

A firewall is a system (or group of systems) that enforces a security policy between a secure internal network and an untrusted network such as the

Internet. Firewalls tend to be seen as a protection between the Internet and a

private network. But generally speaking, a firewall should be considered as a means to divide the world into two or more networks: one or more secure networks and one or more non-secure networks. See Figure 22-10.



Secure internal

network

Company A

Untrusted

network

(

Internet

)

Secure internal

network

Company B

Firewall

Firewall

*Figure 22-10 A firewall illustration*

A firewall can be a PC, a router, a midrange, a mainframe, a UNIX workstation, or a combination of these that determines which information or services can be accessed from the outside and who is permitted to use the information and services from outside. Generally, a firewall is installed at the point where the secure internal network and untrusted external network meet, which is also known as a *choke point*.

In order to understand how a firewall works, consider the network to be a building to which access must be controlled. The building has a lobby as the only entry point. In this lobby, receptionists welcome visitors, security guards watch visitors, video cameras record visitor actions, and badge readers authenticate visitors who enter the building.

Although these procedures can work well to control access to the building, if an unauthorized person succeeds in entering, there is no way to protect the building against this intruder's actions. However, if the intruder's movements are monitored, it can be possible to detect any suspicious activity.

Similarly, a firewall is designed to protect the information resources of the organization by controlling the access between the internal secure network and the untrusted external network (see Figure 22-11 on page 796). However, it is important to note that even if the firewall is designed to permit the trusted data to pass through, deny the vulnerable services, and prevent the internal network from outside attacks, a newly created attack can penetrate the firewall at any time. The network administrator must examine all logs and alarms generated by the firewall on a regular basis. Otherwise, it is generally not possible to protect the internal network from outside attacks.

Client1

Client2

Internet

Untrusted network

organization.com

Secure

network

priv

ate.organization.com

Production server

**Stop**

*Figure 22-11 A firewall controls traffic between the secure network and the Internet*

#### 22.3.2 Components of a firewall system

As mentioned previously, a firewall can be a PC, a midrange, a mainframe, a UNIX workstation, a router, or combination of these. Depending on the requirements, a firewall can consist of one or more of the following functional components:

Packet-filtering router

Application-level gateway (proxy)

Circuit-level gateway

Each of these components has different functions and shortcomings. Generally, in order to build an effective firewall, these components are used together.

##### Packet-filtering router

Most of the time, packet-filtering is accomplished by using a router that can forward packets according to filtering rules. When a packet arrives at the packet-filtering router, the router extracts certain information from the packet header and makes decisions according to the filter rules as to whether the packet will pass through or be discarded (see Figure 22-12). The following information can be extracted from the packet header:

Source IP address

Destination IP address

TCP/UDP source port

TCP/UDP destination port

ICMP message type

Encapsulated protocol information (TCP, UDP, ICMP, or IP tunnel)

The packet-filtering rules are based on the network security policy (see 22.1.4, “Network security policy” on page 776). Therefore, packet-filtering is done by using these rules as input. When determining the filtering rules, outside attacks must be taken into consideration, as well as service level restrictions and source/destination level restrictions.

*Figure 22-12 Packet-filtering router*

Filter

Client1

Client2

Client3

Client4

Trusted network

Untrusted network

###### Service level filtering

Because most services use well-known TCP/UDP port numbers, it is possible to allow or deny services by using related port information in the filter. For example, an FTP server listens for connections on TCP port 21, and for a non-passive mode client, makes outbound data connections from port 20. Therefore, to permit FTP connections to pass through to a secure network, the router can be configured to permit packets that contain 20 and 21 as the TCP port in its header. However, there are some applications, such as NFS, that use RPC and use different ports for each connection. Allowing these kind of services might cause security problems.

###### Source/destination level filtering

The packet-filtering rules allow a router to permit or deny a packet according to the destination or the source information in the packet header. In most cases, if a service is available, only that particular server is permitted to outside users. Other packets that have another destination or no destination information in their headers are discarded.

###### Advanced filtering

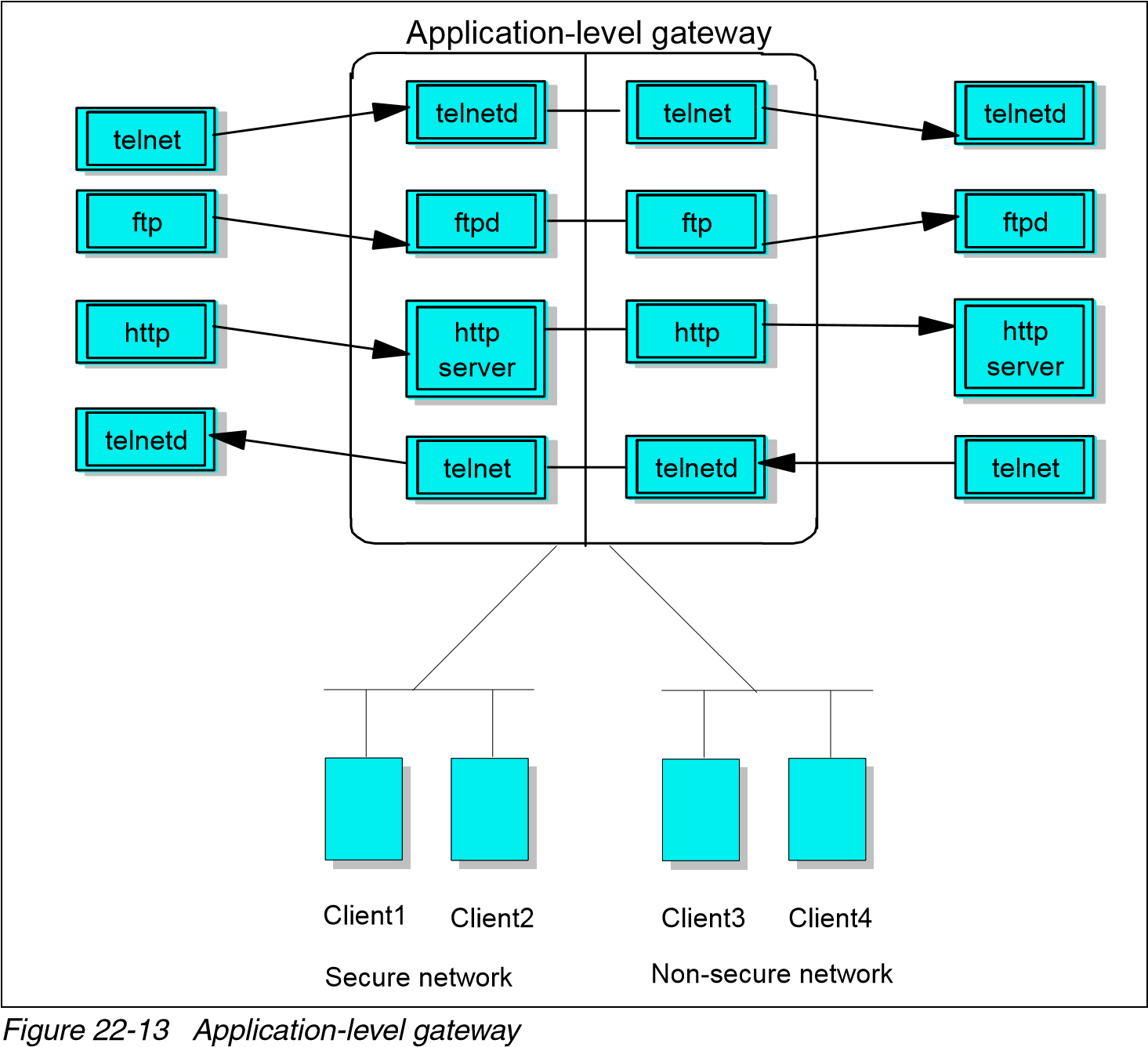
As mentioned previously (see 22.1.1, “Common attacks against security” on page 772), there are different types of attacks that threaten the privacy and network security. Some of them can be discarded by using advanced filtering rules such as checking IP options, fragment offset, and so on.

###### Packet-filtering limitations

Packet-filtering rules are sometimes very complex. When there are exceptions to existing rules, it becomes much more complex. Although there are a few testing utilities available, it is still possible to leave some holes in the network security. Packet filters do not provide an absolute protection for a network. For some cases, it might be necessary to restrict some set of information (for example, a command) from passing through to the internal secure network. It is not possible to control the data with packet filters because they are not capable of understanding the contents of a particular service. For this purpose, an application-level control is required.

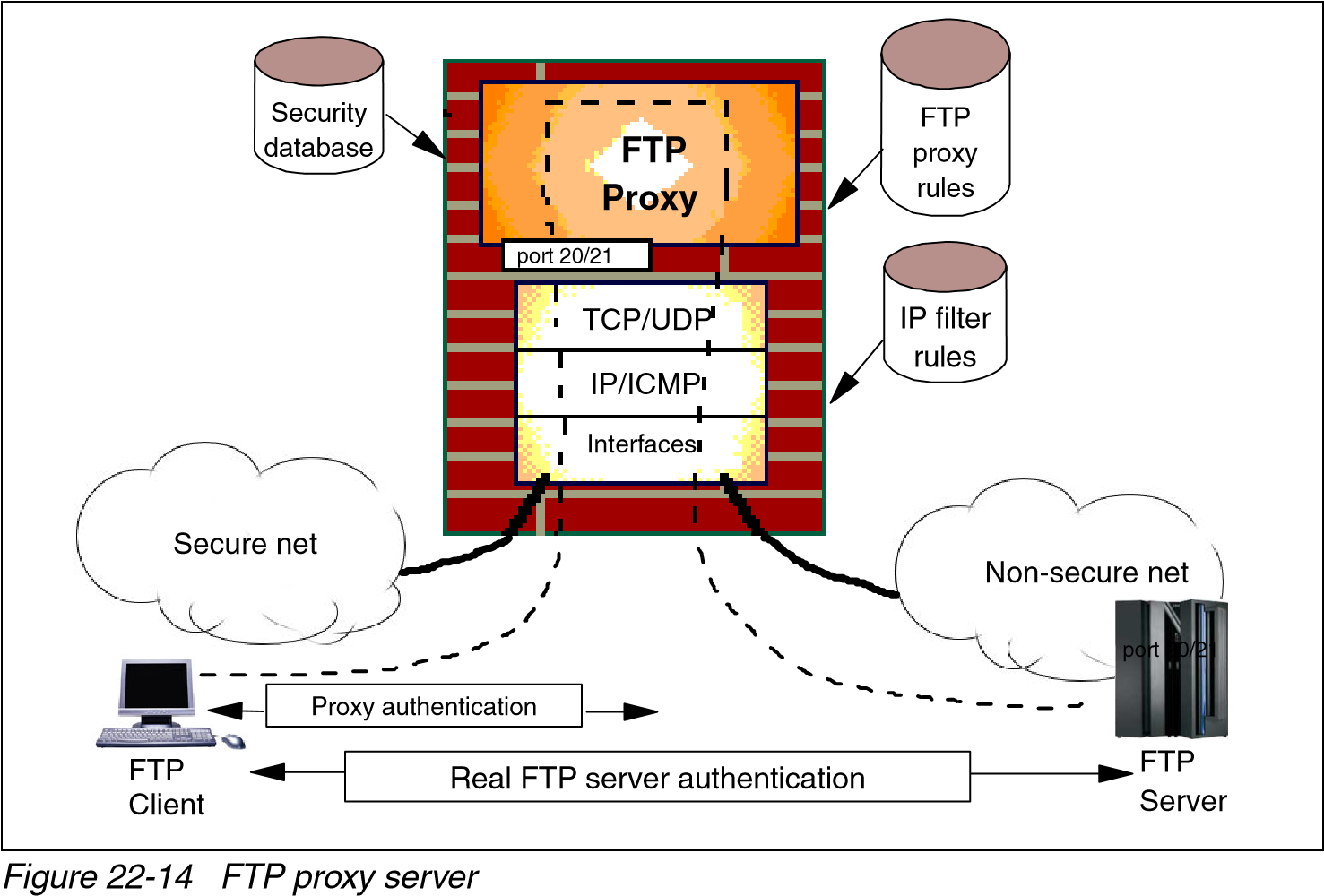
##### Application-level gateway (proxy)

An application-level gateway is often referred to as a *proxy*. An application-level gateway provides higher-level control on the traffic between two networks in that the contents of a particular service can be monitored and filtered according to the network security policy. Therefore, for any desired application, the corresponding proxy code must be installed on the gateway in order to manage that specific service passing through the gateway (see Figure 22-13).



A proxy acts as a server to the client and as a client to the destination server. A virtual connection is established between the client and the destination server. Though the proxy seems to be *transparent* from the point of view of the client and the server, the proxy is capable of monitoring and filtering any specific type of data, such as commands, before sending it to the destination. For example, an FTP server is permitted to be accessed from outside. In order to protect the server from any possible attacks, the FTP proxy in the firewall can be configured to deny PUT and MPUT commands.

A proxy server is an application-specific relay server that runs on the host that connects a secure and a non-secure network. The purpose of a proxy server is to control exchange of data between the two networks at an application level instead of an IP level. By using a proxy server, it is possible to disable IP routing between the secure and the non-secure network for the application protocol the proxy server is able to handle, but still be able to exchange data between the networks by relaying it in the proxy server. Figure 22-14 shows an FTP proxy server.



Note that in order for any client to be able to access the proxy server, the client software must be specifically modified. In other words, the client and server software must support the proxy connection. In the previous example, the FTP client must authenticate itself to the proxy first. If it is successfully authenticated, the FTP session starts based on the proxy restrictions. Most proxy server implementations use more sophisticated authentication methods such as security ID cards. This mechanism generates a unique key that is not reusable for another connection. Two security ID cards are supported by IBM Firewall: the SecureNet card from Axent and the SecureID card from Security Dynamics.

Compared with IP filtering, application-level gateways provide much more comprehensive logging based on the application data of the connections. For example, an HTTP proxy can log the URLs visited by users. Another feature of application-level gateways is that they can use strong user authentication. For example, when using FTP and Telnet services from the unsecure network, users can be forced to authenticate themselves to the proxy. Figure 22-15 shows a proxy server TCP segment flow example.

*Figure 22-15 Proxy server TCP segment flow*

Client host

Proxy server host

Server host

Secure

network

Non-secure

network

epn: Ephemeral port number n

sss: Server port number sss

ssp: Proxy server port number

Proxy Server

Client

Real

Server

ep1

ssp

ep2

sss

###### Application-level gateway limitations

A disadvantage of application-level gateways is that, in order to achieve a connection through a proxy server, the client software must be changed to support that proxy service. This can sometimes be achieved by some modifications in user behavior rather than software modification. For example, to connect to a Telnet server over a proxy, the user usually has to be authenticated by the proxy server then by the destination Telnet server. This requires two user steps to make a connection rather than one. However, a modified Telnet client can make the proxy server transparent to the user by specifying the destination host rather than proxy server in the Telnet command.

###### An example: FTP proxy server

Most of the time, in order to use the FTP proxy server, users must have a valid user ID and password. On UNIX systems, users also must be defined as users of the UNIX system.

FTP can be used in one of two modes:

Normal mode

Passive mode

In normal mode, the FTP client first connects to the FTP server port 21 to establish a control connection. When data transfer is required (for example, as the result of a DIR, GET, or PUT command), the client sends a PORT command to the server instructing the server to establish a data connection from the server's data port (port 20) to a specified ephemeral port number on the client host.

In an FTP proxy server situation, normal mode means that we have to allow inbound TCP connections from the non-secure network to the FTP proxy host. Notice in Figure 22-16 how a connection is established from the FTP server port 20 in the non-secure network to the FTP proxy server's ephemeral port number. To allow this to happen, IP filtering rules are used that allow inbound connection requests from port 20 to an ephemeral port number on the FTP proxy host. This is normally not an IP filter rule. It is sometimes better to add a custom filter rule configuration, because it would allow a cracker to run a program on port 20 and scan all the port numbers above 1023, which, in its simplest form, might result in a denial-of-service situation. Some firewalls handle this correctly by building a table of outgoing FTP requests and matching up the corresponding incoming data transfer request.

Proxy Server

FTP proxy

FTP

client

Client host

FTP proxy server host

FTP

server

Server host

Secure

network

Non-secure

network

epn: Ephemeral port number n

ep1

21

21

ep2

ep4

20

20

ep3

Incoming

*Figure 22-16 Normal mode FTP proxy*

A much more firewall-friendly mode is the passive mode of operation, as shown in Figure 22-17. This mode has been dubbed a firewall-friendly FTP and is described in RFC 1579 – Firewall-Friendly FTP.

Proxy Server

FTP proxy

FTP

client

Client host

FTP proxy server host

FTP

server

Server host

Secure

network

Non-secure

network

epn: Ephemeral port number n

ep1

21

21

ep2

ep4

ep6

ep5

ep3

Outbound

*Figure 22-17 Passive mode FTP proxy (firewall-friendly FTP)*

In passive mode, the FTP client again establishes a control connection to the server's port 21. When data transfer has to start, the client sends a PASV command to the server. The server responds with a port number for the client to contact, in order to establish the data connection, and the client then initiates the data connection.

In this setup, to establish connections to both port 21 and any ephemeral port number in the non-secure network, an ephemeral port number is used on the FTP proxy host. Here, we do not need a rule that allows inbound connections to ephemeral port numbers, because we are now connecting outward.

##### Circuit-level gateway

A circuit-level gateway relays TCP connections and does not provide any extra packet processing or filtering. Some circuit-level gateways can handle UDP packets. A circuit-level gateway can be said to be a special type of application-level gateway. This is because the application-level gateway can be configured to pass all information after the user is authenticated, just as the circuit-level gateway (see Figure 22-18 on page 805). However, in practice, there are significant differences between them, such as:

Circuit-level gateways can handle several TCP/IP applications, as well as UDP applications, without any extra modifications on the client side for each application. Therefore, this makes circuit-level gateways a good choice to satisfy user requirements.

Circuit-level gateways do not provide packet processing or filtering. Therefore, a circuit-level gateway is generally referred to as a *transparent* gateway.

Application-level gateways have a lack of support for UDP.

Circuit-level gateways are often used for outbound connections, while application-level gateways (proxy) are used for both inbound and outbound connections. Generally, when using both types combined, circuit-level gateways can be used for outbound connections and application-level gateways can be used for inbound connections to satisfy both security and user requirements.

Circuit-level gateways can sometimes handle incoming UDP packets or TCP connections. However, a client on the secure side must inform the gateway to expect such packets. SOCKS v5 has this capability.

A well-known example of a circuit-level gateway is SOCKS (refer to 22.5,

“SOCKS” on page 846 for more information). Because the data that flows over SOCKS is not monitored or filtered, a security problem can arise. To minimize security problems, trusted services and resources need to be used on the outside network (untrusted network).

*Figure 22-18 Circuit-level gateway*

Client1

Client3

Client2

Client4

Non-secure network

SOCKS

server

SOCKS-enabled

client program

Unmodified

server program

Secure network

#### 22.3.3 Types of firewalls

A firewall consists of one or more software elements that run on one or more hosts. The hosts can be general purpose computer systems or specialized such as routers. There are four important examples of firewalls. These are:

Packet-filtering firewall

Dual-homed gateway firewall

Screened host firewall

Screened subnet firewall

##### Packet-filtering firewall

The packet-filtering firewall is commonly used because it is inexpensive (see Figure 22-19 on page 806). The firewall is just a router sitting between the external network and the internal secure network. Packet-filtering rules are defined to permit or deny traffic (see “Packet-filtering router” on page 797).

Generally, a packet-filtering firewall is configured to deny any service if it is not explicitly permitted. Although this approach prevents some potential attacks, the firewall is still open to attacks that result from improper filter rule configurations.

Internal

DNS and

Mail server

Router

Packet

filter

Client1

Client2



Internet

Untrusted network

Secure network

organization.com

*Figure 22-19 Packet-filtering firewall*

The filter will allow some of the hosts on the internal network to be directly accessed from the external network. Such hosts need their own authorization mechanism and need to be updated regularly in case of any attacks.

##### Dual-homed gateway firewall

A dual-homed host has at least two network interfaces and therefore at least two IP addresses. IP forwarding is disabled in the firewall, thus all IP traffic between the two interfaces is broken at the firewall (see Figure 22-20 on page 807). Therefore, there is no way for a packet to pass the firewall except through the related proxy or SOCKS service. Unlike the packet-filtering firewalls, dual-homed gateway firewalls make sure that any attack that comes from an unknown service will be blocked. A dual-homed gateway implements the method in which everything not specifically permitted is denied.

*Figure 22-20 Dual-homed firewall*

Internal

DNS and

mail server

Client1

Client2

Packet

filter

Secure network

private.organization.com

Proxy

servers

SOCKS

server

External

DNS

Router



Internet

Untrusted network

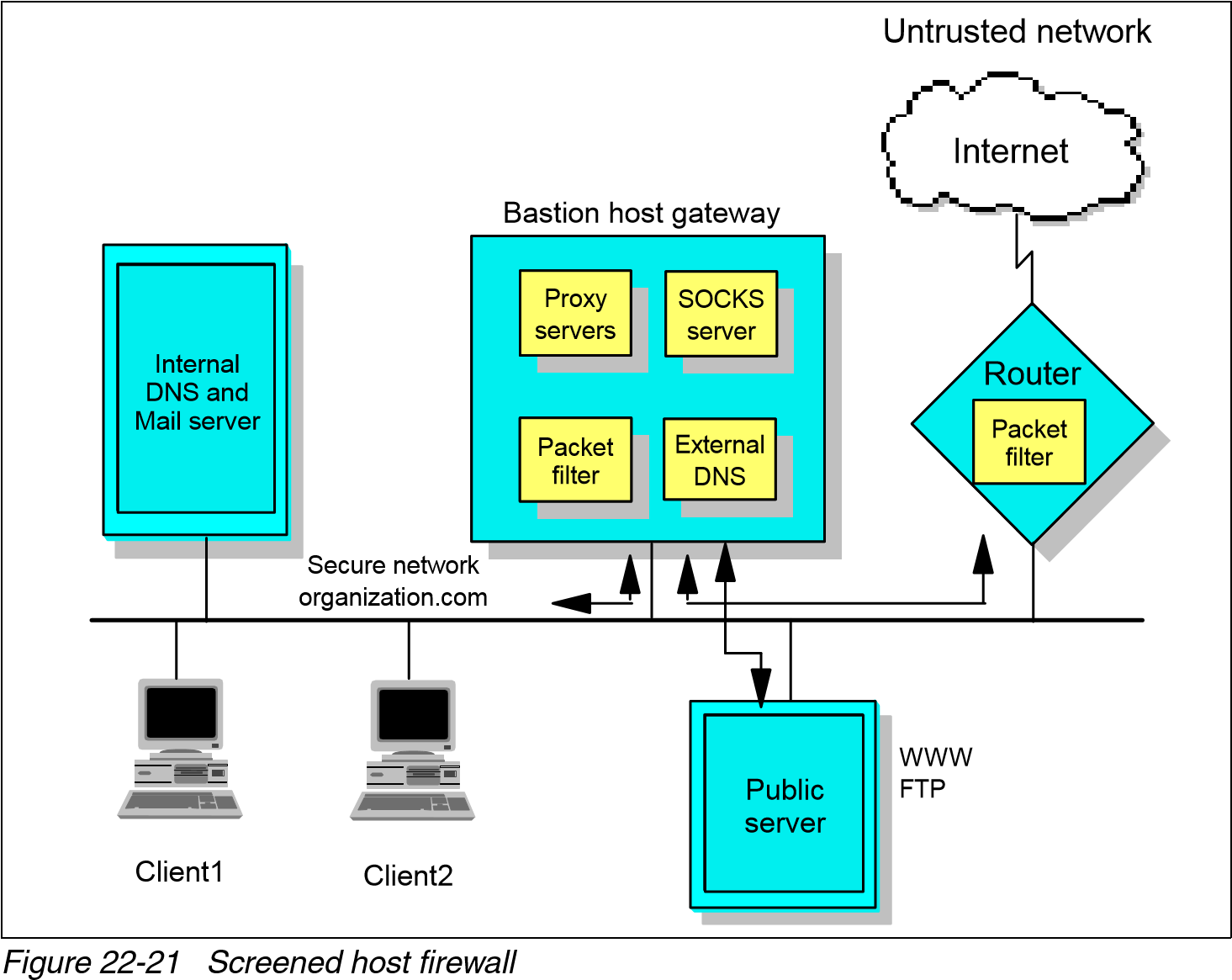
Non-secure network

organization.com

If an information server (such as a Web or FTP server) needs to be located to give access to both inside and outside users, it can either be installed inside the protected network or it can be installed between the firewall and the router, which is relatively insecure. If it is installed beyond the firewall, the firewall must have the related proxy services to give access to the information server from inside the secure network. If the information server is installed between the firewall and the router, the router must be capable of packet filtering and configured accordingly. This type of firewall is called a screened host firewall and discussed in the following section.

##### Screened host firewall

This type of firewall consists of a packet-filtering router and an application-level gateway. The host containing the application-level gateway is known as a bastion host. The router is configured to forward all untrusted traffic to the bastion host and in some cases also to the information server (see Figure 22-21 on page 808). Because the internal network is on the same subnet as the bastion host, the security policy can allow internal users to access outside networks directly or force them to use proxy services to access the outside network. This can be achieved by configuring the router filter rules so that the router only accepts outbound traffic originating from the bastion host.

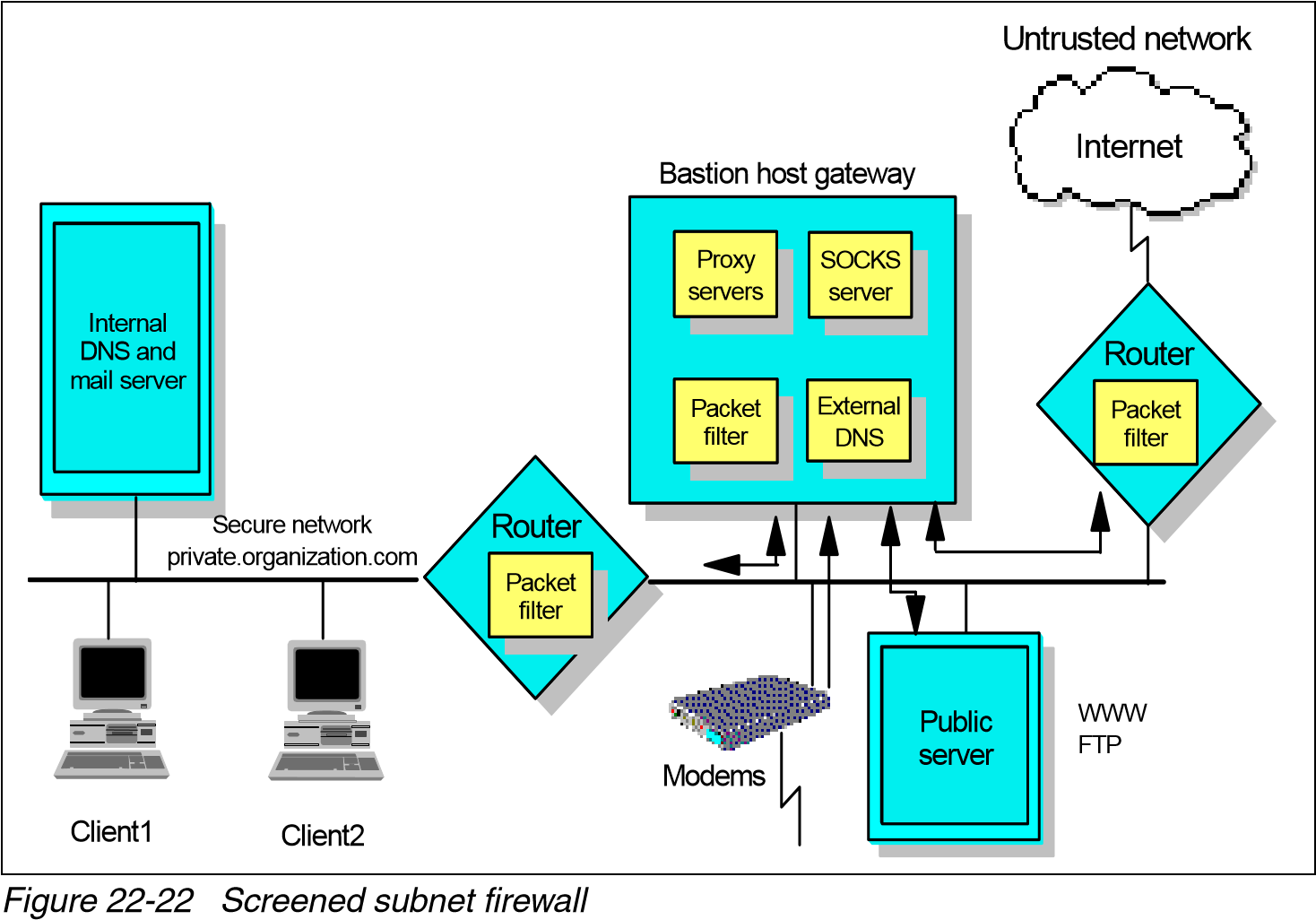


This configuration allows an information server to be placed between the router and the bastion host. Again, the security policy determines whether the information server will be accessed directly by either outside users or internal users, or if it will be accessed through the bastion host. If strong security is needed, traffic from both the internal network to the information server and from outside to the information server can go through the bastion host.

In this configuration, the bastion host can be a standard host or, if a more secure firewall system is needed, it can be a dual-homed host. In this case, all internal traffic to the information server and to the outside through the router is automatically forced to pass the proxy server on the dual-homed host. The bastion host is then the only system that can be accessed from the outside. No one should be permitted to log on to the bastion host; otherwise, an intruder might log on the system and change the configuration to bypass the firewall.

##### Screened subnet firewall (demilitarized zone)

This type of firewall consists of two packet-filtering routers and a bastion host. Screened subnet firewalls provide the highest level security among the different firewall types (see Figure 22-22 on page 809). This is achieved by creating a demilitarized zone (DMZ) between the external and internal network so that the outer router only permits access from the outside to the bastion host (possibly to the information server) and the inner router only permits access from the internal network to the bastion host. The routers force all inbound and outbound traffic through the bastion host. This provides strong security because an intruder has to penetrate three separate systems to reach the internal network.



One of the significant benefits of the DMZ is that because the routers force the systems on both external and internal networks to use the bastion host, there is no need for the bastion host to be a dual-homed host. This provides much faster throughput than achieved by a dual-homed host. Of course, this is complicated and some security problems might be caused by improper router configurations.

### 22.4 IP Security Architecture (IPSec)

This section examines, in detail, the IPSec framework and its three main components, Authentication Header (AH), Encapsulated Security Payload (ESP), and Internet Key Exchange (IKE). We discuss the header formats, the specific cryptographic features, and the different modes of application.

IPSec adds integrity checking, authentication, encryption, and replay protection to IP packets. It is used for end-to-end security and also for creating secure tunnels between gateways.

IPSec was designed for interoperability. When correctly implemented, it does not affect networks and hosts that do not support it. IPSec is independent of the current cryptographic algorithms; it can accommodate new ones as they become available. It works both with IPv4 and IPv6. In fact, IPSec is a mandatory component of IPv6.

IPSec uses state-of-the-art cryptographic algorithms. The specific implementation of an algorithm for use by an IPSec protocol is often called a *transform*. For example, the DES algorithm used by ESP is called the ESP DES-CBC transform. The transforms, like the protocols, are published in the RFCs.

#### 22.4.1 Concepts

Two major IPSec concepts need to be clarified: Security Associations and tunneling. We describe these concepts in the following sections.

##### Security Associations

The concept of a Security Association (SA) is fundamental to IPSec. An SA is a unidirectional (simplex) logical connection between two IPSec systems, uniquely identified by the following triple:

<Security Parameter Index, IP destination address, security protocol>

The definition of the members is as follows:

Security parameter index (SPI)

This is a 32-bit value used to identify different SAs with the same destination address and security protocol. The SPI is carried in the header of the security protocol (AH or ESP). The SPI has only local significance, as defined by the creator of the SA. SPI values in the range 1 to 255 are reserved by the Internet Assigned Numbers Authority (IANA). The SPI value of 0 must be used for local implementation-specific purposes only. RFC 2406 states that a value of 0 must not be transmitted. Generally, the SPI is selected by the destination system during SA establishment.

IP destination address

This address can be a unicast, broadcast, or multicast IP address. However, currently SA management mechanisms are defined only for unicast addresses.

Security protocol

This can be either AH or ESP.

An SA can be in either of two modes, transport or tunnel, depending on the mode of the protocol in that SA. You can find the explanation of these protocol modes later in this chapter.

SAs are simplex, thus, for bidirectional communication between two IPSec systems, there must be two SAs defined, one in each direction.

A single SA gives security services to the traffic carried by it either by using AH or ESP, but not both. In other words, for a connection that needs to be protected by both AH and ESP, two SAs must be defined for each direction. In this case, the set of SAs that define the connection is referred to as an *SA bundle*. The SAs in the bundle do not have to terminate at the same endpoint. For example, a mobile host can use an AH SA between itself and a firewall and a nested ESP SA that extends to a host behind the firewall.

An IPSec implementation maintains two databases related to SAs:

Security Policy Database (SPD)

The Security Policy Database specifies what security services are to be offered to the IP traffic, depending on factors such as source, destination, whether it is inbound, outbound, and so on. It contains an ordered list of policy entries, separate for inbound and outbound traffic. These entries might specify that some traffic must bypass the IPSec processing, some must be discarded, and the rest must be processed by the IPSec module. Entries in this database are similar to firewall rules or packet filters.

Security Association Database (SAD)

The Security Association Database contains parameter information about each SA, such as AH or ESP algorithms and keys, sequence numbers, protocol mode, and SA lifetime. For outbound processing, an SPD entry points to an entry in the SAD. That is, the SPD determines which SA is to be used for a given packet. For inbound processing, the SAD is consulted to determine how the packet must be processed.

**Note:** The user interface of an IPSec implementation usually hides or presents these databases in a friendlier way.

##### Tunneling

Tunneling or encapsulation is a common technique in packet-switched networks. It consists of wrapping a packet in a new one. That is, a new header is attached to the original packet. The entire original packet becomes the payload of the new one, as shown in Figure 22-23.

*Figure 22-23 IP tunneling*

New IP header

IP header

Payload

Original (encapsulated) datagram is

the payload for the new IP header

In general, tunneling is used to carry traffic of one protocol over a network that does not support that protocol directly. For example, NetBIOS or IPX can be encapsulated in IP to carry it over a TCP/IP WAN link. In the case of IPSec, IP is tunneled through IP for a slightly different purpose: To provide total protection, including the header of the encapsulated packet. If the encapsulated packet is encrypted, an intruder cannot figure out, for example, the destination address of that packet. (Without tunneling, the intruder could.) The internal structure of a private network can be concealed in this way.

Tunneling requires intermediate processing of the original packet while en-route. The destination specified in the outer header, usually an IPSec firewall or router, receives the tunneled packet, extracts the original packet, and sends it to the ultimate destination. The processing cost is compensated by the extra security.

A notable advantage of IP tunneling is the possibility to exchange packets with private IP addresses between two intranets over the public Internet, which requires globally unique addresses. Because the encapsulated header is not processed by the Internet routers, only the endpoints of the tunnel (the gateways) need to have globally assigned addresses; the hosts in the intranets behind them can be assigned private addresses (for example, 10.x.x.x). Because globally unique IP addresses are becoming a scarce resource, this interconnection method gains importance.

**Note:** IPSec tunneling is modeled after RFC 2003 – IP Encapsulation within IP. It was originally designed for Mobile IP, an architecture that allows a mobile host to keep its home IP address even if attached to remote or foreign subnets. See 7.1, “Mobile IP overview” on page 276.

#### 22.4.2 Authentication Header (AH)

AH is used to provide integrity and authentication to IP datagrams. Replay protection is also possible. Although its usage is optional, the replay protection service must be implemented by any IPSec-compliant system. The services are connectionless, that is, they work on a per-packet basis. AH is used in two modes, transport mode and tunnel mode.

AH authenticates as much of the IP datagram as possible. In transport mode, some fields in the IP header change en-route and their value cannot be predicted by the receiver. These fields are called *mutable* and are not protected by AH. The mutable IPv4 fields are:

Type of service (TOS)

Flags

Fragment offset

Time to live (TTL)

Header checksum

When protection of these fields is required, tunneling must be used. The payload of the IP packet is considered immutable and is always protected by AH.

AH is identified by protocol number 51, assigned by the IANA. The protocol header (IPv4, IPv6, or extension) immediately preceding the AH contains this value in its protocol (IPv4) or Next header (IPv6, extension) field.

AH processing is applied only to non-fragmented IP packets. However, an IP packet with AH applied can be fragmented by intermediate routers. In this case, the destination first reassembles the packet and then applies AH processing to it. If an IP packet that appears to be a fragment (offset field is non-zero, or the More Fragments bit is set) is input to AH processing, it is discarded. This prevents the so-called *overlapping fragment attack*, which misuses the fragment reassembly algorithm in order to create forged packets and force them through a firewall.

Packets that fail authentication are discarded and never delivered to upper layers. This mode of operation greatly reduces the chances of successful denial-of-service attacks, which aim to block the communication of a host or gateway by flooding it with bogus packets.

##### AH format

The AH format is described in RFC 2402. Figure 22-24 shows the position of the Authentication Header fields in the IP packet.

*Figure 22-24 AH format*

IP Hdr

AH

Payload

Next header

Payld length

Reserved

Security parameter index (SPI)

Sequence number

Authentication data (variable size)

Integrity check value

)

(

32

bits

The fields are as follows:

|  |  |
| --- | --- |
| **Next header** | The next header *t* is an 8-bit field that identifies the type of what follows. The value of this field is chosen from the set of IP protocol numbers defined in the most recent *Assigned Numbers* RFC from the Internet Assigned Numbers Authority (IANA). In other words, the IP header protocol field is set to 51, and the value that would have gone in the protocol field goes in the AH next header field. |
| **Payload length** | This field is 8 bits long and contains the length of the AH header expressed in 32-bit words, minus 2. It does not relate to the actual payload length of the IP packet as a whole. If default options are used, the value is 4 (three  32-bit fixed words plus three 32-bit words of authentication data minus two). |
| **Reserved** | This field is reserved for future use. Its length is 16 bits and it is set to zero. |

###### Security parameter index (SPI)

This field is 32 bits in length. See “Security Associations” on page 810 for a definition.

**Sequence number** This 32-bit field is a monotonically increasing counter, which is used for replay protection. Replay protection is optional; however, this field is mandatory. The sender always includes this field, and it is at the discretion of the receiver to process it or not. At the establishment of an SA, the sequence number is initialized to zero. The first packet transmitted using the SA has a sequence number of 1. Sequence numbers are not allowed to repeat. Therefore, the maximum number of IP packets that can be transmitted on any given SA is 232-1. After the highest sequence number is used, a new SA, and consequently a new key, are established. Anti-replay is enabled at the sender by default. If upon SA establishment the receiver chooses not to use it, the sender need not be concerned with the value in this field anymore.

**Notes:** Typically, the anti-replay mechanism is not used with manual key management. The original AH specification in RFC 1826 did not discuss the concept of sequence numbers. Older IPSec implementations that are based on that RFC can therefore not provide replay protection.

**Authentication data** This is a variable-length field containing the Integrity Check Value (ICV), and is padded to 32 bits for IPv4 or 64 bits for IPv6. The ICV for each packet is calculated with the algorithm selected at SA initialization. As its name implies, it is used by the receiver to verify the integrity of the incoming packet.

In theory, any MAC algorithm can be used to calculate the

ICV. The specification requires that HMAC-MD5-96 and HMAC-SHA-1-96 must be supported. The old RFC 1826 requires Keyed MD5. In practice, Keyed SHA-1 is also used. Implementations usually support two to four algorithms.

When doing the ICV calculation, the mutable fields are considered to be filled with zero.

##### Ways of using AH

AH can be used in two ways: transport mode and tunnel mode.

###### AH in transport mode

In this mode, the authentication header is inserted immediately after the IP header, as shown in Figure 22-25. If the datagram already has IPSec headers, the AH is inserted before them.

IP Hdr

AH

Payload

IP Hdr

Payload

Original IP datagram

Datagram with AH

in transport mode

Authenticated

(

except mutable fields

)

*Figure 22-25 Authentication Header in transport mode*

Transport mode is used by hosts, not by gateways. Gateways are not required to support transport mode.

The advantage of transport mode is fewer processing costs. The disadvantage is that mutable fields are not authenticated.

###### AH in tunnel mode

With this mode, the tunneling concept is applied, a new IP datagram is constructed and the original IP datagram is made the payload of it. AH in transport mode is applied to the resulting datagram. See Figure 22-26 for an illustration.

AH

Authenticated

)

(

except mutable fields

Dest

options\*

Payload

IP Hdr

hop, dest\*,

routing, frag

Ext. Hdr(s)

*Figure 22-26 Authentication Header in tunnel mode*

Tunnel mode is used whenever either end of a Security Association is a gateway. Therefore, between two firewalls, tunnel mode is always used.

Gateways often also support transport mode. This mode is allowed when the gateway acts as a host, that is, in cases when traffic is destined to the gateway itself. For example, SNMP commands can be sent to the gateway using transport mode.

In tunnel mode, the outer headers' IP addresses do not need to be the same as the inner headers' addresses. For example, two security gateways can operate an AH tunnel that is used to authenticate all traffic between the networks they connect together. This is a very typical mode of operation.

The advantages of tunnel mode include total protection of the encapsulated IP datagram and the possibility of using private addresses. However, there are extra processing costs associated with this mode.

**Note:** The original AH specification in RFC 1825 only mentions tunnel mode in passing, not as a requirement. Because of this, there are IPSec implementations based on that RFC that do not support AH in tunnel mode.

##### IPv6 considerations

AH is an integral part of IPv6 (see 9.2.1, “Extension headers” on page 333). In an IPv6 environment, AH is considered an end-to-end payload and it appears after hop-by-hop, routing, and fragmentation extension headers. The destination options extension headers can appear either before or after the Authentication Header. Figure 22-27 illustrates the positioning of AH in transport mode for a typical IPv6 packet. The position of the extension headers marked with an asterisk (\*) is variable, if present at all.

*Figure 22-27 AH in transport mode for IPv6*

AH

Authenticated

(

except mutable fields

)

Dest

options\*

Payload

IP Hdr

hop, dest\*,

routing, frag

Ext. Hdr(s)

For a detailed description of AH in IPv6, refer to RFC 2402.

#### 22.4.3 Encapsulating Security Payload (ESP)

ESP is used to provide integrity check, authentication, and encryption to IP datagrams. Optional replay protection is also possible. These services are connectionless, in that they operate on a per-packet basis. The set of desired services are selectable upon SA establishment. However, some restrictions apply:

Integrity check and authentication are used together.

Replay protection is selectable only in conjunction with integrity check and authentication.

Replay protection can be selected only by the receiver.

Encryption can be selected independently of other services. It is highly recommended that, if encryption is enabled, integrity check and authentication be turned on. If only encryption is used, intruders can forge packets in order to mount cryptanalytic attacks.

Although both authentication (with integrity check) and encryption are optional, at least one of them is always selected; otherwise, you would not be using ESP.

ESP is identified by protocol number 50, as assigned by the IANA. The protocol header (IPv4, IPv6, or extension) immediately preceding the AH header will contain this value in its protocol (IPv4) or the next header field (IPv6, extension).

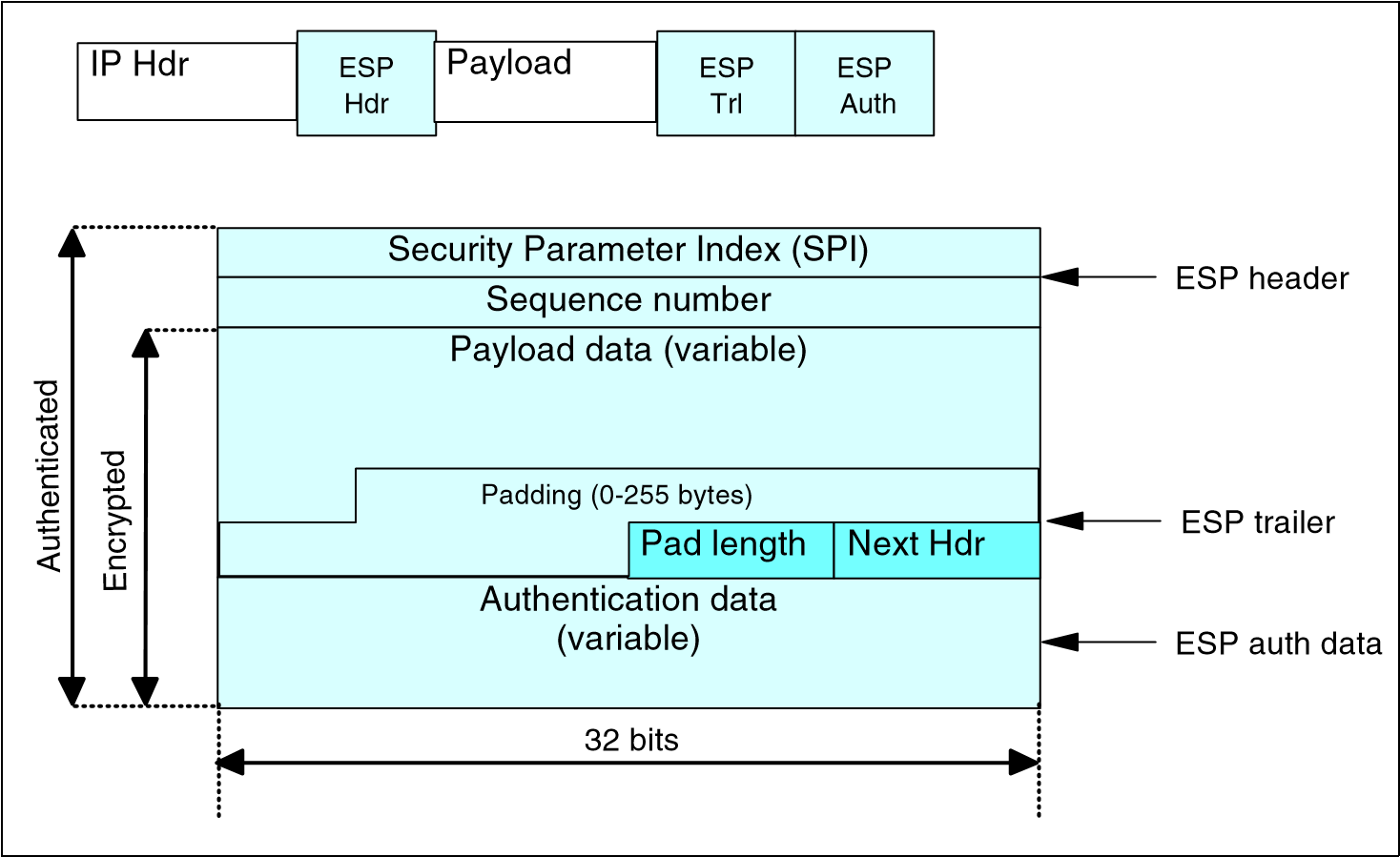
ESP processing is applied only to non-fragmented IP packets. However, an IP packet with ESP applied can be fragmented by intermediate routers. In this case, the destination first reassembles the packet and then applies ESP processing to it. If an IP packet that appears to be a fragment is input to ESP processing (offset field is non-zero, or the More Fragments bit is set), it is discarded. This prevents the overlapping fragment attack mentioned in 22.4.2, “Authentication Header (AH)” on page 813.

If both encryption and authentication with integrity check are selected, the receiver first authenticates the packet and, only if this step was successful, proceeds with decryption. This mode of operation saves computing resources and reduces the vulnerability to denial-of-service attacks.

##### ESP packet format

The current ESP packet format is described in RFC 2406. It contains important modifications compared to the previous ESP specification, RFC 1827. The information in this section is based on RFC 2406.

The format of the ESP packet is more complicated than that of the AH packet. There is not only an ESP header, but also an ESP trailer and ESP authentication data (see Figure 22-28 on page 819). The payload is located (encapsulated) between the header and the trailer, thus the name of the protocol.



*Figure 22-28 ESP header and trailer*

The following fields are part of an ESP packet:

###### Security Parameter Index (SPI)

This field is 32 bits in length. See “AH format” on page 814 for the definition.

**Sequence number** This 32-bit field is a monotonically increasing counter. See “AH format” on page 814 for the definition.

**Notes:** Typically, the anti-replay mechanism is not used with manual key management. The original ESP specification in RFC 1827 did not discuss the concept of sequence numbers. Older IPSec implementations that are based on that RFC can therefore not provide replay protection.

**Payload data** The payload data field is mandatory. It consists of a variable number of bytes of data described by the next header field. This field is encrypted with the cryptographic algorithm selected during SA establishment. If the

algorithm requires initialization vectors, these are also included here.

The ESP specification requires support for the DES algorithm in CBC mode (DES-CBC transform). Often, other encryption algorithms are also supported, such as triple-DES and CDMF, in the case of IBM products.

**Padding** Most encryption algorithms require that the input data must be an integral number of blocks. Also, the resulting ciphertext (including the padding, pad length, and next header fields) must terminate on a 4-byte boundary, so the next header field is right-aligned. For this reason, padding is included. It can also be used to hide the length of the original messages. However, this might adversely impact the effective bandwidth. Padding is an optional field (but needed for some algorithms).

**Note:** The encryption covers the payload data, padding, pad length and next header fields.

**Pad length** This 8-bit field contains the number of the preceding padding bytes. It is always present, and the value of 0 indicates no padding.

**Next header** The next header is an 8-bit mandatory field that shows the data type carried in the payload, for example, an upper-level protocol identifier such as TCP. The values are chosen from the set of IP protocol numbers defined by the IANA.

**Authentication data** This field is variable in length and contains the ICV calculated for the ESP packet from the SPI to the next header field inclusive. The authentication data field is optional. It is included only when integrity check and authentication have been selected at SA initialization time.

The ESP specifications require two authentication algorithms to be supported: HMAC with MD5 and HMAC with SHA-1. Often the simpler keyed versions are also supported by IPSec implementations.

**Notes:** The IP header is not covered by the ICV. The original ESP specification in RFC 1827 discusses the concept of authentication within ESP in conjunction with the encryption transform. That is, there is no authentication data field and it is left to the encryption transforms to eventually provide authentication.

##### Ways of using ESP

Like AH, ESP can be used in two ways: transport mode and tunnel mode.

###### ESP in transport mode

In this mode, the ESP header is inserted right after the IP header, as shown in Figure 22-29. If the datagram already has IPSec header or headers, the ESP header is inserted before any of those. The ESP trailer and the optional authentication data are appended to the payload.

O rig in a l IP d a ta g ra m

ESP

Hdr

D a ta g ra m w ith E S P

in tra n sp o rt m o d e

Encrypted

Authenticated

IP H d r

IP Hdr

P a ylo a d

Payload

ESP

Trl

ESP

Auth

*Figure 22-29 ESP in transport mode*

ESP in transport mode provides neither authentication nor encryption for the IP header. This is a disadvantage, because false packets might be delivered for ESP processing. The advantage of transport mode is the lower processing cost.

As in the case of AH, ESP in transport mode is used by hosts, not gateways. Gateways are not required to support transport mode.

###### ESP in tunnel mode

As expected, this mode applies the tunneling principle. A new IP packet is constructed with a new IP header. ESP is then applied, as in transport mode. This is illustrated in Figure 22-30. Because the original datagram becomes the payload data for the new ESP packet, it is completely protected if both encryption and authentication are selected. However, the new IP header is still not protected.

ESP

Hdr

New

IP Hdr

ESP

Trl

ESP

Auth

IP Hdr

Payload

New

IP Hdr

IP Hdr

Payload

Datagram with ESP

in transport mode

Original IP datagram

Encrypted

Authenticated

IP Hdr

Payload

Tunneled datagram

*Figure 22-30 ESP in tunnel mode*

The tunnel mode is used whenever either end of a Security Association is a gateway. Therefore, between two firewalls the tunnel mode is always used.

Gateways often also support transport mode. This mode is allowed when the gateway acts as a host, that is, in cases when traffic is destined to the gateway itself. For example, SNMP commands can be sent to the gateway using transport mode.

In tunnel mode the outer header's IP addresses does not need to be the same as the inner headers' addresses. For example, two security gateways can operate an ESP tunnel that is used to secure all traffic between the networks they connect together. Hosts are not required to support tunnel mode.

The advantages of tunnel mode are total protection of the encapsulated IP datagram and the possibility of using private addresses. However, there is an extra processing charge associated with this mode.

##### IPv6 considerations

As with AH, ESP is an integral part of IPv6 (see 9.2.1, “Extension headers” on page 333). In an IPv6 environment, ESP is considered an end-to-end payload and it appears after hop-by-hop, routing, and fragmentation extension headers. The destination options extension header(s) could appear either before or after the AH header. Figure 22-31 illustrates the positioning of the AH header in transport mode for a typical IPv6 packet. The position of the extension headers marked with an asterisk (\*) is variable, if present at all.

For more details, refer to RFC 2406.

ESP

Hdr

IP Hdr

hop, dest\*,

routing, frag

ESP

Trl

ESP

Auth

Dest

options\*

Payload

Encrypted

Authenticated

Ext. Hdr

*Figure 22-31 ESP in transport mode for IPv6*

##### Two authentication protocols

Knowing about the security services of ESP, you might ask if there is really a requirement for AH. Why does ESP authentication not cover the IP header as well? There is no official answer to these questions, but here are some points that justify the existence of two different IPSec authentication protocols:

ESP requires strong cryptographic algorithms to be implemented, whether it will actually be used or not. There are restrictive regulations on strong cryptography in some countries. It might be troublesome to deploy ESP-based solutions in such areas. However, authentication is not regulated and AH can be used freely around the world.

Often, only authentication is needed. AH is more performant compared to ESP with authentication only, because of the simpler format and lower processing costs. It makes sense to use AH in these cases.

Having two different protocols means finer-grade control over an IPSec network and more flexible security options. By nesting AH and ESP, for example, you can implement IPSec tunnels that combine the strengths of both protocols.

#### 22.4.4 Combining IPSec protocols

The AH and ESP protocols can be applied alone or in combination. Given the two modes of each protocol, there is quite a number of possible combinations. To make things more complicated, the AH and ESP SAs do not need to have identical endpoints. Luckily, out of the many possibilities, only a few make sense in real-world scenarios.

**Note:** RFC 2406 describes mandatory combinations that must be supported by each IPSec implementation. Other combinations may also be supported, but this might impact interoperability.

We mentioned in “Security Associations” on page 810 that the combinations of IPSec protocols are realized with SA bundles.

There are two approaches to creating an SA bundle:

Transport adjacency: Both security protocols are applied in transport mode to the same IP datagram. This method is practical for only one level of combination.

Iterated (nested) tunneling: The security protocols are applied in tunnel mode, in sequence. After each application, a new IP datagram is created and the next protocol is applied to it. This method has no limit in the nesting levels.

However, more than three levels are impractical.

These approaches can be combined. For example, an IP packet with transport adjacency IPSec headers can be sent through nested tunnels.

When designing a VPN, limit the number of IPSec processing stages. In our view, three stages is the limit beyond which further processing has no benefits. Two stages are sufficient for almost all cases.

Note that, in order to be able to create an SA bundle in which the SAs have different endpoints, at least one level of tunneling must be applied. Transport adjacency does not allow for multiple source/destination addresses, because only one IP header is present.

The practical principle of the combined usage is that, upon the receipt of a packet with both protocol headers, the IPSec processing sequence should be authentication followed by decryption. It is common sense not to bother with decryption of packets of uncertain origin.

Following this principle, the sender first applies ESP and then AH to the outbound traffic. In fact, this sequence is an explicit requirement for transport mode IPSec processing. When using both ESP and AH, a new question arises:

Should ESP authentication be turned on? AH authenticates the packet anyway. The answer is simple.

Turning on ESP authentication makes sense only when the ESP SA extends beyond the AH SA. For example, ESP can be used end-to-end, while AH only goes as far as the remote gateway. In this case, not only does it make sense to use ESP authentication, but we highly recommend doing so to avoid spoofing attacks within the intranet.

As far as the modes are concerned, transport mode is usually used between the endpoints of a connection and tunnel mode is usually used between two machines when at least one of them is a gateway.

Let us take a look at the different ways of using the IPSec protocols, from the simplest to the more complicated nested setups.

##### Case 1: End-to-end security

As shown in Figure 22-32, two hosts are connected through the Internet (or an intranet) without any IPSec gateway between them. They can use ESP, AH, or both. Either transport or tunnel mode can be applied.

*Figure 22-32 End-to-end security*



Internet/

intranet

H1

H2

Connection

IPSec tunnel

The following combinations are required to be supported by any IPSec implementation:

Transport mode

* AH alone
* ESP alone
* AH applied after ESP (transport adjacency)

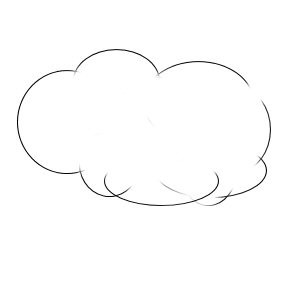
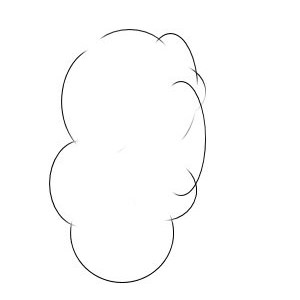
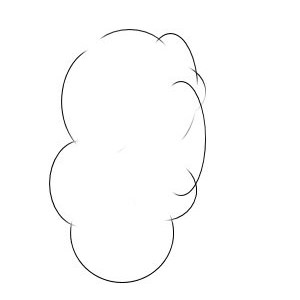
Tunnel mode

* AH alone
* ESP alone

##### Case 2: Basic VPN support

We describe virtual private networks (VPNs) in 22.10, “Virtual private networks (VPNs) overview” on page 861.

Figure 22-33 illustrates the simplest IPSec VPN. The gateways G1 and G2 run the IPSec protocol stack. The hosts in the intranets are not required to support IPSec.



Internet/

intranet

G1

G2

Connection

IPSec tunnel

H1

H2

intranet

intranet

*Figure 22-33 Basic VPN support*

In this case, the gateways are required to support only tunnel mode, either with AH or ESP.

###### Combined tunnels between gateways

Although gateways are required to support either an AH tunnel or ESP tunnel, it is often desirable to have tunnels between gateways that combine the features of both IPSec protocols.

The IBM IPSec implementations support this type of combined AH-ESP tunnels. The order of the headers is user selectable by setting the tunnel policy.

A combined tunnel between gateways does not mean that iterated tunneling takes place. Because the SA bundles comprising the tunnel have identical endpoints, it is inefficient to do iterated tunneling. Instead, one IPSec protocol is applied in tunnel mode and the other in transport mode, which can be conceptually thought of as a combined AH-ESP tunnel. An equivalent approach is to IP tunnel the original datagram and then apply transport adjacency IPSec processing to it. The result is that we have an outer IP header followed by the IPSec headers in the order set by the tunnel policy, and then the original IP packet, as shown in Figure 22-34 on page 827. This is the packet format in a combined AH-ESP tunnel between two IBM firewalls.

**Note:** ESP authentication data was not present in early implementations of the IBM firewall.

*Figure 22-34 Combined AH-ESP tunnel*

ESP

Hdr

IP Hdr

ESP

Trl

Inner

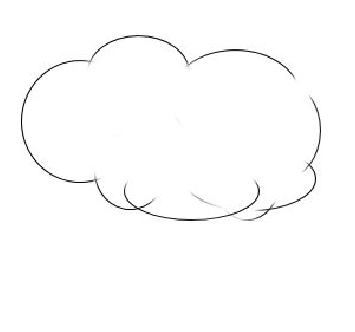
IP Hdr

Payload

AH

##### Case 3: End-to-end security with VPN support

This case is a combination of cases 1 and 2 and does not raise new IPSec requirements for the machines involved (see Figure 22-35). The big difference from case 2 is that now the hosts are also required to support IPSec.



Internet/

intranet

G1

G2

IPSec tunnels

Connection

H1

H2

intranet

intranet

*Figure 22-35 End-to-end security with VPN support*

In a typical setup, the gateways use AH in tunnel mode, while the hosts use ESP in transport mode. An enhanced security version might use a combined AH-ESP tunnel between the gateways. In this way, the ultimate destination addresses are encrypted; the whole packet traveling the Internet would be authenticated and the carried data double encrypted. This is the only case when three stages of IPSec processing might be useful, however, at a cost—the performance impact is considerable.

***AH tunneling of ESP transport*** Let us look in more detail at the common combination of using AH tunneling to protect ESP traffic in transport mode.

Figure 22-36 shows in detail how this combination is realized. Consider that host H1 in Figure 22-35 on page 827 sends an IP packet to host H2. Here is what happens:

1. Host H1 constructs the IP packet and applies ESP transport to it. H1 then sends the datagram to gateway G1, the destination address being H2.
2. Gateway G1 realizes that this packet should be routed to G2. Upon consulting its IPSec databases (SPD and SAD), G1 concludes that AH in tunnel mode must be applied before sending the packet out. It does the required encapsulation. Now the IP packet has the address of G2 as its destination, the ultimate destination H2 being encapsulated.
3. Gateway G2 receives the AH-tunneled packet. It is destined to itself, so it authenticates the datagram and strips off the outer header. G2 sees that the payload is yet another IP packet (that one sent by H1) with destination H2, so it forwards to H2. G2 does not care that this packet has an ESP header.
4. Finally H2 receives the packet. Because this is the destination, ESP-transport processing is applied and the original payload retrieved.

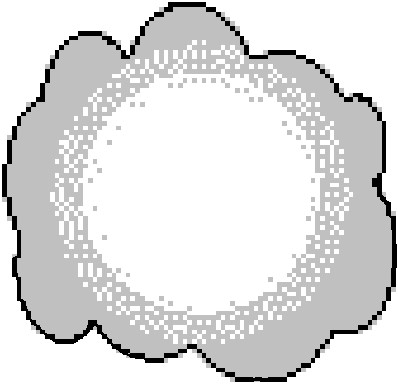
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | | IP Hdr  Src:H1  Dest:H2 | | Payload | | | | | | | IP Hdr  Src:H1  Dest:H2 | | | ESP  Hdr | | | Payload | | | | | ESP  Trl | | | ESP  Auth | | | New IP hdr  Src:G1  Dest:G2 | | | AH | | | IP Hdr  Src:H1  Dest:H2 | | | | | ESP  Hdr | | | Payload | | | | | ESP  Trl | | ESP  Auth | | | IP Hdr  Src:H1  Dest:H2 | | | | ESP  Hdr | | | | Payload | | | | | ESP  Trl | | ESP  Auth | | | IP Hdr  Src:H1  Dest:H2 | | | | Payload | | | | | | |

*Figure 22-36 Nesting of IPSec protocols*

##### Case 4: Remote access

This case, shown in Figure 22-37, applies to remote hosts that use the Internet to reach a server in the organization protected by a firewall. The remote host typically uses a PPP dial-in connection to an ISP.

*Figure 22-37 Remote access*



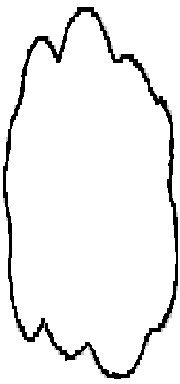
Internet/

intranet

G2

Connection

IPSec tunnels



H1

H2

intranet

Between the remote host H1 and the firewall G2, only tunnel mode is required. The choices are the same as in case 2. Between the hosts themselves, either tunnel mode or transport mode can be used, with the same choices as in case 1.

A typical setup is to use AH in tunnel mode between H1 and G2 and ESP in transport mode between H1 and H2. Older IPSec implementations that do not support AH in tunnel mode cannot implement this.

It is also common to create a combined AH-ESP tunnel between the remote host H1 and the gateway G2. In this case, H1 can access the whole intranet using just one SA bundle, while if it were using the setup shown in Figure 22-37, it only could access one host with one SA bundle.

#### 22.4.5 Internet Key Exchange (IKE) protocol

The Internet Key Exchange (IKE) framework, previously referred to as ISAKMP/Oakley, supports automated negotiation of Security Associations, and automated generation and refresh of cryptographic keys. The ability to perform these functions with little or no manual configuration of machines is a critical element to any enterprise-scale IPSec deployment.

Before describing the details of the key exchange and update messages, some explanations are necessary:

Internet Security Association and Key Management Protocol (ISAKMP)

A framework that defines the management of Security Associations (negotiate, modify, delete) and keys, and it also defines the payloads for exchanging key generation and authentication data. ISAKMP itself does not define any key exchange protocols, and the framework it provides can be applied to security mechanisms in the network, transport, or application layer, and also to itself.

Oakley

A key exchange protocol that can be used with the ISAKMP framework to exchange and update keying material for Security Associations.

Domain of Interpretation (DOI)

Definition of a set of protocols to be used with the ISAKMP framework for a particular environment; also a set of common definitions shared with those protocols regarding the syntax of SA attributes and payload contents, namespace of cryptographic transforms, and so on. In relation to IPSec, the DOI instantiates ISAKMP for use with IP.

Internet Key Exchange (IKE)

A protocol that uses parts of ISAKMP and parts of the Oakley and SKEME key exchange protocols to provide management of keys and Security

Associations for the IPSec AH and ESP protocols and for ISAKMP itself.

##### Protocol overview

ISAKMP requires that all information exchanges must be both encrypted and authenticated, so that no one can eavesdrop on the keying material. The keying material will be exchanged only among authenticated parties. This is required because the ISAKMP procedures deal with initializing the keys, so they must be capable of running over links where no security can be assumed to exist.

In addition, the ISAKMP methods have been designed with the explicit goals of providing protection against several well-known exposures:

Denial of service: The messages are constructed with unique *cookies* that can be used to quickly identify and reject invalid messages without the need to execute processor-intensive cryptographic operations. Man-in-the-middle: Protection is provided against the common attacks such

as deletion of messages, modification of messages, reflecting messages back to the sender, replaying of old messages, and redirection of messages to unintended recipients.

Perfect Forward Secrecy (PFS): Compromise of past keys provides no useful clues for breaking any other key, whether it occurred before or after the compromised key. That is, each refreshed key will be derived without any dependence on predecessor keys.

The following authentication methods are defined for IKE:

Pre-shared key

Digital signatures (DSS and RSA)

Public key encryption (RSA and revised RSA)

The robustness of any cryptography-based solution depends much more strongly on keeping the keys secret than it does on the actual details of the chosen cryptographic algorithms. Therefore, the IETF IPSec Working Group has prescribed a set of extremely robust Oakley exchange protocols. It uses a two-phase approach.

###### Phase 1

This set of negotiations establishes a master secret from which all cryptographic keys will be derived for protecting the users' data traffic. In the most general case, public key cryptography is used to establish an ISAKMP Security Association between systems and to establish the keys that will be used to protect the ISAKMP messages that will flow in the subsequent phase 2 negotiations. Phase 1 is concerned only with establishing the protection suite for the ISAKMP messages themselves, but it does not establish any Security Associations or keys for protecting user data.

In phase 1, the cryptographic operations are the most processor-intensive, but need only be done infrequently, and a single phase 1 exchange can be used to support multiple subsequent phase 2 exchanges. As a guideline, phase 1 negotiations are executed once a day or maybe once a week, while phase 2 negotiations are executed once every few minutes.

###### Phase 2

Phase 2 exchanges are less complex, because they are used only after the security protection suite negotiated in phase 1 has been activated. A set of communicating systems negotiate the Security Associations and keys that will protect user data exchanges. Phase 2 ISAKMP messages are protected by the ISAKMP Security Association generated in phase 1. Phase 2 negotiations generally occur more frequently than phase 1. For example, a typical application of a phase 2 negotiation is to refresh the cryptographic keys once every two to three minutes.

###### Permanent identifiers

The IKE protocol also offers a solution even when the remote host's IP address is not known in advance. ISAKMP allows a remote host to identify itself by a *permanent* identifier, such as a name or an e-mail address. The ISAKMP phase 1 exchanges will then authenticate the remote host's permanent identity using public key cryptography:

Certificates create a binding between the permanent identifier and a public key. Therefore, ISAKMP's certificate-based phase 1 message exchanges can authenticate the remote host's permanent identify.

Because the ISAKMP messages themselves are carried within IP datagrams, the ISAKMP partner (for example, a firewall or destination host) can associate the remote host's dynamic IP address with its authenticated permanent identity.

##### Initializing Security Associations with IKE

This section outlines how ISAKMP/Oakley protocols initially establish Security Associations and exchange keys between two systems that want to communicate securely.

In the remainder of this section, the parties involved are named Host-A and Host-B. Host-A is the initiator of the ISAKMP phase 1 exchanges, and Host-B is the responder. If needed for clarity, subscripts A or B are used to identify the source of various fields in the message exchanges.

##### IKE phase 1: Setting up ISAKMP Security Associations

The Security Associations that protect the ISAKMP messages themselves are set up during the phase 1 exchanges. Because we are starting “cold” (no previous keys or SAs have been negotiated between Host-A and Host-B), the phase 1 exchanges use the ISAKMP Identity Protect Exchange (also known as Oakley Main Mode). Six messages are needed to complete the exchange:

Messages 1 and 2 negotiate the characteristics of the Security Associations. Messages 1 and 2 flow in the clear for the initial phase 1 exchange, and they are unauthenticated.

Messages 3 and 4 exchange nonces (random values) and also execute a Diffie-Hellman exchange to establish a master key (SKEYID). Messages 3 and 4 flow in the clear for the initial phase 1 exchange, and they are unauthenticated.

Messages 5 and 6 exchange the required information for mutually authenticating the parties' identities. The payloads of messages 5 and 6 are protected by the encryption algorithm and keying material established with messages 1 through 4.

A detailed description of the phase 1 messages and exchanged information follows.

###### IKE phase 1, message 1

Because Host-A is the initiating party, it constructs a cleartext ISAKMP message (message 1) and sends it to Host-B. The ISAKMP message itself is carried as the payload of a UDP packet, which in turn is carried as the payload of a normal IP datagram (see Figure 22-38).

IP

Header

UDP

Header

ISAKMP

Header

SA

Proposal

#1

Transform

1)

for #

(

...

Proposal

#n

Transform

(

for #n

)

Host A

Host B

Offer alternatives

Accept one

*Figure 22-38 Message 1 of an ISAKMP phase 1 exchange*

The source and destination addresses to be placed in the IP header are those of Host-A (initiator) and Host-B (responder), respectively. The UDP header will identify that the destination port is 500, which has been assigned for use by the ISAKMP protocol. The payload of the UDP packet carries the ISAKMP message itself.

In message 1, Host-A, the initiator, proposes a set of one or more protection suites for consideration by Host-B, the responder. Therefore, the ISAKMP message contains at least the following fields in its payload:

|  |  |
| --- | --- |
| **ISAKMP header** | The ISAKMP header in message 1 indicates an exchange type of Main Mode and contains a Message ID of 0. Host-A sets the Responder Cookie field to 0 and fills in a random value of its choice for the Initiator Cookie, denoted as Cookie-A. |
| **Security Association** | The Security Association field identifies the Domain of  Interpretation (DOI). Because the hosts plan to run |
| **Proposal Payload** | IPSec protocols between themselves, the DOI is simply IP.  Host-A's Proposal Payload specifies the protocol PROTO\_ISAKMP and sets the SPI value to 0. |

**Note:** For ISAKMP phase 1 messages, the SPI field within the Proposal Payload is not used to identify the ISAKMP Security Association. During phase 1, the ISAKMP SA is identified instead by the pair of values <Initiator Cookie, Responder Cookie>, both of which must be non-zero values. Because the Responder Cookie has not yet been generated by Host-B, the ISAKMP SA is not yet unambiguously identified.

**Transform Payload** The Transform Payload specifies KEY\_OAKLEY. For the KEY\_OAKLEY transform, Host-A must also specify the relevant attributes: namely, the authentication method to be used, the pseudo-random function to be used, and the encryption algorithm to be used.

**Note:** Multiple proposals can be included in message 1.

###### IKE phase 1, message 2

In message 1, Host-A proposed one or more candidate protection suites to be used to protect the ISAKMP exchanges. Host-B uses message 2 to indicate which one, if any, it will support. If Host-A proposed just a single option, Host-B merely needs to acknowledge that the proposal is acceptable.

The source and destination addresses to be placed in the IP header are those of Host-B (responder) and Host-A (initiator), respectively. The UDP header identifies that the destination port is 500, which has been assigned for use by the ISAKMP protocol. The payload of the UDP packet carries the ISAKMP message itself.

The message contents are as follows:

|  |  |  |
| --- | --- | --- |
| **ISAKMP header** | The ISAKMP header in message 2 indicates an exchange type of Main Mode and contains a Message ID of 0. Host-B sets the Responder Cookie field to a random value, which we call Cookie-B, and copies into the Initiator Cookie field the value that was received in the Cookie-A field of message 1. The value pair <Cookie-A, Cookie-B> serves as the SPI for the ISAKMP Security Association. | |
| **Security Association** | The Security Association field identifies the Domain of  Interpretation (DOI). Because the hosts plan to run IPSec protocols between themselves, the DOI is simply IP. | |
| **Proposal Payload** | Host-B's Proposal Payload specifies the protocol PROTO\_ISAKMP and sets the SPI value to 0. |
| **Transform Payload** | The Transform Payload specifies KEY\_OAKLEY. For the KEY\_OAKLEY transform, the attributes that were accepted from the proposal offered by Host-A are copied into the appropriate fields. |

At this point, the properties of the ISAKMP Security Association have been agreed to by Host-A and Host-B. The identity of the ISAKMP SA has been set equal to the pair <Cookie-A, Cookie-B>. However, the identities of the parties claiming to be Host-A and Host-B have not yet been authoritatively verified.

###### IKE phase 1, message 3

The third message of the phase 1 ISAKMP exchange begins the exchange of the information from which the cryptographic keys will eventually be derived (see Figure 22-39 on page 836).

The ISAKMP payload exchanges two types of information.

**Important:** None of the messages themselves carry the actual cryptographic keys. Instead, they carry inputs that will be used by Host-A and Host-B to derive the keys locally.

Diffie-Hellman public value

The Diffie-Hellman public value gx from the initiator. The exponent x in the public value is the private value that must be kept secret.

|  |  |
| --- | --- |
| **Nonce** | The nonce Ni from the initiator. (Nonce is a name for a value that is considered to be random according to some very strict mathematical guidelines.) |
| **ID** | If the RSA public key is used for authentication, the nonces are encrypted with the public key of the other party. Likewise for the IDs of either party, which are then also exchanged at this stage. |

If authentication with revised RSA public key is used, the KE and ID payloads are encrypted with a secret key that is derived from the nonces and the encryption algorithm agreed to in messages 1 and 2, thus avoiding one CPU-intensive public key operation.

Certificates can optionally be exchanged in either case of public key authentication, as well as a hash value thereof.

These values are carried in the Key Exchange, and the Nonce and the ID fields, respectively.



IP

Header

UDP

Header

ISAKMP

Header

g

x

N

j

ID

Certificate

Signature

Host A

Host B

g

x

, N

j

g

y

, N

r

*Figure 22-39 Message 3 of an ISAKMP phase 1 exchange*

###### IKE phase 1, message 4

After receiving a Diffie-Hellman public value and a nonce from Host-A, Host-B responds by sending to Host-A its own Diffie-Hellman public value (gy from the responder) and its nonce (Nr from the responder).

###### Generating the keys (phase 1)

At this point, each host knows the values of the two nonces (Ni and Nr). Each host also knows its own private Diffie-Hellman value (x and y) and also knows its partner's public value (gx or gy). Therefore, each side can construct the composite value gxy. And finally, each side knows the values of the initiator cookie and the responder cookie.

Given all these bits of information, each side can then independently compute identical values for the following quantities:

SKEYID: This collection of bits is sometimes referred to as keying material, because it provides the raw input from which actual cryptographic keys will be derived later in the process. It is obtained by applying the agreed-to keyed pseudorandom function (prf) to the known inputs:

* For digital signature authentication:

SKEYID = prf(Ni, Nr, gxy)

* For authentication with public keys:

SKEYID = prf(hash(Ni, Nr), CookieA, CookieB) – For authentication with a pre-shared key: SKEYID = prf(pre-shared key, Ni, Nr)

Having computed the value SKEYID, each side then proceeds to generate two cryptographic keys and some additional keying material:

* SKEYID\_d is keying material that will be subsequently used in phase 2 to derive the keys that will be used in non-ISAKMP SAs for protecting user traffic:

SKEYID\_d = prf(SKEYID, gxy, CookieA, CookieB, 0)

* SKEYID\_a is the key used for authenticating ISAKMP messages:

SKEYID\_a = prf(SKEYID, SKEYID\_d, gxy, CookieA, CookieB, 1) – SKEYID\_e is the key used for encrypting ISAKMP exchanges:

SKEYID\_e = prf(SKEYID, SKEYID\_a, gxy, CookieA, CookieB, 2)

At this point in the protocol, both Host-A and Host-B have derived identical authentication and encryption keys that they will use to protect the ISAKMP exchanges. And they have also derived identical keying material from which they will derive keys to protect user data during phase 2 of the ISAKMP negotiations. However, at this point, the two parties' identities still have not been authenticated to one another.

###### IKE phase 1, message 5

At this point in the phase 1 flows, the two hosts exchange identity information with each other to authenticate themselves. As shown in Figure 22-40, the ISAKMP message carries an identity payload, a signature payload, and an optional certificate payload. Host-A uses message 5 to send information to Host-B that will allow Host-B to authenticate Host-A.

IP

Header

UDP

Header

ISAKMP

Header

Identity

Certificate

Signature

*Figure 22-40 Message 5 of an ISAKMP phase 1 exchange*

When an actual certificate is present in the Certificate Payload field, the receiver can use the information directly, after verifying that it has been signed with a valid signature of a trusted certificate authority. If there is no certificate in the message, it is the responsibility of the receiver to obtain a certificate using some implementation method. For example, it can send a query to a trusted certificate authority using a protocol such as LDAP, or it can query a secure DNS server, or it can maintain a secure local cache that maps previously used certificates to their respective ID values, or it can send an ISAKMP Certificate Request message to its peer, who must then immediately send its certificate to the requester.

**Note:** The method for obtaining a certificate is a local option, and is not defined as part of IKE. In particular, it is a local responsibility of the receiver to check that the certificate in question is still valid and has not been revoked.

There are several points to bear in mind:

At this stage of the process, all ISAKMP payloads, whether in phase 1 or phase 2, are encrypted, using the encryption algorithm (negotiated in messages 1 and 2) and the keys (derived from the information in messages 3 and 4). The ISAKMP header itself, however, is still transmitted in the clear.

In phase 1, IPSec's ESP protocol is not used; that is, there is no ESP header. The recipient uses the encryption bit in the Flags field of the ISAKMP header to determine if encryption has been applied to the message. The pair of values <CookieA, CookieB>, which serve as an SPI for phase 1 exchanges, provide a pointer to the correct algorithm and key to be used to decrypt the message.

The digital signature, if used, is not applied to the ISAKMP message itself. Instead, it is applied to a hash of information that is available to both Host-A and Host-B.

The identity carried in the identity payload does not necessarily bear any relationship to the source IP address; however, the identity carried in the identity payload must be the identity to which the certificate, if used, applies.

Host-A (the initiator) generates the following hash function, and then places the result in the Signature Payload field:

HASH\_I = prf(SKEYID, gx, gy, CookieA, CookieB, SAp, IDA)

If digital signatures were used for authentication, this hash will also be signed by Host-A.

IDA is Host-A's identity information that was transmitted in the identity payload of this message, and SAp is the entire body of the SA payload that was sent by Host-A in message 1, including all proposals and all transforms proposed by Host-A. The cookies, public Diffie-Hellman values, and SKEYID were explicitly carried in messages 1 through 4, or were derived from their contents.

###### IKE phase 1, message 6

After receiving message 5 from Host-A, Host-B verifies the identity of Host-A by validating the hash.

If digital signatures were used for authentication, the signature of this hash are verified by Host-B.

If this is successful, Host-B sends message 6 to Host-A to allow Host-A to verify the identity of Host-B.

The structure of message 6 is the same as that of message 5, with the obvious changes that the identity payload and the certificate payload now pertain to Host-B:

HASH\_R = prf(SKEYID, gy, gx, CookieB, CookieA, SAp, IDB)

Notice that the order in which Diffie-Hellman public values and the cookies appear has been changed, and the final term now is the identity payload that Host-B has included in message 6.

If digital signatures were used for authentication, this hash is also signed by Host-B, which is different from the one previously signed by Host-A.

When Host-A receives message 6 and verifies the hash or digital signature, the phase 1 exchanges are then complete. At this point, each participant has authenticated itself to its peer. Both have agreed on the characteristics of the ISAKMP Security Associations, and both have derived the same set of keys (or keying material).

###### Miscellaneous phase 1 facts

There are several miscellaneous facts worth noting:

Regardless of the specific authentication mechanism that is used, there will be six messages exchanged for the Oakley Main Mode. However, the content of the individual messages differs, depending on the authentication method.

Although Oakley exchanges make use of both encryption and authentication, they do not use either IPSec's ESP or AH protocol. ISAKMP exchanges are protected with application-layer security mechanisms, not with network-layer security mechanisms.

ISAKMP messages are sent using UDP. There is no guaranteed delivery for them.

The only way to identify that an ISAKMP message is part of a phase 1 flow rather than a phase 2 flow is to check the Message ID field in the ISAKMP header. For phase 1 flows, it must be 0, and (although not explicitly stated in the ISAKMP documents) for phase 2 flows, it must be non-zero.

##### IKE phase 2: Setting up protocol Security Associations

After completing the phase 1 negotiation process to set up the ISAKMP Security Associations, Host-A's next step is to initiate the Oakley phase 2 message exchanges (also known as Oakley Quick Mode) to define the Security Associations and keys that will be used to protect IP datagrams exchanged between the pair of users. (In the Internet drafts, these are referred to somewhat obtusely as “non-ISAKMP SAs.”)

Because the purpose of the phase 1 negotiations was to agree on how to protect ISAKMP messages, all ISAKMP phase 2 payloads, but not the ISAKMP header itself, must be encrypted using the algorithm agreed to by the phase 1 negotiations.

When Oakley Quick Mode is used in phase 2, authentication is achieved through the use of several cryptographically based hash functions. The input to the hash functions comes partly from phase 1 information (SKEYID) and partly from information exchanged in phase 2. Phase 2 authentication is based on certificates, but the phase 2 process itself does not use certificates directly. Instead, it uses the SKEYID\_a material from phase 1, which itself was authenticated through certificates.

Oakley Quick Mode comes in two forms:

Without a Key Exchange attribute, Quick Mode can be used to refresh the cryptographic keys, but does not provide the property of Perfect Forward Secrecy (PFS).

With a Key Exchange attribute, Quick Mode can be used to refresh the cryptographic keys in a way that provides PFS. This is accomplished by including an exchange of public Diffie-Hellman values within messages 1 and 2.

**Note:** PFS apparently is a property that is very much desired by cryptography experts, but strangely enough, the specifications treat PFS as optional. They mandate that a system must be capable of handling the Key Exchange field when it is present in a Quick Mode message, but do not require a system to include the field within the message.

A detailed description of the phase 2 messages and exchanged information follows.

###### IKE phase 2, message 1

Message 1 of a Quick Mode Exchange allows Host-A to authenticate itself, to select a nonce, to propose Security Associations to Host-B, to execute an exchange of public Diffie-Hellman values, and to indicate if it is acting on its own behalf or as a proxy negotiator for another entity. An overview of the format of message 1 is shown in Figure 22-41.

**Note:** Inclusion of a Key Exchange field is optional. However, when Perfect Forward Secrecy is used, it must be present.

IP

Header

UDP

Header

ISAKMP

Header

Hash

SA

Proposal

#1

Transform

#1

...

Proposal

#n

Transform

#n

N

K

E

IDs

Host A

Host B

Hash-1,SA(ESP & AH),g

x

, N

j

Hash-2,SA(ESP & AH),g

y

, N

r

Hash-3

*Figure 22-41 Message 1 of an ISAKMP phase 2 Quick Mode Exchange*

Because we assumed that Host-A and Host-B are each acting on their own behalf, the user identity fields illustrated in Figure 22-41 will not be present. The message will consist of:

**ISAKMP header** The ISAKMP header indicates an exchange type of Quick Mode, includes a non-zero Message ID chosen by Host-A, includes the initiator and responder cookie values chosen in phase 1 (that is, Cookie-A and Cookie-B), and turns on the encryption flag to indicate that the payloads of the ISAKMP message are encrypted according to the algorithm and key negotiated during phase 1.

**Hash** A Hash payload must immediately follow the ISAKMP header. HASH\_1 uses the keyed pseudo-random function that was negotiated during the phase 1 exchanges, and is derived from the following information:

HASH\_1 = prf(SKEYID\_a, M-ID, SA, Nqmi, KE, IDqmi, IDqmr)

* SKEYID\_a was derived from the phase 1 exchanges.
* M-ID is the message ID of this message.
* SA is the Security Association payload carried in this message, including all proposals that were offered.
* Nonce is a new value different from the one used in phase 1.
* KE is the public Diffie-Hellman value carried in this message. This quantity is chosen by Host-A, and is denoted as gqmx. Note that this is not the same quantity as gx that was used in the phase 1 exchanges.
* IDs, which can identify either the endpoints of the phase 1 exchange or endpoints on whose behalf the protocol SA should be negotiated (proxy IDs when IKE is used in client mode). These can subsequently be different from the IDs used in phase 1.

**Note:** The use of KE and ID is optional, depending if PFS is used.

**Security Association** Indicates IP as the Domain of Interpretation.

Proposal, Transform Pairs

There can be one or more of these pairs in this message. The first proposal payload is numbered 1, identifies an IPSec protocol to be used, and includes an SPI value that is randomly chosen by Host-A for use with that protocol. The proposal payload is followed by a single transform payload that indicates the cryptographic algorithm to be used with that protocol. The second proposal payload is numbered 2, and so on.

**Nonce payload** This contains the nonce Nqmi that was chosen

randomly by Host-A.

|  |  |
| --- | --- |
| **KE** | This is the key exchange payload that carries the public Diffie-Hellman value chosen by Host-A, gqmx. There is also a field called Group that indicates the  prime number and generator used in the Diffie-Hellman exchange. |
| **ID payload** | Specifies the endpoints for this SA. |

###### IKE phase 2, message 2

After Host-B receives message 1 from Host-A and successfully authenticates it using HASH\_1, it constructs a reply, message 2, to be sent back to Host-A. The Message ID of the reply is the same one that Host-A used in message 1.

Host-B chooses new values for the following:

**Hash** The hash payload now carries the value HASH\_2,

which is defined as:

HASH\_2 = prf(SKEYID\_a, Nqmi, M-ID, SA, Nqmr, KE, IDqmi, IDqmr)

|  |  |
| --- | --- |
| **Security Association** | The Security Association payload only describes the single chosen proposal and its associated transforms, not all of the protection suites offered by Host-A. Host-B also chooses an SPI value for the selected protocol. Host-B's SPI does not depend in any way on the SPI that Host-A assigned to that protocol when it offered the proposal. That is, it is not necessary that SPIA be the same as SPIB; it is only necessary that they each be non-zero and that they each be randomly chosen. |
| **Nonce** | Nonce payload now carries Nr, a random value chosen by Host-B. |
| **KE** | Key exchange payload now carries Host-B's public Diffie-Hellman value, gqmy. |

At this point, Host-A and Host-B have exchanged nonces and public Diffie-Hellman values. Each one can use this in conjunction with other information to derive a pair of keys, one for each direction of transmission.

###### Generating the keys (phase 2)

Using the nonces, public Diffie-Hellman values, SPIs, protocol code points exchanged in messages 1 and 2 of phase 2, and the SKEYID value from phase 1, each host now has enough information to derive two sets of keying material:

When PFS is used:

* For data generated by Host-A and received by Host-B, the keying material is:

KEYMATAB = prf(SKEYID\_d, gqmxy, protocol, SPIB, Nqmi, Nqmr)

* For data generated by Host-B and received by Host-A, the keying material is:

KEYMATBA = prf(SKEYID\_d, gqmxy, protocol, SPIA, Nqmi, Nqmr) When PFS is not used:

* For data generated by Host-A and received by Host-B, the keying material is:

KEYMATAB = prf(SKEYID\_d, protocol, SPIB, Nqmi, Nqmr)

* For data generated by Host-B and received by Host-A, the keying material is:

KEYMATBA = prf(SKEYID\_d, protocol, SPIA, Nqmi, Nqmr)

**Note:** Depending on the particular case, Host-A might need to derive multiple keys for the following purposes:

Generating the integrity check value for transmitted datagrams

Validating the integrity check value of received datagrams

Encrypting transmitted datagrams

Decrypting received datagrams

Likewise, Host-B needs to derive the mirror image of the same keys. For example, the key that Host-B uses to encrypt its outbound messages is the same key that Host-A uses to decrypt its inbound messages, and so on.

###### IKE phase 2, message 3

At this point, Host-A and Host-B have exchanged all the information necessary for them to derive the necessary keying material. The third message in the Quick Mode exchange is used by Host-A to prove its alive state, which it does by producing a hash function that covers the message ID and both nonces that were exchanged in messages 1 and 2. Message 3 consists only of the ISAKMP header and a hash payload that carries:

HASH\_3 = prf(SKEYID\_a, 0, M-ID, Nqmi, Nqmr)

When Host-B receives this message and verifies the hash, both systems can begin to use the negotiated security protocols to protect their user data streams.

##### Negotiating multiple Security Associations

It is also possible to negotiate multiple Security Associations, each with its own set of keying material, within a single three-message Quick Mode exchange.

The message formats are very similar to the previously illustrated ones, so we only highlight the differences:

Message 1 carries multiple Security Association payloads, each offering a range of protection suites.

HASH\_1 covers the entire set of all offered Security Associations carried in message 1. That is, each Security Association and all of its offered proposals are included.

In message 2, for each offered SA, Host-B selects a single protection suite. That is, if n SAs are open for negotiation, Host-B chooses n protection suites, one from each proposal.

As was the case for HASH\_1, HASH\_2 now covers the entire set of all offered Security Associations carried in message 1. That is, each Security Association and all of its offered proposals are included.

After messages 1 and 2 have been exchanged, Host-A and Host-B generate the keying material for each of the accepted protection suites, using the same formulas as in “Generating the keys (phase 2)” on page 844, applied individually for each accepted SA. Even though the nonces and the public Diffie-Hellman values are the same for all selected suites, the keying material derived for each selected protection suite is different because each proposal has a different SPI.

Because multiple Security Associations have been negotiated, it is a matter of local choice as to which one is used to protect a given datagram. A receiving system must be capable of processing a datagram that is protected by any SA that has been negotiated. That is, it is legal for a given source host to send two consecutive datagrams to a destination system, where each datagram was protected by a different SA.

##### Using IKE with remote access

The critical element in the remote access scenario is the use of Oakley to identify the remote host by name, rather than by its dynamically assigned IP address. After the remote host's identity has been authenticated and the mapping to its dynamically assigned IP address has been ascertained, the remainder of the processes are the same as we have described for the other scenarios. For example, if the corporate intranet is considered to be trusted, the remote host needs to establish a single SA between itself and the firewall. But if the corporate intranet is considered to be untrusted, it might be necessary for the remote host to set up two SAs: one between itself and the firewall, and a second between itself and the destination host.

Recall that a single ISAKMP phase 1 negotiation can protect several subsequent phase 2 negotiations. Phase 1 ISAKMP negotiations use computationally intensive public key cryptographic operations, while phase 2 negotiations use the less computationally intensive symmetric key cryptographic operations. Therefore, the heavy computational load only occurs in phase 1, which is only executed when the dial-up connection is first initiated.

The principal points that pertain to the remote access case are:

The remote host's dynamically assigned address is the one that is placed in the IP header of all ISAKMP messages.

The remote host's permanent identifier (such as an e-mail address) is the quantity that is placed in the ID field of the ISAKMP phase 1 messages.

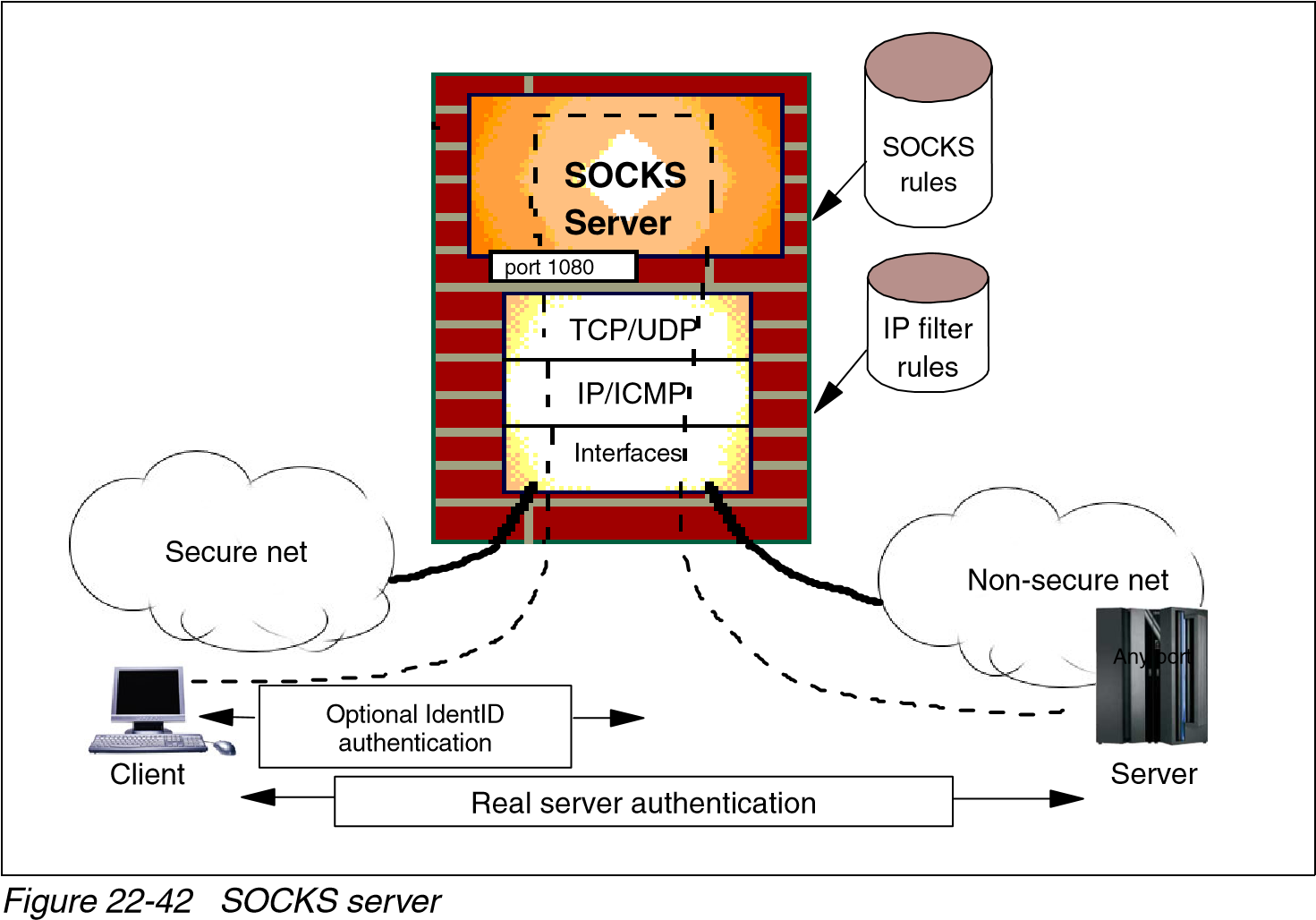
The remote host's certificate used in the ISAKMP exchange must be associated with the remote host's permanent identifier.

In traffic-bearing datagrams, the remote host's dynamically assigned IP address is used. This is necessary because the destination IP address that appears in the datagram's IP header is used in conjunction with the SPI and protocol type to identify the relevant IPSec Security Association for processing the inbound datagram.

### 22.5 SOCKS

SOCKS is a standard for circuit-level gateways. It does not require the processing costs associated with a more conventional proxy server where a user has to consciously connect to the firewall first before requesting the second connection to the destination (see Figure 22-42 on page 847).

The user starts a client application with the destination server IP address. Instead of directly starting a session with the destination server, the client initiates a session to the SOCKS server on the firewall. The SOCKS server then validates that the source address and user ID are permitted to establish an onward connection into the nonsecure network, and then creates the second session.



SOCKS needs to have new versions of the client code (called SOCKS-enabled clients) and a separate set of configuration profiles on the firewall. However, the server machine does not need modification; indeed, it is unaware that the session is being relayed by the SOCKS server. Both the client and the SOCKS server need to have SOCKS code. The SOCKS server acts as an application-level router between the client and the real application server. SOCKSv4 is for outbound TCP sessions only. It is simpler for the private network user, but does not have secure password delivery, so it is not intended for sessions between public network users and private network applications. SOCKSv5 provides for several authentication methods and can therefore be used for inbound connections as well, though these need to be used with caution. SOCKSv5 also supports UDP-based applications and protocols.

The majority of Web browsers are SOCKS-enabled and you can get SOCKS-enabled TCP/IP stacks for most platforms. For additional information, refer to RFC 1928, RFC 1929, RFC 1961, and the following URL: [http://www.socks.nec.com](http://www.socks.nec.com/)

#### 22.5.1 SOCKS Version 5 (SOCKSv5)

SOCKS version 5 is a proposed standard protocol with a status of elective. It is described in RFC 1928.

Application-level gateways provide secure connections for some applications such as Telnet, FTP, and SMTP. However, it is not easy to write proxy code for each new application. Generally, the proxy service becomes available after some time, even if the service can be used directly and application-level gateways do not allow UDP connections. SOCKSv5 satisfies all these shortcomings and requirements with a strong authentication mechanism and the hiding of addresses from a non-secure network. Although supporting UDP might seem to be vulnerable, it can be configured to pass UDP for particular users and particular applications only.

The SOCKSv5 concept is based on SOCKSv4 with some extensions such as UDP support, new and various sophisticated authentication methods, and extended addressing schemes to cover domain-name and IPv6. SOCKSv5 supports a range of authentication methods, including:

User name/password authentication

One-time password generators

Kerberos

Remote Authentication Dial-In User Services (RADIUS)

Password Authentication Protocol (PAP)

IPSec authentication method

SOCKSv5 also supports the following encryption standards:

DES

Triple DES

IPSec

The following tunneling protocols are supported:

PPTP

L2F

L2TP

The following key management systems are supported:

SKIP

ISAKMP/Oakley

*Figure 22-43 Socks TCP segment flow*

Proxy Server

SOCKS

Client

Client host

SOCKS host

Real

server

Server host

Secure

network

Non-secure

network

epn: Ephemeral port number n

sss: Server port number sss

ep1

1080

IdentD

113

sss

ep2

ep3

The SOCKSv5 server listens for connections on a given port, usually 1080. According to the connection type (TCP or UDP), the steps discussed in the following sections establish a connection.

##### SOCKSv5 TCP connection

To establish a connection using TCP, the client first sends a TCP packet that contains session request information through port 1080 to the server (see Figure 22-43). If the access permissions allow this operation and the connection request succeeds, the client enters an authentication negotiation. In this state, the authentication type is determined, after which the client sends a relay request. The SOCKSv5 server evaluates the request and either establishes the connection or rejects it. The client sends the following message, which contains a version identifier and method options (Figure 22-44).

ver

nmethods

methods

1

byte 1 byte 1 to 255 bytes

*Figure 22-44 SOCKSv5: Version identifier and method selection message format*

Where:

|  |  |
| --- | --- |
| **VER** | Indicates the version of SOCKS. For SOCKSv5, the value is hexadecimal X'05'. |
| **NMETHODS** | Indicates the number of the methods in the methods field. |
| **METHODS** | Indicates the supported authentication and encapsulation methods. |

The server responds by the following message (Figure 22-45).

ver

method

1

byte 1 byte

*Figure 22-45 SOCKSv5: Selected method message format*

The hexadecimal values for current standard methods are as follows:

|  |  |
| --- | --- |
| **X'00'** | No authentication required |
| **X'01'** | GSSAPI |
| **X'02'** | User name/password |
| **X'03' to X'7F'** | IANA assigned |
| **X'80' to X'FE'** | Reserved for private methods |
| **X'FF'** | No acceptable methods |

All implementations should support user name/password and GSSAPI authentication methods.

###### SOCKSv5 Connect

After authentication completes successfully, the client sends the request details. If an encapsulation method is negotiated during the method negotiation, the selected encapsulation method must be applied for the following messages. The detail request message format issued by the client is as shown in Figure 22-46.

ver

cmd

RSV

ATYP

DST ADDR

DST Port

1

byte 1 byte X'00' 1 byte variable 2 bytes

*Figure 22-46 SOCKSv5: Detail request message format*

Where:

|  |  |
| --- | --- |
| **VER** | Socks protocol version. For SOCKSv5, the value is hexadecimal X'05'. |
| **CMD** | SOCKS command in octets: |
| **X'01'** | Connect |
| **X'02'** | BIND |
| **X'03'** | UDP associate |
| **RSV** | Reserved for future use. |
| **ATYP** | Address types in octets: |
| **X'01'** | IPv4 address |
| **X'03'** | Domain-name |
| **X'04'** | IPv6 address |
| **DST.ADDR** | Desired destination address. |
| **DST.PORT** | Desired destination port in network octet order. |

An IPv4 address is stored as 4 bytes. An IPv6 address is stored as 16 bytes.

A domain name is stored as a length byte, and then a fully qualified domain name. There is no trailing null at the end of the domain name.

The server evaluates the request detail message and replies with one or more messages. Here is the reply message format issued by the server (Figure 22-47).

ver

rep

RSV

ATYP

BND.ADDR

BND.Port

1

byte 1 byte X'00' 1 byte variable 2 bytes

*Figure 22-47 SOCKSv5: Server reply message format*

Where:

|  |  |  |
| --- | --- | --- |
| **VER** | Socks protocol version. For SOCKSv5, the value is hexadecimal X'05'. | |
| **REP**  **X'00' X'01' X'02'** | Reply field:    Succeeded  General SOCKS server failure  Connection not allowed by ruleset | |
| **X'03'** | Network unreachable |
| **X'04'** | Host unreachable |
| **X'05'** | Connection refused |
| **X'06'** | TTL expired |
| **X'07'** | Command not supported |
| **X'08'** | Address type not supported |
| **X'09' to X'FF'** | Unassigned |
| **RSV** | Reserved for future use. |
| **ATYP** | Address types in octets: |
| **X'01'** | IPv4 address |
| **X'03'** | Domain name |
| **X'04'** | IPv6 address |
| **BND.ADDR** | Server bound address. |
| **BND.PORT** | Server bound port in network octet order. |

###### SOCKSv5 BIND

To accept an incoming connection from the Internet, use the same request and reply format as described earlier for SOCKSv5 Connect, setting the CMD field to BIND. However, you receive two reply packets.

The first reply contains the IP address and port number on which the SOCKS server has put a listener.

When the remote system calls into the SOCKS server, you get a second reply with the BND.ADDR and BIND.Port fields containing details of the remote server.

##### SOCKSv5 UDP connection

To be able use a UDP connection over a SOCKS server, the client first issues the UDP ASSOCIATE command to the SOCKSv5 server. The SOCKSv5 server then assigns a UDP port to which the client sends all UDP datagrams. Each UDP datagram has a UDP request header. The UDP request header format is as follows (Figure 22-48).

RSV

frag

ATYP

DST.ADDR

DST.Port

data

2

bytes 1 byte 1 byte variable 2 bytes variable

*Figure 22-48 SOCKSv5: UDP datagram request header format*

Where:

|  |  |
| --- | --- |
| **RSV** | Reserved for future use. All bytes are zero. |
| **FRAG** | Current fragment number. |
| **ATYP** | Address types in octets: |
| **X'01'** | IPv4 address |
| **X'03'** | Domain-name |
| **X'04'** | IPv6 address |
| **DST.ADDR** | Desired destination address. |
| **DST.PORT** | Desired destination port in network octet order. |
| **DATA** | User data. |

The UDP relay server gets the IP address of the client, which sends UDP datagrams to the port specified by DST.PORT. It then discards any datagram that comes from another source.

### 22.6 Secure Shell (1 and 2)

SSH can secure connections between systems. It allows application traffic, such as that generated by Telnet, FTP POP3, or even X Window System, to be both encrypted and compressed. Compression is useful over slow modem links. Implementations allow the user a choice of encryption methods.

Client software often offers both SSH1 and SSH2 support. The user is authenticated by password or public/private key.

SSH1 offers Blowfish, DES, 3DES, and RC4 encryption ciphers.

SSH2 offers 3DES, RC4, and Twofish encryption ciphers.

#### 22.6.1 SSH overview

SSH establishes a single TCP/IP connection from the client to the server. The traffic sent down this connection is encrypted, and optionally compressed using LempleZiv compression. Public/private keys can be used to verify both the user and the identity of the remote system.

##### SSH and X Window System

X Window System sessions can pass through the SSH connection. The SSH server generates a new DISPLAY variable (and xauth key) for the remote

X Window System’s clients. SSH forwards the X Window System traffic to the user’s local X Server. Users have to supply their own X Server applications; make sure it is listening on the local host.

##### SSH port forwarding

SSH offers the ability to map TCP/IP ports across systems. For example, you can configure SSH to copy data between a port on the client’s local host and the servers POP3 port. By running a POP3 client and pointing it at the local host, you establish a secure encrypted session over which to read e-mail.

### 22.7 Secure Sockets Layer (SSL)

SSL is a security protocol that was developed by Netscape Communications Corporation, along with RSA Data Security, Inc. The primary goal of the SSL protocol is to provide a private channel between communicating applications, which ensures privacy of data, authentication of the partners, and integrity.

#### 22.7.1 SSL overview

SSL provides an alternative to the standard TCP/IP socket API that has security implemented within it. Therefore, in theory, it is possible to run any TCP/IP application in a secure way without changing the application. In practice, SSL is only widely implemented for HTTP connections, but Netscape Communications Corp. has stated an intention to employ it for other application types, such as NNTP and Telnet, and there are several such implementations freely available on the Internet. IBM, for example, uses SSL to enhance security for TN3270 sessions in the IBM WebSphere Host On-Demand and eNetwork Communications Server products.

SSL is composed of two layers:

At the lower layer, a protocol for transferring data using a variety of predefined cipher and authentication combinations, called the *SSL Record Protocol*. Figure 22-49 on page 855 illustrates this and contrasts it with a standard HTTP socket connection. Note that this diagram shows SSL as providing a simple socket interface on which other applications can be layered. In reality, current implementations have the socket interface

embedded within the application and do not expose an API that other applications can use.

On the upper layer, a protocol for initial authentication and transfer of encryption keys, called the *SSL Handshake Protocol*.

API

socket

Client

Server

API

socket

**Session**

Standard HTTP

socket API

socket

API

Client

Server

socket

API

socket

API

**Session**

SSL

SSL Record Protocol

*Figure 22-49 SSL: Comparison of standard and SSL sessions*

An SSL session is initiated as follows:

1. On the client (browser), the user requests a document with a special URL that starts with https: instead of http:, either by typing it into the URL input field, or by clicking a link.
2. The client code recognizes the SSL request and establishes a connection through TCP port 443 to the SSL code on the server.
3. The client then initiates the SSL handshake phase, using the SSL Record Protocol as a carrier. At this point, there is no encryption or integrity checking built in to the connection.

The SSL protocol addresses the following security issues:

|  |  |
| --- | --- |
| **Privacy**  **Integrity** | After the symmetric key is established in the initial handshake, the messages are encrypted using this key.  Messages contain a message authentication code (MAC) ensuring the message integrity. |

**Authentication** During the handshake, the client authenticates the server using an asymmetric or public key. It can also be based on certificates.

SSL requires that each message is encrypted and decrypted and therefore has a high performance and resource cost.

##### Differences between SSL V2.0 and SSL V3.0

There is backward compatibility between SSL V2.0 and SSL V3.0. An SSL V3.0 server implementation should be able accept the connection request from an SSL V2.0 client. The main differences between SSL V2.0 and SSL V3.0 are as follows:

SSL V2.0 does not support client authentication.

SSL V3.0 supports more ciphering types in the CipherSpec.

#### 22.7.2 SSL protocol

The SSL protocol is located at the top of the transport layer. SSL is also a layered protocol itself. It simply takes the data from the application layer, reformats it, and transmits it to the transport layer. SSL handles a message as follows:

The sender performs the following tasks:

1. Takes the message from upper layer.
2. Fragments the data to manageable blocks.
3. Optionally compresses the data.
4. Applies a message authentication code (MAC).
5. Encrypts the data.
6. Transmits the result to the lower layer.

The receiver performs the following tasks:

1. Takes the data from lower layer.
2. Decrypts.
3. Verifies the data with the negotiated MAC key.
4. Decompresses the data if compression was used.
5. Reassembles the message.
6. Transmits the message to the upper layer.

An SSL session works in different states. These states are *session* and *connection* states. The SSL handshake protocol (see “SSL handshake protocol” on page 858) coordinates the states of the client and the server. In addition, there are read and write states defined to coordinate the encryption according to the change CipherSpec messages.

When either party sends a change CipherSpec message, it changes the pending write state to current write state. Again, when either party receives a change CipherSpec message, it changes the pending read state to the current read state.

The session state includes the following components:

|  |  |
| --- | --- |
| **Session identifier** | An arbitrary byte sequence chosen by the server to identify an active or resumable session state. |
| **Peer certificate** | Certificate of the peer. This field is optional; it can be empty. |
| **Compression method** | The compression algorithm. |
| **CipherSpec** | Specifies data encryption algorithm (such as null, DES) and a MAC algorithm. |
| **Master secret** | 48-byte shared secret between the client and the server. |
| **Is resumable** | A flag indicating whether the session can be used for new connections. |

The connection state includes the following components:

**Server and client random** An arbitrary byte sequence chosen by the client and server for each connection.

|  |  |
| --- | --- |
| **Server write MAC secret** | The secret used for MAC operations by the server. |
| **Client write MAC secret** | The secret used for MAC operations by the client. |
| **Server write key** | The cipher key for the server to encrypt the data and the client to decrypt the data. |
| **Client write key** | The cipher key for the client to encrypt the data and the server to decrypt the data. |
| **Initialization vectors** | Initialization vectors store the encryption information. |
| **Sequence numbers** | A sequence number indicates the number of the message transmitted since the last change  CipherSpec message. Both the client and the server maintain sequence numbers. |

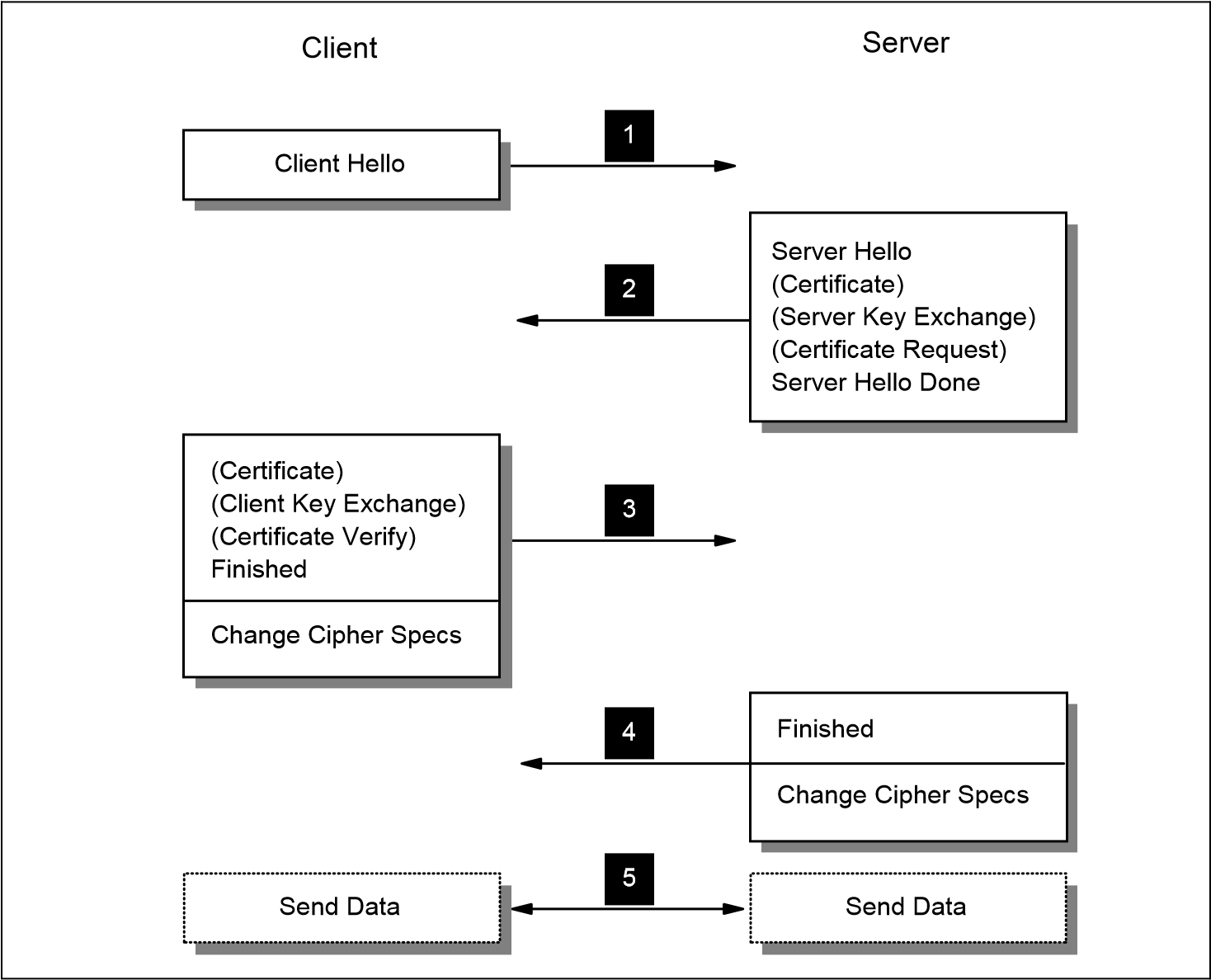
##### Change CipherSpec protocol

The change CipherSpec protocol is responsible for sending change CipherSpec

messages. At any time, the client can request to change current cryptographic parameters such as the handshake key exchange. Following the change CipherSpec notification, the client sends a handshake key exchange and if available, certificate verify messages, and the server sends a change CipherSpec message after processing the key exchange message. After that, the newly agreed keys will be used until the next change CipherSpec request. The change CipherSpec message is sent after the hello messages during the negotiation.

##### SSL handshake protocol

The SSL handshake protocol allows the client and server to determine the required parameters for an SSL connection such as protocol version, cryptographic algorithms, optional client or server authentication, and public key encryption methods to generate shared secrets. During this process, all handshake messages are forwarded to the SSL record layer to be encapsulated into special SSL messages. Figure 22-50 illustrates an SSL handshake process.



*Figure 22-50 SSL: Handshake process*

We explain the SSL handshake process detailed in Figure 22-50 in more detail:

1. The client sends a connection request with a client hello message. This message includes:
   * Desired version number.
   * Time information (the current time and date in standard UNIX 32-bit format).
   * Optionally, a session ID. If it is not specified the server will try to resume previous sessions or return an error message.
   * Cipher suites. (List of the cryptographic options supported by the client. These are authentication modes, key exchange methods, encryptions, and MAC algorithms.)
   * Compression methods supported by the client.
   * A random value.
2. The server evaluates the parameters sent by the client hello message and returns a server hello message that includes the following parameters that were selected by the server to be used for the SSL session:
   * Version number
   * Time information (the current time and date in standard UNIX 32-bit format)
   * Session ID
   * Cipher suite
   * Compression method
   * A random value

Following the server hello message, the server sends the following messages:

* + Server certificate if the server is required to be authenticated
  + A server key exchange message if there is no certificate available or the certificate is for signing only
  + A certificate request if the client is required to be authenticated

Finally, the server sends a server hello done message and begins to wait for the client response.

1. The client sends the following messages:
   * If the server has sent a certificate request, the client must send a certificate or a no certificate message.
   * If the server has sent a server key exchange message, the client sends a client key exchange message based on the public key algorithm determined with the hello messages.
   * If the client has sent a certificate, the client verifies the server certificate and sends a certificate verify message indicating the result.

The client then sends a finished message indicating the negotiation part is completed. The client also sends a change CipherSpec message to generate shared secrets. Note that this is not controlled by the handshake protocol; the change CipherSpec protocol manages this part of the operation.

1. The server sends a finished message indicating that the negotiation part is completed. The server then sends the change CipherSpec message.
2. Finally, the session partners separately generate an encryption key, in which they derive the keys to use in the encrypted session that follows from the master key. The handshake protocol changes the state to the connection state. All data taken from the application layer is transmitted as special messages to the other party.

There are significant additional processing costs associated with starting up an SSL session compared with a normal HTTP connection. The protocol avoids some of these costs by allowing the client and server to retain session key information and to resume that session without negotiating and authenticating a second time.

Following the handshake, both session partners have generated a master key. From that key, they generate other session keys, which are used in the symmetric-key encryption of the session data and in the creation of message digests. The first message encrypted in this way is the finished message from the server. If the client can interpret the finished message, it means:

Privacy has been achieved, because the message is encrypted using a symmetric-key bulk cipher (such as DES or RC4).

The message integrity is assured, because it contains a message authentication code (MAC), which is a message digest of the message itself plus material derived from the master key.

The server has been authenticated, because it was able to derive the master key from the pre-master key. Because this was sent using the server's public key, it can only be decrypted by the server (using its private key). Note that this relies on the integrity of the server's public key certificate.

##### SSL record protocol

After the master key has been determined, the client and server can use it to encrypt application data. The SSL record protocol specifies a format for these messages. In general, they include a message digest to ensure that they have not been altered and the whole message is encrypted using a symmetric cipher. Usually, this uses the RC2 or RC4 algorithm, although DES, triple-DES, and IDEA are also supported by the specification.

The U.S. National Security Agency (NSA), a department of the United States federal government, imposed restrictions on the size of the encryption key that can be used in software exported outside the U.S. These rules have been reviewed, but originally the key was limited to an effective size of 56 bits. The RC2 and RC4 algorithms achieved this by using a key in which all but 56 bits are set to a fixed value. International (export) versions of software products had this hobbled security built into them. SSL checks for mismatches between the export and nonexport versions in the negotiation phase of the handshake. For example, if a U.S. browser tries to connect with SSL to an export server, they will agree on export-strength encryption. See 22.2.7, “Export/import restrictions on cryptography” on page 793 for more information about recent changes of U.S. export regulations of cryptographic material.

### 22.8 Transport Layer Security (TLS)

The Transport Layer Security 1.0 protocol is based on SSL. The TLS 1.0 protocol is documented in RFC 2246. Two applications (without knowing each other’s code) can use TLS to communicate securely. There are no significant differences between SSL 3.0 and TLS 1.0. They can interoperate with some modifications of the message formats. A TLS 1.0 application can back down to an SSL 3.0 connection.

### 22.9 Secure Multipurpose Internet Mail Extension (S-MIME)

Secure Multipurpose Internet Mail Extension (S-MIME) can be thought of as a very specific SSL-like protocol. S-MIME is an application-level security construct, but its use is limited to protecting e-mail through encryption and digital signatures. It relies on public key technology, and uses X.509 certificates to establish the identities of the communicating parties. S-MIME can be implemented in the communicating end systems; it is not used by intermediate routers or firewalls.

### 22.10 Virtual private networks (VPNs) overview

The Internet has become a popular, low-cost backbone infrastructure. Its universal reach has led many companies to consider constructing a secure virtual private network (VPN) over the public Internet. The challenge in designing a VPN for today's global business environment will be to exploit the public Internet backbone for both intra-company and inter-company communication while still providing the security of the traditional private, self-administered corporate network.

In this chapter, we begin by defining a virtual private network (VPN) and explaining the benefits that clients can achieve from its implementation. After discussing the security considerations and planning aspects, we then describe the VPN solutions available in the market today.

#### 22.10.1 VPN introduction and benefits

With the explosive growth of the Internet, companies are beginning to ask: “How can we best exploit the Internet for our business?” Initially, companies were using the Internet to promote their company's image, products, and services by providing World Wide Web access to corporate Web sites. Today, however, the Internet potential is limitless, and the focus has shifted to e-business, using the global reach of the Internet for easy access to key business applications and data that reside in traditional IT systems. Companies can now securely, and cost-effectively, extend the reach of their applications and data across the world through the implementation of secure virtual private network (VPN) solutions.

A virtual private network (VPN) is an extension of an enterprise's private intranet across a public network such as the Internet, creating a secure private connection, essentially through a private *tunnel*. VPNs securely convey information across the Internet connecting remote users, branch offices, and business partners into an extended corporate network, as shown in Figure 22-51 on page 863. Internet service providers (ISPs) offer cost-effective access to the Internet (via direct lines or local telephone numbers), enabling companies to eliminate their current, expensive leased lines, long-distance calls, and toll-free telephone numbers.



A 1997 VPN Research Report, by Infonetics Research, Inc., estimates savings from 20% to 47% of wide area network (WAN) costs by replacing leased lines to remote sites with VPNs. And, for remote access VPNs, savings can be 60% to 80% of corporate remote access dial-up costs. Additionally, Internet access is available worldwide where other connectivity alternatives might not be available.

The technology to implement these virtual private networks, however, is just becoming standardized. Some networking vendors today are offering nonstandards-based VPN solutions that make it difficult for a company to incorporate all its employees and business partners/suppliers into an extended corporate network. However, VPN solutions based on Internet Engineering Task Force (IETF) standards will provide support for the full range of VPN scenarios with more interoperability and expansion capabilities.

The key to maximizing the value of a VPN is the ability for companies to evolve their VPNs as their business needs change and to easily upgrade to future TCP/IP technology. Vendors that support a broad range of hardware and software VPN products provide the flexibility to meet these requirements. VPN solutions today run mainly in the IPv4 environment, but it is important that they have the capability of being upgraded to IPv6 to remain interoperable with your business partner's and supplier's VPN solutions. Perhaps equally critical is the ability to work with a vendor that understands the issues of deploying a VPN. The implementation of a successful VPN involves more than technology. The vendor's networking experience plays heavily into this equation.

### 22.11 Kerberos authentication and authorization system

The Kerberos Network Authentication Service Version 5 is a *proposed standard protocol*. Its status is *elective* and described in RFC 1510.

According to *The Enlarged Devil's Dictionary*, by Ambrose Bierce, Kerberos is “the watchdog of Hades, whose duty it was to guard the entrance against whom or what does not clearly appear; Kerberos is known to have had three heads.”

A Kerberos service is normally run on its own system in a secure area. Users have to validate themselves to Kerberos before they are allowed to connect to other servers in the network. The server’s identities can also be checked against Kerberos.

The Kerberos Authentication and Authorization System is an encryption-based security system that provides mutual authentication between the users and the servers in a network environment. The assumed goals for this system are:

Authentication to prevent fraudulent requests/responses between users and servers that must be confidential and between groups of at least one user and one service.

Authorization can be implemented independently from the authentication by each service that wants to provide its own authorization system. The authorization system can assume that the authentication of a user/client is reliable.

Permits the implementation of an accounting system that is integrated, secure, and reliable, with modular attachment and support for “chargebacks” or billing purposes.

The Kerberos system is mainly used for authentication purposes, but it also provides the flexibility to add authorization information.

#### 22.11.1 Assumptions

Kerberos assumes the following:

The environment using this security system includes public and private workstations that can be located in areas with minimal physical security, a campus network without link encryption that can be composed of dispersed local networks connected by backbones or gateways, centrally operated servers in locked rooms with moderate physical security, and centrally operated servers with considerable physical security.

Confidential data or high-risk operations such as a bank transaction cannot be part of this environment without additional security, because after you have a workstation as a terminal, you can emulate certain conditions and normal data will be flowing without any encryption protection.

One of the cryptosystems used is the Data Encryption Standard (DES), which has been developed to be modular and replaceable by the Kerberos designers.

Kerberos assumes a loosely synchronized clock in the whole system, so the workstation has to have a synchronization tool such as the time server provided.

#### 22.11.2 Naming

A *principal identifier* is the name that identifies a client or a service for the Kerberos system.

In Version 4, the identifier consists of three components:

The *principal* name is unique for each client and service assigned by the Kerberos Manager.

The *instance* name used for distinct authentication is an added label for clients and services, which exist in several forms. For users, an instance can provide different identifiers for different privileges. For services, an instance usually specifies the host name of the machine that provides this service.

The *realm* name used to allow independently administered Kerberos sites. The principal name and the instance are qualified by the realm to which they belong, and are unique only within that realm. The realm is commonly the domain name.

In Version 4, each of the three components has a limit of 39 characters long. Due to conventions, the period (.) is not an acceptable character.

In Version 5, the identifier consists of two parts only, the *realm* and the *remainder*, which is a sequence of however many components are needed to name the principal. Both the realm and each component of the remainder are defined as ASN.1 (Abstract Syntax Notation One, ISO standard 8824) GeneralStrings. This puts few restrictions on the characters available for principal identifiers.

#### 22.11.3 Kerberos authentication process

In the Kerberos system, a client that wants to contact a server for its service, first has to ask for a *ticket* from a mutually trusted third party, the Kerberos Authentication Server (KAS). This ticket is obtained as a function where one of the components is a private key known only by the service and the Kerberos Authentication Server so that the service can be confident that the information on the ticket originates from Kerberos. The client is known to the KAS as a principal name (c). The private key (Kc) is the authentication key known only to the user and the Kerberos Authentication Server (KAS).

In this section, the symbol {X,Y} indicates a message containing information (or data) X and Y. {X,Y}Kz indicates that a message that contains the data X and Y has been enciphered using the key Kz.

Figure 22-52 shows the authentication process.

Client c

Kerberos

Authentication

Server (KAS)

Kerberos

Ticket

Granting

Server (TGS)

Kerberos

Database

1

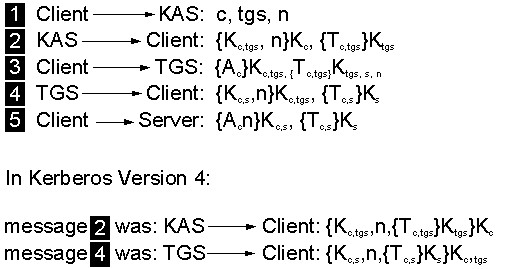
Server s

2

3

4

5



*Figure 22-52 Kerberos authentication scheme*

The authentication process consists of exchanging five messages (see Figure 22-52 on page 867):

1. Client → KAS

The client sends a message {c, tgs, n} to the KAS, containing its identity (c), a nonce (a time stamp or other means to identify this request), and requests for a ticket for use with the ticket-granting server (TGS).

1. KAS → client

The authentication server looks up the client name (c) and the service name (the ticket-granting server, tgs) in the Kerberos database and obtains an encryption key for each (Kc and Ktgs).

The KAS then forms a response to send back to the client. This response contains an initial ticket Tc,tgs, which grants the client access to the requested server (the ticket-granting server). Tc,tgs contains Kc,tgs, c, tgs, nonce, lifetime, and some other information. The KAS also generates a random encryption key Kc,tgs, called the session key. It then encrypts this ticket using the encryption key of the ticket-granting server (Ktgs). This produces what is called a *sealed ticket* {Tc,tgs}Ktgs. A message is then formed consisting of the sealed ticket and the TGS session key Kc,tgs.

|  |
| --- |
| **Note:** In Kerberos Version 4, the message is:  {Kc,tgs,n,{Tc,tgs}Ktgs}Kc  While in Kerberos Version 5, the message is of a simpler form: {Kc,tgs, n}Kc, {Tc,tgs}Ktgs  This simplifies the (unnecessary) double encryption of the ticket. |

1. Client → TGS

Upon receiving the message, the client decrypts it using its secret key Kc, which is only known to it and the KAS. It checks to see if the nonce (n) matches the specific request, and then caches the session key Kc,tgs for future communications with the TGS.

The client then sends a message to the TGS. This message contains the initial ticket {Tc,tgs}Ktgs, the server name (s), a nonce, and a new authenticator Ac containing a time stamp. Ac is {c, nonce}. The message is:

{Ac}Kc,tgs, {Tc,tgs}Ktgs, s, n

1. TGS → client

The ticket-granting server (TGS) receives the above message from the client (c), and first deciphers the sealed ticket using its TGS encryption key. (This ticket was originally sealed by the Kerberos authentication server in step 2 using the same key.) From the deciphered ticket, the TGS obtains the TGS-session-key. It uses this TGS session key to decipher the sealed authenticator. (Validity is checked by comparing the client name both in the ticket and in the authenticator, the TGS server name in the ticket, the network address that must be equal in the ticket, in the authenticator, and in the received message.)

Finally, it checks the current time in the authenticator to make certain the message is recent. This requires that all the clients and servers maintain their clocks within some prescribed tolerance. The TGS now looks up the server name from the message in the Kerberos database and obtains the encryption key (Ks) for the specified service.

The TGS forms a new random session key Kc,s for the benefit of the client (c) and the server (s), and then creates a new ticket Tc,s containing:

Kc,s, n, nonce, lifetime,

It then assembles and sends a message to the client.

|  |
| --- |
| **Note:** In Kerberos Version 4, the message is:  {Kc,s,n,{Tc,s}Ks}Kc,tgs  While in Kerberos Version 5, the message is of a simpler form: {Kc,s,n}Kc,tgs, {Tc,s}Ks  This simplifies the (unnecessary) double encryption of the ticket. |

5. Client → server

The client receives this message and deciphers it using the TGS session key that only it and the TGS share. From this message, it obtains a new session key Kc,s that it shares with the server (s) and a sealed ticket that it cannot decipher because it is enciphered using the server's secret key Ks.

The client builds an authenticator and seals it using the new session key Kc,s. At last, it sends a message containing the sealed ticket and the authenticator to the server (s) to request its service.

The server (s) receives this message and first deciphers the sealed ticket using its encryption key, which only it and KAS know. It then uses the new session key contained in the ticket to decipher the authenticator and does the same validation process that was described in step 4.

After the server has validated a client, an option exists for the client to validate the server. This prevents an intruder from impersonating the server. The client requires then that the server sends back a message containing the time stamp (from the client's authenticator, with one added to the time stamp value). This message is enciphered using the session key that was passed from the client to the server.

Let us summarize some of the central points in this scheme:

In order for the workstation to use any end server, a ticket is required. All tickets, other than the first ticket (also called the *initial ticket*), are obtained from the TGS. The first ticket is special; it is a ticket for the TGS itself and is obtained from the Kerberos authentication server.

Every ticket is associated with a session key that is assigned every time a ticket is allocated.

Tickets are reusable. Every ticket has a lifetime, typically eight hours. After a ticket has expired, you have to identify yourself to Kerberos again, entering your login name and password.

Unlike a ticket, which can be reused, a new authenticator is required every time the client initiates a new connection with a server. The authenticator carries a time stamp within it, and the authenticator expires a few minutes after it is issued. (This is the reason why clocks must be synchronized between clients and servers.)

A server maintains a history of previous client requests for which the time stamp in the authenticator is still valid. This way, a server can reject duplicate requests that might arise from a stolen ticket and authenticator.

#### 22.11.4 Kerberos database management

Kerberos needs a record of each user and service in its realm and each record keeps only the needed information, as follows:

Principal identifier (c,s)

Private key for this principal (Kc,Ks)

Date of expiration for this identity

Date of the last modification in this record

Identity of the principal that last modified this record (c,s)

Maximum lifetime of tickets to be given to this principal (lifetime)

Attributes (unused)

Implementation data (not visible externally)

The private key field is enciphered using a master key so that removing the database will not cause any problem because the master key is not in it.

The entity responsible for managing this database is the Kerberos Database Manager (KDBM). There is only one KDBM in a realm, but it is possible to have more than one Kerberos Key Distribution Server (KKDS), each one having a copy of the Kerberos database. This is done to improve availability and performance so that the user can choose one in a group of KKDSs to send its request to. The KKDS performs read-only operations, leaving the actualization to the KDBM, which copies the entire database a few times a day. This is done to simplify the operation using a Kerberos protected protocol. This protocol is basically a mutual authentication between KDBM and KKDS before a file transfer operation with checkpoints and checksum.

#### 22.11.5 Kerberos Authorization Model

The Kerberos Authentication Model permits only the service to verify the identity of the requester but it gives no information about whether the requester can use the service or not. The Kerberos Authorization Model is based on the principle that each service knows the user so that each one can maintain its own authorization information. However, the Kerberos Authentication System can be extended by information and algorithms that can be used for authorization purposes. (This is made easier in Version 5, as shown in the following section.) Kerberos can then check if a user/client is allowed to use a certain service.

Obviously, both the client and the server applications must be able to handle the Kerberos authentication process. That is, both the client and the server must be *kerberized*.

#### 22.11.6 Kerberos Version 5 enhancements

Kerberos Version 5 has a number of enhancements over Version 4. Some of the important ones are:

Use of encryption has been separated into distinct program modules which allows for supporting multiple encryption systems.

Network addresses that appear in protocol messages are now tagged with a type and length field. This allows support of multiple network protocols.

Message encoding is now described using the Abstract Syntax Notation 1 (ASN.1) syntax in accordance with ISO standards 8824 and 8825.

The Kerberos Version 5 ticket has an expanded format to support new features (for example, the inter-realm cooperation).

As mentioned in 22.11.2, “Naming” on page 865, the principal identifier naming has changed.

Inter-realm support has been enhanced.

Authorization and accounting information can now be encrypted and transmitted inside a ticket in the authorization data field. This facilitates the extension of the authentication scheme to include an authorization scheme as well.

A binding is provided for the Generic Security Service API (GSSAPI) to the Kerberos Version 5 implementation.

### 22.12 Remote access authentication protocols

Remote dial-in to the corporate intranet and to the Internet has made the remote access server a very vital part of today's internetworking services. More and more mobile users are requiring access not only to central-site resources, but to information sources on the Internet. The widespread use of the Internet and the corporate intranet has fueled the growth of remote access services and devices. There is an increasing demand for a simplified connection to corporate network resources from mobile computing devices, such as a notebook computer, or a palmtop device for e-mail access.

The emergence of remote access has caused significant development work in the area of security. The AAA (triple A) security model has evolved in the industry to address the issues of remote access security. Authentication, authorization, and accounting answers the questions who, what, and when, respectively. Here we provide a brief description of each of the three As in the AAA security model:

|  |  |
| --- | --- |
| **Authentication** | This is the action of determining who a user (or entity) is. Authentication can take many forms. Traditional authentication uses a name and a fixed password. Most computers work this way. However, fixed passwords have limitations, mainly in the area of security. Many modern authentication mechanisms utilize one-time passwords or a challenge-response query. Authentication generally takes place when the user first logs in to a machine or requests a service of it. |
| **Authorization** | This is the action of determining what a user is allowed to do. Generally, authentication precedes authorization, but again, this is not required. An authorization request might indicate that the user is not authenticated. (we do not know who they are.) In this case, it is up to the authorization agent to determine if an unauthenticated user is allowed the services in question. In current remote authentication protocols, authorization does not merely provide yes or no answers, but it can also customize the service for the particular user. |

**Accounting** This is typically the third action after authentication and authorization. But again, neither authentication nor authorization are required. Accounting is the action of recording what a user is doing and has done.

In the distributed client/server security database model, a number of communications servers, or clients, authenticate a dial-in user's identity through a single, central database, or authentication server. The authentication server stores all information about users, their passwords, and access privileges. Distributed security provides a central location for authentication data that is more secure than scattering the user information on different devices throughout a network. A single authentication server can support hundreds of communications servers, serving up to tens of thousand of users.

Communications servers can access an authentication server locally or remotely over WAN connections.

Several remote access vendors and the Internet Engineering Task Force (IETF) have been in the forefront of this remote access security effort, and the means whereby such security measures are standardized. Remote Authentication Dial In User Service (RADIUS) and Terminal Access Controller Access Control System (TACACS) are two such cooperative ventures that have evolved out of the Internet standardizing body and remote access vendors.

Remote Authentication Dial-In User Service (RADIUS) is a distributed security system developed by Livingston Enterprises. RADIUS was designed based on a previous recommendation from the IETF's Network Access Server Working Requirements Group. An IETF Working Group for RADIUS was formed in January 1996 to address the standardization of RADIUS protocol; RADIUS is now an IETF-recognized dial-in security solution (RFC 2058 and RFC 2138).

Similar to RADIUS, Terminal Access Controller Access Control System

(TACACS) is an industry standard protocol specification, RFC 1492. Similar to RADIUS, TACACS receives an authentication request from an NAS client and forwards the user name and password information to a centralized security server. The centralized server can either be a TACACS database or an external security database. Extended TACACS (XTACACS) is a version of TACACS with extensions that Cisco added to the basic TACACS protocol to support advanced features. TACACS+ is another Cisco extension that allows a separate access server (the TACACS+ server) to provide independent authentication, authorization, and accounting services.

Although RADIUS and TACACS authentication servers can be set up in a variety of ways, depending on the security scheme of the network they are serving, the basic process for authenticating a user is essentially the same. Using a modem, a remote dial-in user connects to a remote access server (also called the network access server or NAS) with a built-in analog or digital modem. After the modem connection is made, the NAS prompts the user for a name and password. The NAS then creates the so-called authentication request from the supplied data packet, which consists of information identifying the specific NAS device sending the authentication request, the port that is being used for the modem connection, and the user name and password.

For protection against eavesdropping by hackers, the NAS, acting as the RADIUS or TACACS client, encrypts the password before it sends it to the authentication server. If the primary security server cannot be reached, the security client or NAS device can route the request to an alternate server. When an authentication request is received, the authentication server validates the request and then decrypts the data packet to access the user name and password information. If the user name and password are correct, the server sends an authentication acknowledgment packet. This acknowledgement packet can include additional filters, such as information on the user's network resource requirements and authorization levels. The security server can, for instance, inform the NAS that a user needs TCP/IP or IPX using PPP, or that the user needs SLIP to connect to the network. It can include information about the specific network resource that the user is allowed to access.

To circumvent snooping in the network, the security server sends an authentication key, or signature, identifying itself to the security client. After the NAS receives this information, it enables the necessary configuration to allow the user the necessary access rights to network services and resources. If at any point in this log-in process all necessary authentication conditions are not met, the security database server sends an authentication reject message to the NAS device and the user is denied access to the network.

### 22.13 Extensible Authentication Protocol (EAP)

*Extensible Authentication Protocol* (EAP) is used for the exchange of authentication information. EAP is defined in RFC 2284 and is an extension to the Point-to-Point Protocol (PPP). EAP supports multiple authentication vehicles such as:

Kerberos

Public key authentication

Key tokens

One time passwords

EAP typically runs over the link layer and has a number of deployment solutions including:

EAP MD5

EAP-Tunneled TLS (EAP-TTLS)

Lightweight EAP (LEAP)

Protected EAP (PEAP)

When used in wireless communications, IEEE 802.1x defines how EAP is encapsulated in LAN frames. The wireless EAP solution is typically activated when a user connects to wireless access point (AP) and enters in authentication credentials. The AP verifies the identity of the user through a RADIUS server and, if the credentials are approved, access is granted to the user.

For further EAP details, refer to Chapter 23, “Port based network access control” on page 889.

### 22.14 Layer 2 Tunneling Protocol (L2TP)

L2TP permits the tunneling of PPP. Any protocol supported by PPP can be tunneled. This protocol extends the span of a PPP connection. Instead of beginning at the remote host and ending at a local ISP's point of presence (PoP), the *virtual PPP* link now extends from the remote host all the way back to the corporate gateway. L2TP tunneling is currently supported over IP/UDP. The specification is in RFC 2661.

L2TP is a consensus standard that came from the merging of two earlier tunneling protocols: Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Forwarding (L2F, described in RFC 2341). These earlier protocols did not provide as complete a solution as the L2TP protocol; one addresses tunnels created by ISPs and the other addresses tunnels created by remote hosts. L2TP supports both host-created and ISP-created tunnels.

L2TP adds the ability to create a virtual private network where multiple protocols and privately addressed IP, IPX, and AppleTalk (AT) are allowed. In addition, L2TP gives remote users the ability to connect to a local ISP and tunnel through the Internet to a home network, avoiding long distance charges. It also provides a mechanism on which to solve the multiple box PPP multilink problem. (Calls connecting to different physical routers that are destined for the same MP bundle can be tunneled to the same endpoint where MP can be terminated for all links.)

#### 22.14.1 Terminology

Before describing the protocol, we provide a definition of some L2TP terminology

L2TP access concentrator (LAC)

A device attached to one or more public switched telephone network (PSTN)

or Integrated Services Digital Network (ISDN) lines capable of handling both the PPP operation and L2TP protocol. The LAC implements the media over which L2TP operates. L2TP passes the traffic to one or more L2TP servers (LNS).

L2TP network server (LNS)

An LNS operates on any platform that can be a PPP endstation. The LNS handles the server side of the L2TP protocol. Because L2TP relies only on the single media over which L2TP tunnels arrive, the LNS can have only a single LAN or WAN interface, yet is still able to terminate calls arriving from any PPP interfaces supported by a LAC, such as async, synchronous, ISDN, V.120, and so on.

Network access servers (NAS)

A device providing temporary, on demand network access to users. This access is point-to-point using PSTN or ISDN lines.

Session (Call)

L2TP creates a session when an end-to-end PPP connection is attempted between a dial-in user and the LNS, or when an outbound call is initiated. The datagrams for the session are sent over the tunnel between the LAC and the LNS. The LNS and LAC maintain the state information for each user attached to a LAC.

Tunnel

A tunnel is defined by an LNS-LAC pair. The tunnel carries PPP datagrams between the LAC and the LNS. A single tunnel can multiplex many sessions. A control connection operating over the same tunnel controls the establishment, release, and maintenance of all sessions and of the tunnel itself.

Attribute value air (AVP)

A uniform method of encoding message types and bodies. This method maximizes the extensibility while permitting interpretability of L2TP.

#### 22.14.2 Protocol overview

Because the host and the gateway share the same PPP connection, they can take advantage of PPP's ability to transport protocols other than just IP. For example, L2TP tunnels can support remote LAN access as well as remote IP access. Figure 22-53 outlines a basic L2TP configuration.

Internet

ISP

LNS

LAC

Dial

Connection

L2TP Tunnel

PPP Connection

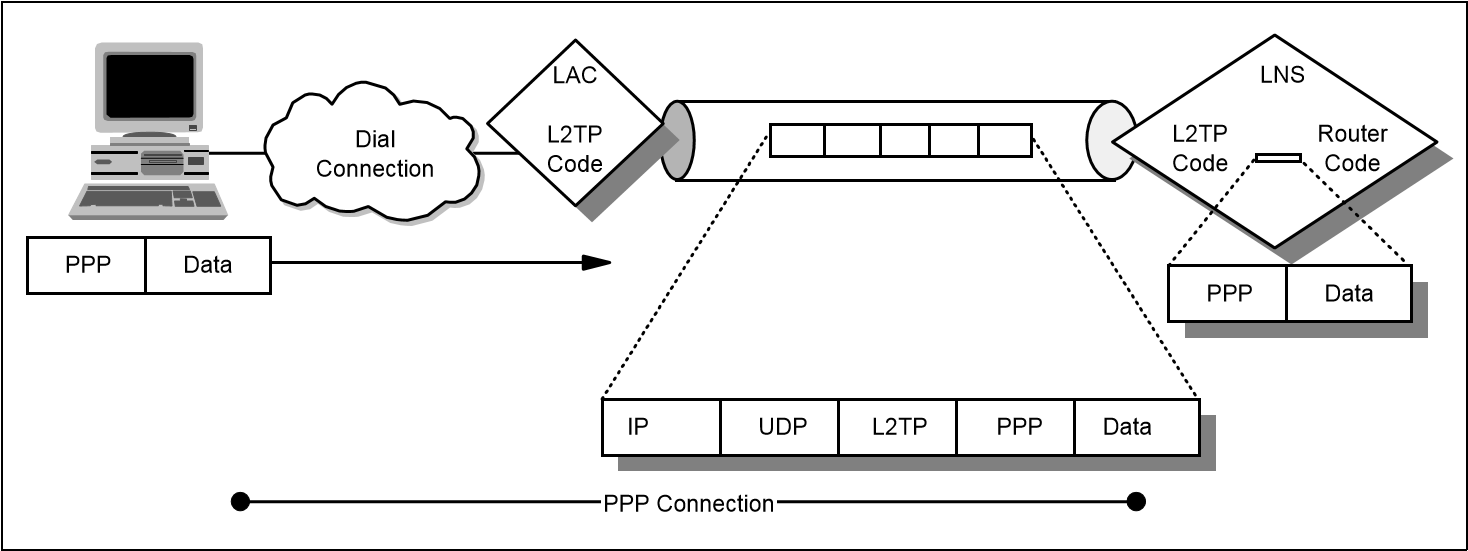
*Figure 22-53 Layer 2 Tunnel Protocol (L2TP) scenario*

Referring to Figure 22-53, the following actions occur:

1. The remote user initiates a PPP connection.
2. The NAS accepts the call.
3. The NAS identifies the remote user using an authorization server.
4. If the authorization is OK, the NAS/LAC initiates an L2TP tunnel to the desired LNS at the entry to the enterprise.
5. The LNS authenticates the remote user through its authentication server and accepts the tunnel.
6. The LNS confirms acceptance of the call and the L2TP tunnel.
7. The NAS logs the acceptance.
8. The LNS exchanges PPP negotiation with the remote user.
9. End-to-end data is now tunneled between the remote user and the LNS.

L2TP is actually another variation of an IP encapsulation protocol. As shown in Figure 22-54 on page 878, an L2TP tunnel is created by encapsulating an L2TP frame inside a UDP packet, which in turn is encapsulated inside an IP packet whose source and destination addresses define the tunnel's endpoints. Because the outer encapsulating protocol is IP, clearly IPSec protocols can be applied to

this composite IP packet, thus protecting the data that flows within the L2TP tunnel. AH, ESP, and ISAKMP/Oakley protocols can all be applied in a straightforward way.



*Figure 22-54 L2TP packet changes during transit*

L2TP can operate over UDP/IP and support the following functions:

Tunneling of single user dial-in clients

Tunneling of small routers, for example, a router with a single static route to set up based on an authenticated user's profile

Incoming calls to an LNS from a LAC

Multiple calls per tunnel

Proxy authentication for PAP and CHAP

Proxy LCP

LCP restart in the event that proxy LCP is not used at the LAC

Tunnel endpoint authentication

Hidden AVP for transmitting a proxy PAP password

Tunneling using a local realm (that is, user@realm) lookup table

Tunneling using the PPP user name lookup in the AAA subsystem (22.12,

“Remote access authentication protocols” on page 872)

UDP

IP

L2TP

PPP

Data

Data

L2

Net

L2TP

Code

IP

Code

IP Cloud

Data

L2

Net

L2TP

Code

IP

Code

*Figure 22-55 L2TP packet flow through any IP cloud*

#### 22.14.3 L2TP security issues

Although L2TP provides cost-effective access, multiprotocol transport, and remote LAN access, it does not provide cryptographically robust security features. For example:

Authentication is provided only for the identity of tunnel endpoints, but not for each individual packet that flows inside the tunnel. This can expose the tunnel to man-in-the-middle and spoofing attacks.

Without per-packet integrity, it is possible to mount denial-of-service attacks by generating bogus control messages that can terminate either the L2TP tunnel or the underlying PPP connection.

L2TP itself provides no facility to encrypt user data traffic. This can lead to embarrassing exposures when data confidentiality is an issue.

While the payload of the PPP packets can be encrypted, the PPP protocol suite does not provide mechanisms for automatic key generation or for automatic key refresh. This can lead to someone listening in on the wire to finally break that key and gain access to the data being transmitted.

Realizing these shortcomings, the PPP Extensions Working Group of the IETF considered how to remedy these shortfalls. Rather than duplicate work done

elsewhere, it was decided to recommend using IPSec within L2TP. This is described in RFC 2888.

In summary, Layer 2 Tunnel Protocols are an excellent way of providing cost-effective remote access. And when used in conjunction with IPSec, they are an excellent technique for providing secure remote access. However, without complementary use of IPSec, an L2TP tunnel alone does not furnish adequate security.

### 22.15 Secure Electronic Transaction (SET)

SET is the outcome of an agreement by MasterCard International and Visa International to cooperate on the creation of a single electronic credit card system. Prior to SET, each organization had proposed its own protocol and each had received support from a number of networking and computing companies. Now, most of the major players are behind the SET specification (for example, IBM, Microsoft, Netscape, and GTE).

The following sections describes at a high level the components and processes that make up the specification. Refer to the MasterCard and Visa home pages for more information about SET.

#### 22.15.1 SET roles

The SET specification defines several roles involved in the payment process:

|  |  |
| --- | --- |
| **The merchant** | This is any seller of goods, services, or information. |
| **The acquirer** | This is the organization that provides the credit card service and keeps the money flowing. The most widely known acquirers are MasterCard and Visa. |
| **The issuer** | This is the organization that issued the card to the purchaser in the first place. Usually, this is a bank or some other financial institution, which would know the purchaser best. |
| **The cardholder** | This is the Web surfer, who has been given a credit card by the issuer and now wants to exercise his or her purchasing power on the Web. |

##### The acquirer payment gateway

This provides an interface between the merchant and the bankcard network used by the acquirer and the issuer. It is important to remember that the bankcard network already exists. The acquirer payment gateway provides a well-defined, secure interface to that established network from the Internet. Acquirer payment gateways will be operated on behalf of the acquirers, but they might be provided by third-party organizations, such as Internet service providers (ISPs).

**The certificate authority**SET processing uses public key cryptography, so each element of the system need one or more public key certificates. Several layers of CA are described in the specification. (We discuss SET certificates in 22.15.3,

“The SET certificate scheme” on page 883.)

#### 22.15.2 SET transactions

The SET specification describes a number of transaction flows for purchasing, authentication, payment reversal, and so on. Figure 22-56 shows the transactions involved in a typical online purchase.

*Figure 22-56 Typical SET transaction sequence*

PInitReq

PInitRes

PReq

AuthReq

AuthRes

PRes

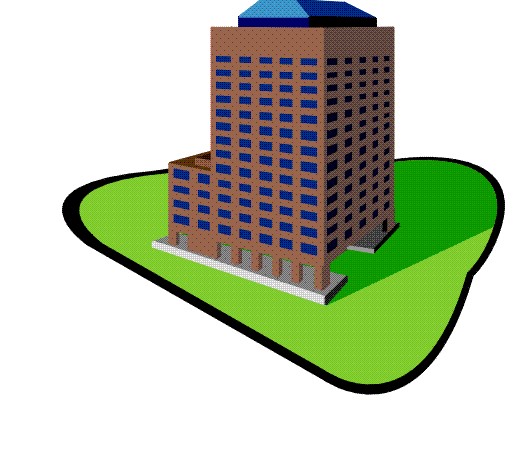
InqReq

InqRes

CapReq

CapRes

Cardholder



Merchant

*MasterCard*

*International*

*Mas*

*~~terC~~*

*ard*

Acquirer

Gateway

1

2

3

4

5

The diagram shows the following transactions (each transaction consists of a request/response pair):

1. PInit

This initializes the system, including details such as the brand of card being used and the certificates held by the cardholder. SET does not insist that cardholders have signing certificates, but it does recommend them. A cardholder certificate binds the credit card account number to the owner of a public key. If the acquirer receives a request for a given card number signed with the cardholder's public key, it knows that the request came from the real cardholder. To be precise, it knows that the request came from a computer where the cardholder's keyring was installed and available. It *could* still be a thief who had stolen the computer and cracked the keyring password.

1. Purchase order

This is the request from the cardholder to buy something. The request message is in fact two messages combined, the order instruction (OI), which is sent in the clear to the merchant, and the purchase instruction (PI), which the merchant passes on to the acquirer payment gateway. The PI is encrypted in the public key of the acquirer, so the merchant cannot read it. The merchant stores the message for later transmission to the acquirer. The PI also includes a hash of the OI, so the two messages can only be handled as a pair. Note that the card number is only placed in the PI portion of the request. This means that the merchant never has access to it, thereby preventing a fraudulent user from setting up a false store front to collect credit card information.

The purchase order has a response, which is usually sent (as shown here) after acquirer approval has been granted. However, the merchant can complete the transaction with the cardholder before authorization, in which case the cardholder would see a message that the request was accepted pending authorization.

1. Authorization

In this request, the merchant asks the acquirer, through the acquirer payment gateway, to authorize the request. The message includes a description of the purchase and the cost. It also includes the PI from the purchase order that the cardholder sent. In this way, the acquirer knows that the merchant and the cardholder both agree on what is being purchased and the amount.

When the acquirer receives the request, it uses the existing bank card network to authorize the request and sends back an appropriate response.

1. Inquiry

The cardholder might want to know how his or her request is proceeding. The SET specification provides an inquiry transaction for that purpose.

1. Capture

Up to this point, no money has changed hands. The capture request from the merchant tells the acquirer to transfer the previously authorized amount to its account.

In fact, capture can be incorporated as part of the authorization request/response (see the previous information). However, there are situations in which the merchant might want to capture the funds later. For example, most mail order operations do not debit the credit card account until the goods have been shipped.

There are several other transactions within the SET specification, but the previous summary shows the principles on which it is based.

#### 22.15.3 The SET certificate scheme

The SET specification envisions hundreds of thousands of participants worldwide. Potentially, each of these would have at least one public key

certificate. In fact, the protocol calls for an entity to have multiple certificates in some cases. For example, the acquirer payment gateways need one for signing messages and another for encryption purposes.

Key management on such a large scale requires something beyond a simple, flat certification structure. The organization of certifying authorities proposed for SET is shown in Figure 22-57.

Cardholder

CA

Cardholder

CA

Cardholder

CA

Cardholder

Cardholder

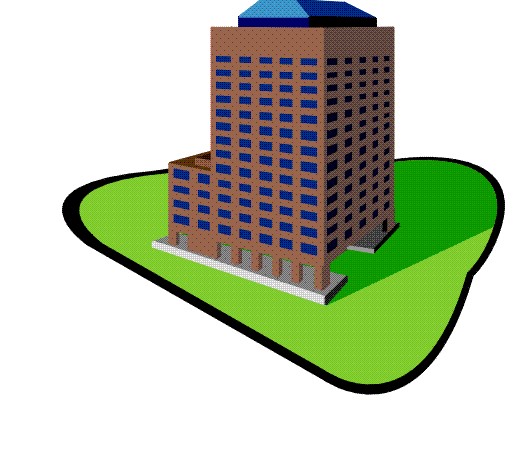
CA

Cardholder

CA

Merchant

CA



Merchant

Cardholder

CA

Cardholder

CA

Payment

CA

*ard*

*~~terC~~*

*Mas*

Acquirer

Gateway

Root

CA

Brand

CA

Geo-Political CA

optional

)

(

*Figure 22-57 SET certifying authorities*

At the top of the certificate chain, the root certifying authority is to be kept offline under extremely tight arrangements. It will only be accessed when a new credit card brand joins the SET consortium. At the next level in the hierarchy, the brand level CAs are also very secure. They are administered independently by each credit card brand.

There is some flexibility permitted under each brand for different operating policies. It would be possible to set up CAs based on region or country, for example. At the base of the CA hierarchy are the CAs that provide certificates for merchants, cardholders, and acquirer payment gateways. The SET specification provides protocols for merchants and cardholders to request certificates online. It is important to have a simple process because SET aims to encourage cardholders to have their own certificates. It envisions the cardholder surfing to the CA Web site, choosing a Request Certificate option to invoke the certificate request application on the browser, and then filling in a form to send and receive the certificate request.

Of course, if the system allows certificates to be created easily, it must also be able to revoke them easily in the event of a theft or other security breach. The SET specification includes some certificate update and revocation protocols for this purpose. Although the mechanism for requesting a certificate might be simple, there is still a need for user education. For example, it is obvious that a cardholder needs to notify the credit card company if his or her wallet is stolen, but less obvious that he or she also needs to notify them if his or her computer is stolen. However, if the computer includes his keyring file containing the private key and certificate, it might allow the thief to go shopping at the cardholder's expense.

### 22.16 RFCs relevant to this chapter

The following RFCs provide detailed information about the TCP/IP security solutions presented in this chapter:

RFC 1492 – An Access Control Protocol, Sometimes Called TACACS (July 1993)

RFC 1579 – Firewall-Friendly FTP (February 1994)

RFC 1928 – SOCKS Protocol Version 5 (March 1996)

RFC 1929 – Username/Password Authentication for SOCKS V5 (March 1996)

RFC 1961 – GSS-API Authentication Method for SOCKS Version 5 (June 1996)

RFC 2003 – IP Encapsulation within IP (October 1996)

RFC 2104 – HMAC: Keyed-Hashing for Message Authentication (February 1997)

RFC 2138 – Remote Authentication Dial In User Service (RADIUS) (April 1997)

RFC 2315 – PKCS 7: Cryptographic Message Syntax Version 1-5 (March 1998)

RFC 2403 – The Use of HMAC-MD5-96 within ESP and AH

(November 1998)

RFC 2404 – The Use of HMAC-SHA-1-96 within ESP and AH (November 1998)

RFC 2405 – The ESP DES-CBC Cipher Algorithm With Explicit IV (November 1998)

RFC 2407 – The Internet IP Security Domain of Interpretation for ISAKMP

(November 1998)

RFC 2410 – The NULL Encryption Algorithm and Its Use With IPSec

(November 1998)

RFC 2411 – IP Security Document Roadmap (November 1998)

RFC 2412 – The OAKLEY Key Determination Protocol (November 1998)

RFC 2661 – Layer Two Tunneling Protocol “L2TP” (August 1999)

RFC 2888 – Secure Remote Access with L2TP (August 2000)

RFC 2986 – PKCS #10: Certification Request Syntax Specification Version

1.7 (November 2000)

RFC 3022 – The IP Network Address Translator (NAT) (January 2001)

RFC 3162 – Radius and IPv6 (August 2001)

RFC 3174 – US Secure Hash Algorithm 1 (SHA1) (September 2001)

RFC 3207 – SMTP Service Extension for Secure SMTP over Transport Layer Security (February 2002)

RFC 3365 – Strong Security Requirements for Internet Engineering Task

Force Standard Protocols (August 2002)

RFC 3447 - Public-Key Cryptography Standards (PKCS) #1: RSA

Cryptography Specifications Version 2.1 (February 2003)

RFC 3514 – The Security Flag in the IPv4 Header (April 2003)

RFC 3586 – IP Security Policy (IPSP) Requirements (August 2003)

RFC 3686 – Using Advanced Encryption Standard (AES) Counter Mode With

IPSec Encapsulating Security Payload (ESP) (January 2004)

RFC 3711 – The Secure Real-time Transport Protocol (SRTP) (March 2004)

RFC 3715 – IPSec-Network Address Translation (NAT) Compatibility

Requirements (March 2004)

RFC 3748 – Extensible Authentication Protocol (EAP) (June 2004)

RFC 3749 – Transport Layer Security Protocol Compression Methods

(May 2004)

RFC 3750 – Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Certificate Handling (April 2004)

RFC 3751 – Secure/Multipurpose Internet Mail Extensions (S/MIME) Version

3.1 Message Specification (April 2004)

RFC 3852 – Cryptographic Message Syntax (CMS) (July 2004)

RFC 3871 – Operational Security Requirements for Large Internet Service

Provider (ISP) IP Network Infrastructure (September 2004)

RFC 4033 – DNS Security Introduction and Requirements (March 2005)

RFC 4050 – The Secure Shell (SSH) Protocol Assigned Numbers (April 2005)

RFC 4051 – The Secure Shell (SSH) Protocol Architecture (April 2005)

RFC 4052 – The Secure Shell (SSH) Authentication Protocol (April 2005)

RFC 4053 – The Secure Shell (SSH) Transport Layer Protocol (April 2005)

RFC 4054 – The Secure Shell (SSH) Connection Protocol (May 2005)

RFC 4055 – Using DNS to Securely Publish Secure Shell (SSH) Key

Fingerprints (June 2005)

RFC 4056 – Generic Message Exchange Authentication for the Secure Shell

Protocol (SSH) (June 2005)

RFC 4120 – The Kerberos Network Authentication Service (V5) (July 2005)

RFC 4301 – Security Architecture for the Internet Protocol (December 2005)

RFC 4302 – IP Authentication Header (December 2005)

RFC 4303 – IP Encapsulating Security Payload (ESP) (December 2005)

RFC 4306 – Internet Key Exchange (IKEv2) Protocol (December 2005)

RFC 4344 – The Secure Shell (SSH) Transport Layer Encryption Modes

RFC 4346 – The Transport Layer Security (TLS) Protocol Version 1.1 (April 2006)

RFC 4366 – Transport Layer Security (TLS) Extensions (April 2006)

RFC 4470 – Minimally Covering NSEC Records and DNSSEC On-line Signing (April 2006)

|  |  |  |
| --- | --- | --- |
|  | |  | | --- | | **24** | |

## Chapter 24. Availability, scalability, and load balancing

This chapter discusses the various availability, scalability, and load balancing techniques used within enterprises in an attempt to ensure continuous data flow and minimize outages.

This chapter describes the following topics:

Availability

Scalability

Load balancing

Clustering

Virtualization

Virtual Router Redundancy Protocol (VRRP)

Round-robin DNS

Alternate solutions to load balancing

© Copyright IBM Corp. 1989-2006. All rights reserved.

The Internet business has grown so rapidly that continuous availability of mission-critical data and applications residing on servers is a very important requirement for enterprises. The Internet challenges companies to develop new strategies for increasing revenue and providing detailed product and delivery information. The result raises client and business partner satisfaction. Also, the management of enterprises' internal business processes that are accessed through the Internet by the workforce must be better optimized.

Increasing demands from client, business partners, and employees for access to applications and data are challenges for the development of new server and networking strategies and services. Consider the following three main aspects:

How can availability to an enterprise's information be made available 24 hours a day and 7 days a week?

How can these services also be guaranteed even if the number of transactions increases very rapidly, for example, because of a spike in client or business partner inquiries?

How can the access to server applications and data be shared among parallel installed servers?

The answers are availability, scalability, and load balancing. In this chapter, we discuss techniques that can be employed to achieve availability, scalability, and load balancing. We discuss each technique at a fairly high level.

### 24.1 Availability

Application instances, network interfaces, and machines can fail (planned for maintenance or unplanned due to application or system error). In these cases, users must not lose their service. Recovering from application instance failure is fairly straightforward in that the application is simply restarted. Network interface failures can also be tolerated by making use of a virtual IP address, which is not tied to any particular physical interface and thus will never fail.

A *virtual IP address* can be given to a device that has one or more network interfaces. This allows the users’ machines to pick up a specific IP associated with a specific machine or device. However, the IP address given is not tied to the physical IP address of the device’s interfaces. Therefore, if one of the interfaces fails, the users are unaware of the failure.

Machine failure, however, is a bit more complex. Users must be able to immediately reconnect to the service without knowing that they now are using an alternate image of the application on another system. Users also must not be aware that the path to the other system has been automatically changed. The use of virtualization can be very advantageous with regards to increasing the availability of a system. Virtualization is discussed further later.

### 24.2 Scalability

Scalability means to provide a solution for a growing business that requires additional system capacity. When workload capacity becomes smaller due to many more new connection requests from clients or business partners, a nondisruptive growth of the current system environment must be made available.

In a traditional single system environment (no clustered systems), a nondisruptive upgrade of systems is relatively limited. In order to raise capacity, these systems have to be taken down to install new features. Therefore, they are not available for a certain time.

The implementation of clustered systems is a better approach (discussed in more depth later). Adding a new system to the cluster running equal applications instances does not impact the other systems in the cluster. This solution adds seamless capacity for a growing business. Compared to traditional systems, the user is not bound to a given system in a clustered server environment.

Therefore, the management of user connections to servers is more flexible. When a new system comes online, new connections are directed to that machine taking over a new workload.

Generic techniques to enhance scalability include clustering, virtualization, and the monitoring of devices to ensure that if certain resource thresholds are met, the resources are upgraded. We discuss clustering and virtualization in more detail later.

### 24.3 Load balancing

Assigning applications with user connections to a specific system can overload this system's capacity, while other systems with fewer connection requests to other applications might waste free capacity.

To reach the goal for an equal level of load of all systems, these systems must be organized in a clustered system group. All systems in this cluster can provide information about their workload to the load balancing device. This device will now be responsible for distributing connection requests from users to the systems of the application servers, based on workload information.

Users are not aware of such clusters. They try to connect to a service, assuming it is running in the machine of the load balancer. The load balancer forwards the connection request to the real service provider based on the current workload of all systems in the cluster. The information about the state of the workload can be provided by a function, such as a workload manager residing in every target system.

If there is no workload information from target systems, the load balancer can use distribution rules, such as:

A simple round-robin distribution

Number of distributed connections

We discuss techniques used to assist with or provide load balancing, scalability, and availability next.

### 24.4 Clustering

In order to provide the referenced availability requirement, another system organization has to be applied. This leads to running multiple application instances on multiple machines, including TCP/IP stacks with parallel connections to the TCP/IP network. This solution, called the clustering technique in general terms, is used for load balancing purposes but is also valid for solving high availability requirements.

The clustering technique dispatches connections to target servers, excluding failed servers, from a list of target servers that can receive connections. In this way, the dispatching function avoids routing connections to a server that is not capable of satisfying such a request.

The clustering technique requires the implementation of equal application instances running on different machines. If the application, the operating system with TCP/IP stack, or the machine fails, the dispatching technique immediately provides a backup.

A user requesting service from a particular server would no longer address an application in a particular server but now would address a group of servers. The connection request is now sent to the dispatcher, who decides to which available application server it is forwarded. Therefore, users are not aware to which application server (within the group) they are connected.

The clustering technique requires addresses that refer to groups of applications. This can be solved through virtual IP addresses. A virtual IP address (VIPA) is the IP address of a group of application servers, for example, a Telnet server. This VIPA is used for a connection request. The dispatcher is the receiver of the connection request from the user. It selects from a list of available servers a real server and forwards the request to this server.

The process of selecting an available application server may be extended by the dispatcher by using different kind distribution rules. The distribution of connection requests will be discussed in the load balancing section.

Another aspect of availability to consider is when the dispatcher fails. In this case, a backup dispatcher has to be implemented with the same IP address so that users can send their connection requests to the backup dispatcher. A backup dispatcher also propagates its IP address to the network. Therefore, routers use the new path that directs the user’s connection requests to the backup dispatcher.

If dispatchers maintain client/server connections, the backup dispatcher has to take over the currently running connections. A takeback process must be implemented to return running connections to the primary dispatcher.

Virtualization is also a technique used to provide availability and scalability. Virtualization has similarities to the clustering technique with regards to transparency shown to the users regarding which physical machine is being used as well as the there being no impact to the users if a machine is to fail. We discuss virtualization next.

### 24.5 Virtualization

Virtualization is the logical representation of resources not inhibited by physical

boundaries. The main objective of virtualization is to simplify the IT infrastructure. It simplifies access to resources and the management of those resources. A user accesses the required service through standard interfaces supported and maintained by the virtualized resource. The standard interfaces allows availability issues to be minimized when changes to the IT infrastructure occur.

There many types of virtualization, and we describe some in the following sections.

For additional information, refer to:

The IBM developerWorks® article “Virtualization in a nutshell: A pattern point of view” <http://www.ibm.com/developerworks/grid/library/gr-virt/>

The IBM Redpaper *Virtualization and the On Demand Business*, REDP-9115 <http://www.redbooks.ibm.com/redpapers/pdfs/redp9115.pdf>

#### *Server virtualization*

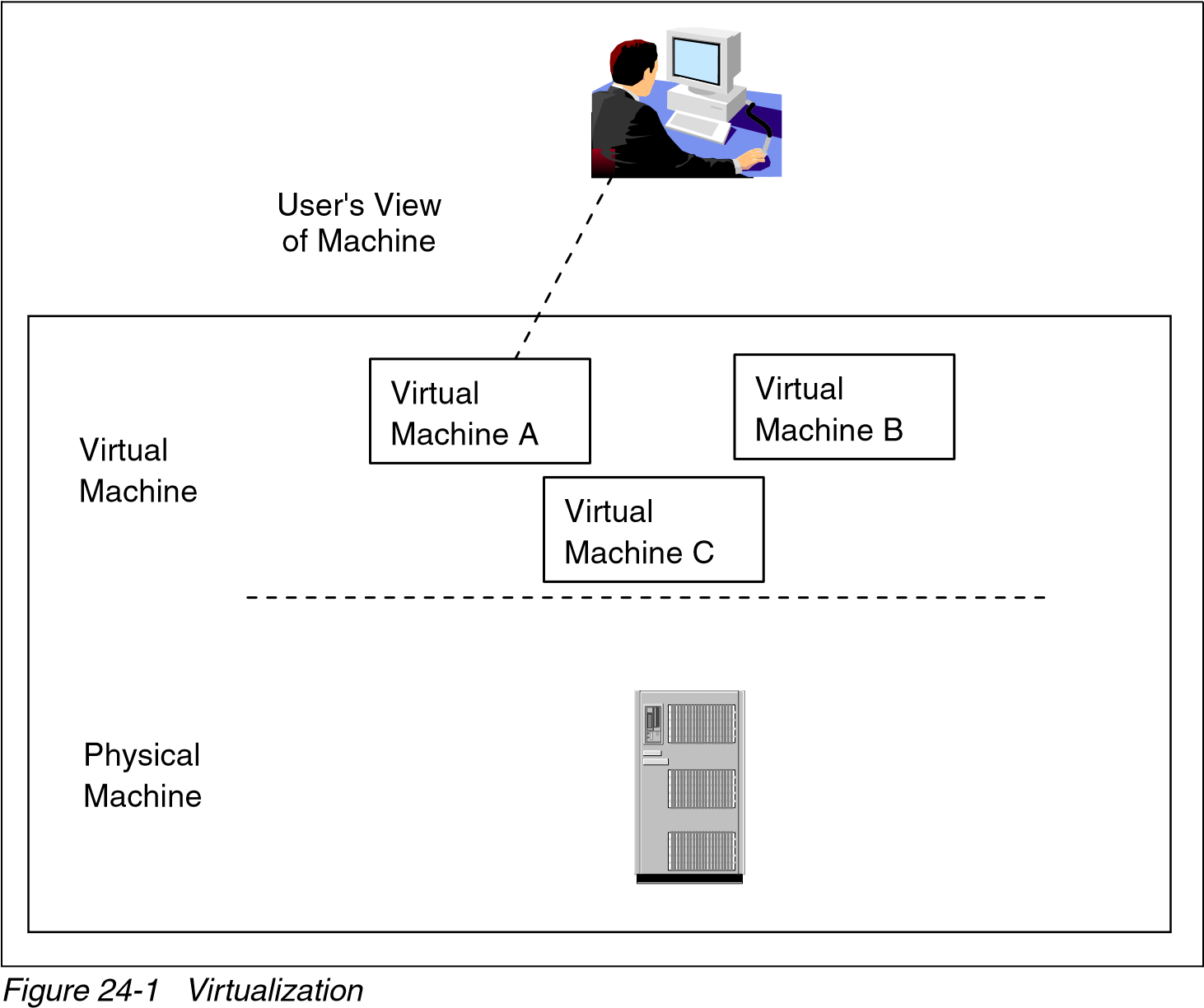
Many applications cannot be hosted on the same physical server due to resource conflicts. This creates issues regarding the number of servers deployed as well as the utilization of the existing resources. This lack of utilization is expensive, especially considering the cost of wasted storage space, server processing ability, and network utilization. Server virtualization is one way to resolve these issues.

Server virtualization is used to detach the applications from the physical configurations and limitations. Server virtualization is generally used as an IT optimization technique and has numerous benefits regarding availability and scalability.

Server virtualization provides the flexibility to dynamically change the allocation of system resources for the virtualized environments. The virtual servers can run on any of the physical machines. This means that the machine resources are fully shared. This makes it possible to run the physical server at high utilization levels. In addition, if any of the underlying physical resources need to be changed, it does not affect the virtualized servers. This enhances the level of scalability and availability associated with each virtual server.

Another aspect of availability to consider is if one of the virtual server instances fails. In such a case, it does not affect any of the other virtual servers currently residing on the same physical machine. Each instance of the virtual servers is completely isolated from each other. This also eliminates any security issues or concerns regarding data leakage. Each instance of the server is also kept as a file, which can then easily be copied onto a new virtual server if the instance fails. This assists with the time taken to recover the virtual servers and the overall availability of the service provided.

As shown in Figure 24-1, many virtual servers are running off of one physical server. This also illustrates how the users are unaware that the server being used is a virtual one as opposed to a physical one.



#### *Storage virtualization*

Storage virtualization is the combination of the capacity of multiple storage controllers into a single resource with a single view of the storage resources. This virtual layer between the physical storage devices and the users or host application provides the ability to conceal the physical infrastructure from the application and user. A benefit of storage virtualization is the ability to add, upgrade, or remove space and disks without the applications or the users service being affected.

#### *Network virtualization*

Network virtualization enables administrators to manage portions of a network that might be shared among different enterprises as virtual networks, while still

continuing to preserve the isolation of traffic and resource utilization. Network

virtualization also enables the administrator to prioritize traffic across the network

to ensure the optimum performance for vital business applications and processes. This includes technologies such as virtual private networks (VPNs), HiperSockets™, virtual networks, and virtual LANs.

### 24.6 Virtual Router Redundancy Protocol (VRRP)

Virtual Router Redundancy Protocol (VRRP) was issued to the IETF by IBM, Ascend Communications, Microsoft, and Digital Equipment Corporation in April 1998 and is documented in RFC 3768. Its status is a proposed standard.

#### 24.6.1 Introduction

The use of a statically configured default route is quite popular for host IP configurations. It minimizes configuration and processing inefficiencies on the end host and is supported by virtually every IP implementation. This mode of operation is likely where dynamic host configuration protocols (such as 3.7, “Dynamic Host Configuration Protocol (DHCP)” on page 130) are deployed, which typically provide configuration for an end host IP address and default gateway. However, this creates a single point of failure. Loss of the default router results in a catastrophic event, isolating all end hosts that are unable to detect any alternate path that may be available. Figure 24-2 illustrates VRRP.

Host

Host

Router

B

Router

Backbone

Network

Router

A

Server

Backup

Client

VRRP

*Figure 24-2 An illustration of VRRP*

VRRP is designed to eliminate the single point of failure inherent in the static, default, routed environment. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP addresses associated with a virtual router is called the master, and it forwards packets sent to these IP addresses. The election process provides dynamic fail-over in the forwarding responsibility if the master becomes unavailable. Any of the virtual router's IP addresses on a LAN can then be used as the default first hop router by end hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end host (see router discovery protocols in 3.2, “Internet Control Message Protocol (ICMP)” on page 109).

#### 24.6.2 VRRP definitions

Some terms used in VRRP are:

|  |  |
| --- | --- |
| **VRRP router** | A router running the Virtual Router Redundancy |
| **Virtual router**  **IP address owner**  **Primary IP address**  **Virtual router master**  **Virtual router backup** | Protocol. It can participate in one or more virtual routers.  An abstract object managed by VRRP that acts as a default router for hosts on a shared LAN. It consists of a virtual router identifier and a set of associated IP addresses depending on the definition, across a common LAN. A VRRP router can back up one or more virtual routers.  The VRRP router that has the virtual router's IP addresses as real interface addresses. This is the router that, when up, responds to packets addressed to one of these IP addresses for ICMP pings, TCP connections, and so on.  An IP address selected from the set of real interface addresses. One possible selection algorithm is to always select the first address. VRRP advertisements are always sent using the primary IP address as the source of the IP packet.  The VRRP router that is assuming the responsibility of forwarding packets sent to the IP addresses associated with the virtual router and answering ARP requests for these IP addresses. Note that if the IP address owner is available, it will always become the master.  The set of VRRP routers available to assume forwarding responsibility for a virtual router if the current master fails. |

#### 24.6.3 VRRP overview

VRRP specifies an election protocol to provide the virtual router function described earlier. All protocol messaging is performed using IP multicast datagrams (see Chapter 6, “IP multicast” on page 237), thus the protocol can operate over a variety of multiaccess LAN technologies supporting an IP multicast. Each VRRP virtual router has a single well-known MAC address allocated to it. The virtual router MAC address is used as the source in all periodic VRRP messages sent by the master router to enable bridge learning in an extended LAN.

A virtual router is defined by its virtual router identifier (VRID) and a set of IP addresses. A VRRP router can associate a virtual router with its real addresses on an interface and can also be configured with additional virtual router mappings and priority for virtual routers it is willing to back up. The mapping between VRID and addresses must be coordinated among all VRRP routers on a LAN. However, there is no restriction against reusing a VRID with a different address mapping on different LANs.

The scope of each virtual router is restricted to a single LAN. To minimize network traffic, only the master for each virtual router sends periodic VRRP advertisement messages. A backup router will not attempt to preempt the master unless it has higher priority. This eliminates service disruption unless a more preferred path becomes available. It is also possible to administratively prohibit all preemption attempts. The only exception is that a VRRP router will always become master of any virtual router associated with addresses it owns. If the master becomes unavailable, the highest priority backup will transition to master after a short delay, providing a controlled transition of the virtual router responsibility with minimal service interruption.

The VRRP protocol design provides rapid transition from master to backup to minimize service interruption and incorporates optimizations that reduce protocol complexity while guaranteeing controlled master transition for typical operational scenarios. The optimizations result in an election protocol with minimal runtime state requirements, minimal active protocol states, and a single message type and sender. The typical operational scenarios are defined to be two redundant routers or distinct path preferences among each router, or both. A side effect when these assumptions are violated (for example, more than two redundant paths all with equal preference) is that duplicate packets can be forwarded for a brief period during the master election. However, the typical scenario assumptions are likely to cover the vast majority of deployments, loss of the master router is infrequent, and the expected duration in master election convergence is quite small (< 1 second). Therefore, the VRRP optimizations represent significant simplifications in the protocol design while incurring an insignificant probability of brief network degradation.

#### 24.6.4 Sample configuration

Figure 24-3 shows a simple example network with two VRRP routers implementing one virtual router.

*Figure 24-3 VRRP simple configuration example*

Host-2

Host-1

Host-3

Host-4

RTR-1

VRID=1 (master)

RTR-2

VRID=1

9.180.20.4

9.180.20.3

This configuration shows a very simple VRRP scenario. In this configuration, the end hosts install a default route to the IP address of virtual router #1 (IP address 9.180.20.3) and both routers run VRRP. The router on the left becomes the master for virtual router #1 (VRID=1), and the router on the right is the backup for virtual router #1. If the router on the left fails, the other router takes over virtual router #1 and its IP addresses, and provides uninterrupted service for the hosts. Note that in this example, IP address 9.180.20.4 is not backed up by the router on the left. IP address 9.180.20.4 is only used by the router on the right as its interface address. In order to back up IP address 9.180.20.4, a second virtual router needs to be configured. This is shown in Figure 24-4.

Host-2

Host-1

Host-3

Host-4

RTR-1

VRID=1 (master)

RTR-2

VRID=1

9.180.20.4

9.180.20.3

*Figure 24-4 VRRP simple load-splitting configuration example*

Figure 24-4 on page 918 shows a configuration with two virtual routers with the hosts splitting their traffic between them. This example is expected to be very common in actual practice. In this configuration, half of the hosts install a default route to virtual router #1 (IP address of 9.180.20.3), and the other half of the hosts install a default route to virtual router #2 (IP address o f 9.180.20.4). This has the effect of load balancing the traffic from the hosts through the routers, while also providing full redundancy.

#### 24.6.5 VRRP packet format

The purpose of the VRRP packet is to communicate to all VRRP routers the priority and the state of the master router associated with the virtual router ID. VRRP packets are sent encapsulated in IP packets. They are sent to the IPv4 multicast address assigned to VRRP. The IP address, as assigned by the IANA for VRRP, is 224.0.0.18. This is a link local scope multicast address. Routers must not forward a datagram with this destination address regardless of its TTL (see 3.1, “Internet Protocol (IP)” on page 68). The TTL must be set to 255. A VRRP router receiving a packet with the TTL not equal to 255 must discard the packet. Figure 24-5 shows the VRRP packet format.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 4 8 16 24 31   |  |  |  |  |  | | --- | --- | --- | --- | --- | | vers | type | virtual router ID | priority | count IP addrs | | auth type | | advert int | checksum |  | | IP address (1) | | | | | | . . . | | | | | | authentication data (1) | | | | | | authentication data (2) | | | | | |

*Figure 24-5 VRRP packet format*

The fields of the VRRP header are defined as follows:

**Version** The version field specifies the VRRP protocol version of this packet. (In RFC 3768, the version is 2.)

**Type** The type field specifies the type of this VRRP packet. The only packet type defined in this version of the protocol is 1.

**Virtual router ID (VRID)** The virtual router identifier (VRID) field identifies the virtual router for which this packet is reporting the status.

**Priority** The priority field specifies the sending VRRP router's

priority for the virtual router. Higher values equal higher priorities. The priority value for the VRRP router that owns the IP addresses associated with the virtual router must be 255. VRRP routers backing up a virtual router must use priority values between 1-254. The default priority value for VRRP routers backing up a virtual router is 100. The priority value zero (0) has special meaning, indicating that the current master has stopped participating in VRRP. This is used to trigger backup routers to quickly transition to master without having to wait for the current master to time out.

**Count IP addrs** The number of IP addresses contained in this VRRP advertisement.

**Auth type** The authentication type field identifies the authentication method being utilized. Authentication type is unique on a per interface basis. The authentication type field is an 8-bit unsigned integer. A packet with unknown authentication type or that does not match the locally configured authentication method must be discarded. The authentication methods currently defined are: 0 - No authentication

1. - Simple text password
2. - IP authentication header

##### Advertisement interval (Adver Int)

The default is 1 second. This field can be used for

troubleshooting misconfigured routers.

**Checksum** This is used to detect data corruption in the VRRP message.

|  |  |
| --- | --- |
| **IP address(es)** | One or more IP addresses that are associated with the virtual router. |
| **Authentication data** | The authentication string is currently only used for simple text authentication. |

### 24.7 Round-robin DNS

Early solutions to address load balancing were often located at the point where host names are translated into actual IP addresses: the Domain Name System (see 12.1, “Domain Name System (DNS)” on page 426). By rotating through a table of alternate IP addresses for a specific service, some degree of load balancing is achieved. This approach is often called round-robin DNS. The advantages of this approach are that it is protocol-compliant and transparent both to the client and the destination host. Also, it is performed only once at the start of the transaction.

Unfortunately, this approach is sometimes defeated because intermediate name servers and client software (including some of the most popular browsers) cache the IP address returned by the DNS service and ignore an expressly specified time-to-live (TTL) value (see 3.1, “Internet Protocol (IP)” on page 68), particularly if the TTL is short or zero. As a result, the balancing function provided by the DNS is bypassed, because the client continues to use a cached IP address instead of resolving it again. Even if a client does not cache the IP address, basic round-robin DNS still has limitations:

It does not provide the ability to differentiate by port.

It has no awareness of the availability of the servers.

It does not take into account the workload on the servers.

RFC 1794 discusses DNS support for load balancing and mentions round-robin DNS.

### 24.8 Alternative solutions to load balancing

There are many vendors currently offering load balancing hardware or software products. The techniques used vary widely and have advantages and disadvantages.

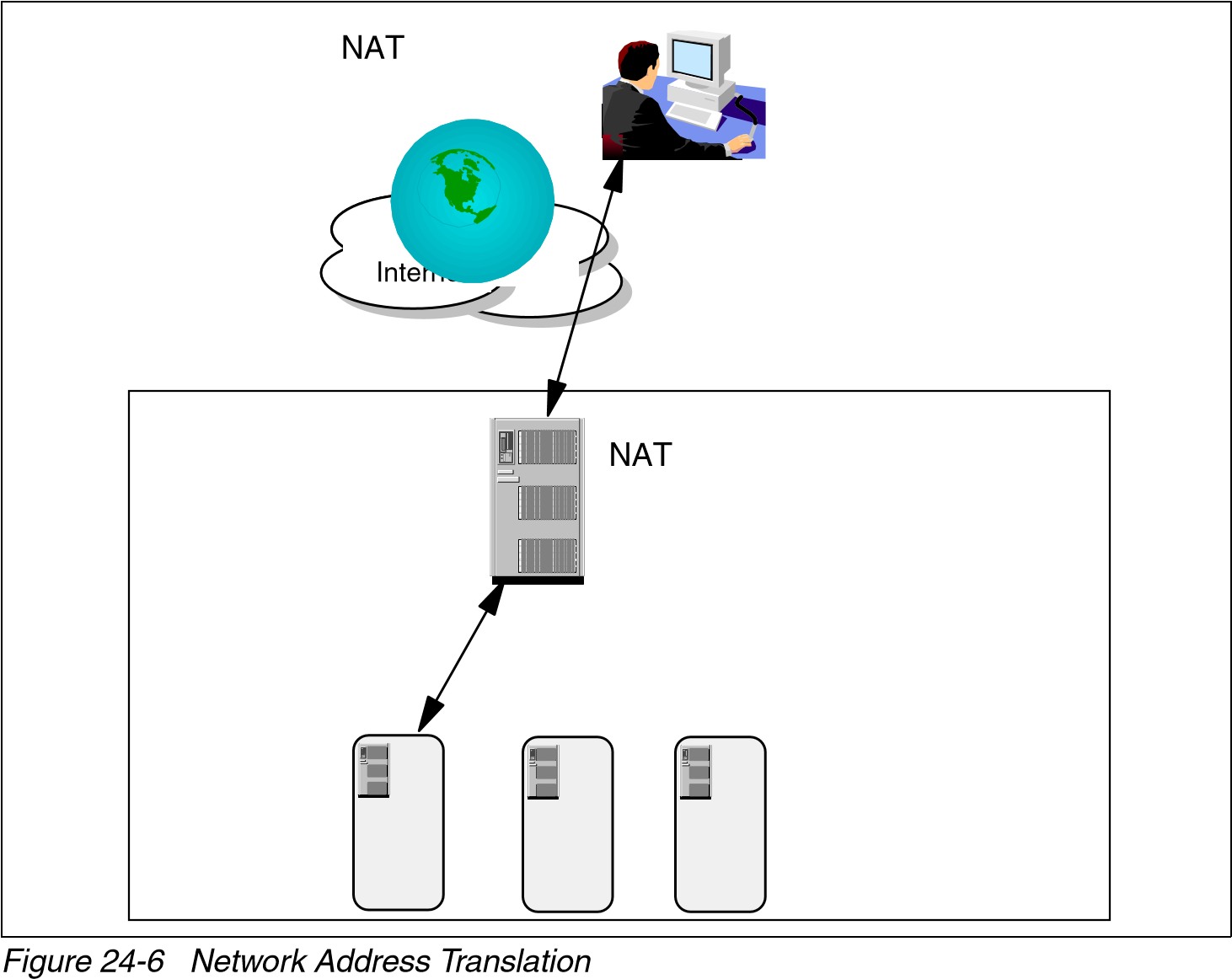
#### 24.8.1 Network Address Translation

Network Address Translation (NAT) works by modifying the source and target IP addresses in the inbound client-to-server packets and restoring the IP address to the original values in the outbound server-to-client packets. (Refer to 3.1.7,

“Network Address Translation (NAT)” on page 89.)

Note that if NAT is to be transparent to the server, eliminating the need for specialized agent code on the server, all packets sent back to the client must pass back through the load balancer in order to restore the IP addresses originally used by the client, as shown in Figure 24-6. This is a significant inefficiency, which will have a varying impact on the load balancer and the servers whose resources it manages.

This added processing charge and latency can mean network delay, and queuing delay in the load balancer itself. This drastically limits the potential scalability of NAT solutions. To overcome such delays, the capacity of the load balancer must not only be sufficient to handle both inbound and outbound packets, but also be able to cope with the disproportionately higher volume of outbound traffic.



As shown in Figure 24-6 on page 922, NAT offerings sometimes enforce the need to see both inbound and outbound requests by obliging the NAT device to be installed as a bridge (without permitting bridges of any other kind), thus forcing the servers on to what is essentially a private segment. This can complicate installation, because it requires a significant physical change to existing networks. All traffic for those servers must pass through the load balancer whether the traffic is to be load balanced or not.

The one advantage of NAT as originally conceived (the ability to forward packets to remote destinations across a wide area network) cannot be usefully deployed because the wide area network connection is behind the bridge and, therefore, can only be within the site's private network. Additionally, the same NAT device must still be the only exit from the wide area network link.

To attempt to overcome these limitations, some NAT solutions add to the overall inefficiency that is fundamental to NAT by providing add-ons. For example, the capability to map one port address to another. Refer to “Network Address Port Translation (NAPT)” on page 93.

To check if a server is up, NAT-based load balancing solutions need to sacrifice an actual client request, and so a server outage is typically perceived only as a result of a timeout of one of these real client requests.

NAT devices often only map affinity or *stickiness* based on the client's IP address, and not at the port level. This means that after a client has contacted a server, all traffic from that client that is intended for other applications is forwarded to the same server. This drastically restricts configuration flexibility, in many cases rendering the sticky capability unusable in the real world.

#### 24.8.2 Encapsulation

Another approach to load balancing is proxies that encapsulate packets rather than modifying them, and then pass them to the server. This approach has some merit, particularly because it permits the load balancer to forward traffic across a wide area network, unlike the bridging NAT solutions. But other implementations use encapsulation for all traffic, and this requires an agent of the load balancer to be installed on each server. This agent reverses the encapsulation process. As a result, the choice of server platform is, by definition, restricted to the platforms for which the server agent is available. Also, like NAT, it entails further processing of

the packet, which increases the likelihood that it will not be scalable to the levels required for major sites.

Encapsulation is discussed in further detail in RFC 1701, which appears to be updated by RFC 2784.

### 24.9 RFCs relevant to this chapter

The following RFCs provide detailed information about availability, scalability, and load balancing as presented throughout this chapter:

[RFC 1794 – DNS Support for Load Balancing (April 1995)](http://www.ietf.org/rfc/rfc1794.txt)

[RFC 3768 – Virtual Router Redundancy Protocol (VRRP) (April 2004)](http://www.ietf.org/rfc/rfc3768.txt)

[RFC 2784 – Generic Routing Encapsulation (GRE) (March 2000)](http://www.ietf.org/rfc/rfc2784.txt)

[RFC 1701 – Generic Routing Encapsulation (GRE) (October 1994)](http://www.ietf.org/rfc/rfc1701.txt)

|  |  |  |
| --- | --- | --- |
|  | |  | | --- | | **24** | |

## Appendix A. Multiprotocol Label Switching

This chapter provides an overview of the Multiprotocol Label Switching (MPLS) process and Generalized MPLS (GMPLS) architecture.

This chapter describes the following topics:

The ideas behind processing MPLS

An explanation of the differences between conventional, connectionless routing and flow routing

A definition of the terminology for MPLS concepts

A summary of the benefits of MPLS flow routing

A review of the details of MPLS protocols

An introduction to GMPLS

© Copyright IBM Corp. 1989-2006. All rights reserved.

### A.1 MPLS: An introduction

The idea behind MPLS was to emulate some property of circuit-switching network over a packet network, and to strike a happy middleground between extreme connection-oriented switching and pure connectionless routing service.

The theory for the idea of “mixing types to meet in the middle” was based on the observation that a sequence of correlated packets exist for stream and multimedia applications. We wanted to process them in the same routing path in a uniform fashion in order to guarantee quality of service (QoS). And we did not want to repeatedly examine and process those packet headers. The idea is feasible because we note that the headers in those related packets are the same or similar because those related packets in a stream desire consistent and similar processing treatment.

Multiprotocol Label Switching (MPLS) follows the same idea and comes up with new techniques to make a pseudo (and short-term) connection in a path (or subpath) for a sequence of correlated IP packets. The technology was proposed in RFC 3031. The Multiprotocol Label Switching (MPLS) standard represents the effort in the continued evolution of multilayer switching.

Generalized MPLS or GMPLS extends MPLS to encompass time-division (for example, SONET/SDH), wavelength (lambdas), and spatial switching (for example, incoming port or fiber to outgoing port or fiber). The focus of GMPLS is on the control plane of these various layers to dynamically provision resources and to provide network survivability using protection and restoration techniques.

#### A.1.1 Conventional routing versus MPLS forwarding mode

First, let us describe how the new paradigm shift might help in improving QoS performance by comparing conventional routing to the MPLS forwarding mode.

In an MPLS environment, conventional layer-3 or network-layer routing (that is, IP routing) is used to determine a path through the network. After the path is determined, data packets are then switched through each node as they traverse the network.

##### Conventional routing mode

In a traditional, connectionless network, every router runs a layer-3 routing algorithm. As a packet traverses through the network, each router along the path makes an independent forwarding decision for that packet. Using information contained in the packet header, as well as information obtained from the routing algorithm, the router chooses a “next hop” destination for the packet. In an IP network, this process involves matching the destination address stored in the IP header of each packet with the most specific route obtained from the IP routing table. This comparison process determines the next hop destination for the packet. This analysis and classification of the layer-3 header can be processor-intensive. In a traditional connectionless environment, this activity occurs at every node along the end-to-end path.

##### MPLS forwarding model

In an MPLS environment, optimum paths through the network are identified in advance. Then, as data packets enter the MPLS network, ingress devices use information in the layer-3 header to assign the packets to one of the predetermined paths. This assignment is used to append a *label* referencing the end-to-end path into the packet. The label accompanies the data packet as it traverses the network. Subsequent routers along the path use the information in the label to determine the next hop device. Because these devices only manipulate information in the label, processor-intensive analysis and classification of the layer-3 header occurs only at the ingress point.

#### A.1.2 Benefits

In additional to reducing the processing requirements on devices in the core of the network, MPLS has a number of additional advantages over conventional layer-3 routing, which we describe in the following sections.

##### Traffic engineering

Traffic engineering is the process of selecting network paths so that the resulting traffic patterns achieve a balanced utilization of resources.

Routing based on conventional Interior Gateway Protocol (IGP) algorithms might select network paths that result in unbalanced resource utilization. In these environments, some network resources are overused, while others are underused. A limited degree of engineering can be provided by manipulating the IGP metrics associated with network links. However, this effort is difficult to manage in environments with a large number of redundant paths.

To achieve the benefits of traffic engineering, MPLS can be used in-conjunction with IGP algorithms. MPLS provides the ability to specify the specific route data packets should use to traverse the network. This explicit routing of data packets ensures that a particular stream of data uses a specific path. By monitoring and managing these data streams, efficient utilization of network resources can be achieved. Explicit routing has been available through the source routing options of traditional IP routing. However, because this is a processor-intensive activity, its usage has been limited. MPLS makes the efficient use of explicit routing possible.

MPLS also provides the ability to analyze fields outside the IP packet header when determining the explicit route for a data packet. For example, the network administrator can develop traffic flow policies based on how or where a packet entered the network. In a traditional network, this information is only available at the ingress point. The additional analysis provides the administrator with a higher level of control, resulting in a more predictable level of service.

##### Quality of service routing

QoS routing is the ability to choose a route for a particular data stream so that the path provides a desired level of service. These levels of service can specify acceptable levels of bandwidth, delay, or packet loss in the network. This provides the intelligence to deliver different levels of service based on overall network policies.

Providing a network path delivering a desired QoS often requires the use of explicit routing. For example, it is straightforward to allocate a path for a particular stream requiring a specific bandwidth allocation. However, it is possible that the combined bandwidth of multiple streams may exceed existing capacity. In this scenario, individual streams, even those between the same ingress and egress nodes, might need to be individually routed. This requires a finer level of granularity than that provided by standard traffic engineering.

There are two approaches to providing QoS routing in an MPLS environment:

The MPLS label contains class of service (CoS) information. As traffic flows through the network, this information can be used to intelligently prioritize traffic at each network hop.

The MPLS network can provision multiple paths between ingress and egress devices. Each path is engineered to provide a different level of service. Traffic is then intelligently assigned to an appropriate path as it enters the network.

These approaches simply classify packets into a class of service category. Local network administration policies determine the service provided to each category.

##### Multiprotocol support

The Multiprotocol Label Switching standard provides support for existing network-layer protocols, including IPv4, IPv6, IPX, and AppleTalk. The standard also provides link layer support for Ethernet, token ring, FDDI, ATM, frame relay, and point-to-point links. Activities continue to extend this standard to other protocols and network types.

MPLS is not limited to a specific link layer technology; it can function on any media over which network layer packets can pass.

#### A.1.3 Terminology

The following sections define the terms that are used with MPLS.

##### Forwarding equivalency class (FEC)

An FEC is a group of layer-3 packets that are forwarded in the same manner. All packets in this group follow the same network path and have the same prioritization. Packets within an FEC can have different layer-3 header information. However, to simply make a forwarding decision, these packets are indistinguishable.

Common examples of FEC groups are:

A set of packets that have the same most specific route in the IP routing table.

A set of packets that have the same most specific route in the IP routing table and the same IP type of service setting.

In an MPLS network, an FEC is identified by a label.

##### Label and labeled packet

As stated previously, a label identifies a unique FEC. MPLS devices forward all identically labeled packets in the same way.

A label is locally significant between a pair of MPLS devices. It represents an agreement between the two devices describing the mapping between a label and an FEC. The fact that labels are locally significant enhances the scalability of MPLS into large environments, because the same label need not be used at every hop.

The MPLS label can be located at different positions in the data frame, depending on the layer-2 technology used for transport. If the layer-2 technology supports a label field, the MPLS label is encapsulated in the native label field. In an ATM network, the VPI/VCI fields can be used to store an MPLS label. Similarly, the DLCI field can be used to store an MPLS label in frame relay networks.

If the layer-2 technology does not natively support a label, the MPLS label resides in an encapsulation header appended specifically for this purpose. The header is located between the layer-2 header and the IP header. This use of a dedicated header permits MPLS service over any layer-2 technology (see

Figure A-1 on page 930, which depicts the 32-bit MPLS header).

TTL

CoS

Label

S

20

bits

8

bits 1 bit

3

bits

Layer 2

Header

MPLS

Header

IP

Header

Payload

*Figure A-1 The 32-bit MPLS header*

The contents of the MPLS header include:

A label field that contains the value of the MPLS label.

A CoS field that can be used to affect the queuing and discard algorithms applied to the packet as it traverses the network.

A S (stack) field that supports a hierarchical label stack.

A TTL (time-to-live) field that supports conventional IP TTL functionality.

A labeled packet is a packet into which a label has been encoded. To support enhanced MPLS functions, the packet might contain more than one label. This is known as a label stack. The stack establishes an ordered relationship between individual labels. The stack is implemented using the last-in, first-out model. This feature is further discussed in A.2.3, “Label stack and label hierarchies” on page 934.

##### Label stack router (LSR)

A label stack router is an MPLS node that is also capable of forwarding native layer-3 packets. There are two important types of LSRs in an MPLS network:

An *ingress node* connects the MPLS network with a node that does not execute MPLS functionality. The ingress node handles traffic as it enters the MPLS network.

An *egress node* connects the MPLS network with a node that does not execute MPLS functionality. The egress node handles traffic as it leaves the MPLS network.

##### Next hop label forwarding entry (NHLFE)

An NHLFE is used by an MPLS node to forward packets. There is at least one NHLFE for each FEC flowing through the node. Each node is responsible for maintaining an NHLFE information base containing the following information:

The packet’s next hop address

The operation performed on the label stack:

* Replace the label at the top of the stack with a specified new label. This is known as *popping* the old label and *pushing* a new label.
* Pop the label at the top of the stack.
* Replace the label at the top of the stack with a specified new label, and then push one or more specified new labels onto the label stack. When this action is complete, the stack will contain at least two MPLS labels.

The data link encapsulation used to transmit the packet (optional)

The label stack encoding used to transmit the packet (optional)

Any other information needed in order to properly process the packet

##### Incoming label map (ILM)

The ILM is used by an MPLS node to forward labeled packets. The label in an incoming packet is used as a reference to the ILM. The ILM information allows the node to select a set of NHLFEs containing forwarding instructions.

The ILM can map a label to a group of NHLFEs. This provides the ability to load balance over multiple equal-cost paths.

##### FEC-to-NHLFE map (FTN)

The FTN is used by an MPLS node to process packets that arrive unlabeled, but need to be labeled before forwarding. An unlabeled data packet is assigned a specific FEC at the ingress MPLS node. This FEC is used as a reference to the FTN. The FTN map allows the node to select a set of NHLFEs containing forwarding instructions. This activity is performed at the ingress node of the MPLS network.

The FTN can map a label to a group of NHLFEs. This provides the ability to load balance over multiple equal cost paths.

##### Label swapping

Label swapping is the process used by an MPLS node to forward a data packet to the next hop device. This process is used regardless of whether the packet arrives labeled or unlabeled. The process is similar to the method used in ATM and frame relay networks to forward traffic through a virtual circuit.

##### Label switched path (LSP)

An LSP represents a set of MPLS nodes traversed by packets belonging to a specific FEC. The set is an ordered, unidirectional list. Traffic flows from the node at the head-end of the list toward the node at the tail-end of the list.

##### Label stack and label hierarchies

A labeled packet can contain more than one label. The labels are maintained in a last-in, first-out stack. The stack implements an ordered hierarchy among the set of labels.

This hierarchy is used when an MPLS node delivers a packet to a partner MPLS node, but the nodes are not consecutive routers on the hop-by-hop path for the packet. In this situation, a tunnel is created between the two MPLS nodes. The tunnel is implemented as an LSP and label switching is used to forward traffic through the tunnel.

### A.2 MPLS network processing

The primary goal of MPLS is the integration of label swapping paradigms with traditional network layer routing. This integration bring efficiencies in data forwarding as well as positioning the network for advanced QoS functions.

#### A.2.1 Label swapping

Label swapping is the process used by an MPLS node to forward a data packet to the next hop device. This process is used regardless of whether the packet arrives labeled or unlabeled. The process is similar to the method used in ATM and frame relay networks to forward traffic through a virtual circuit.

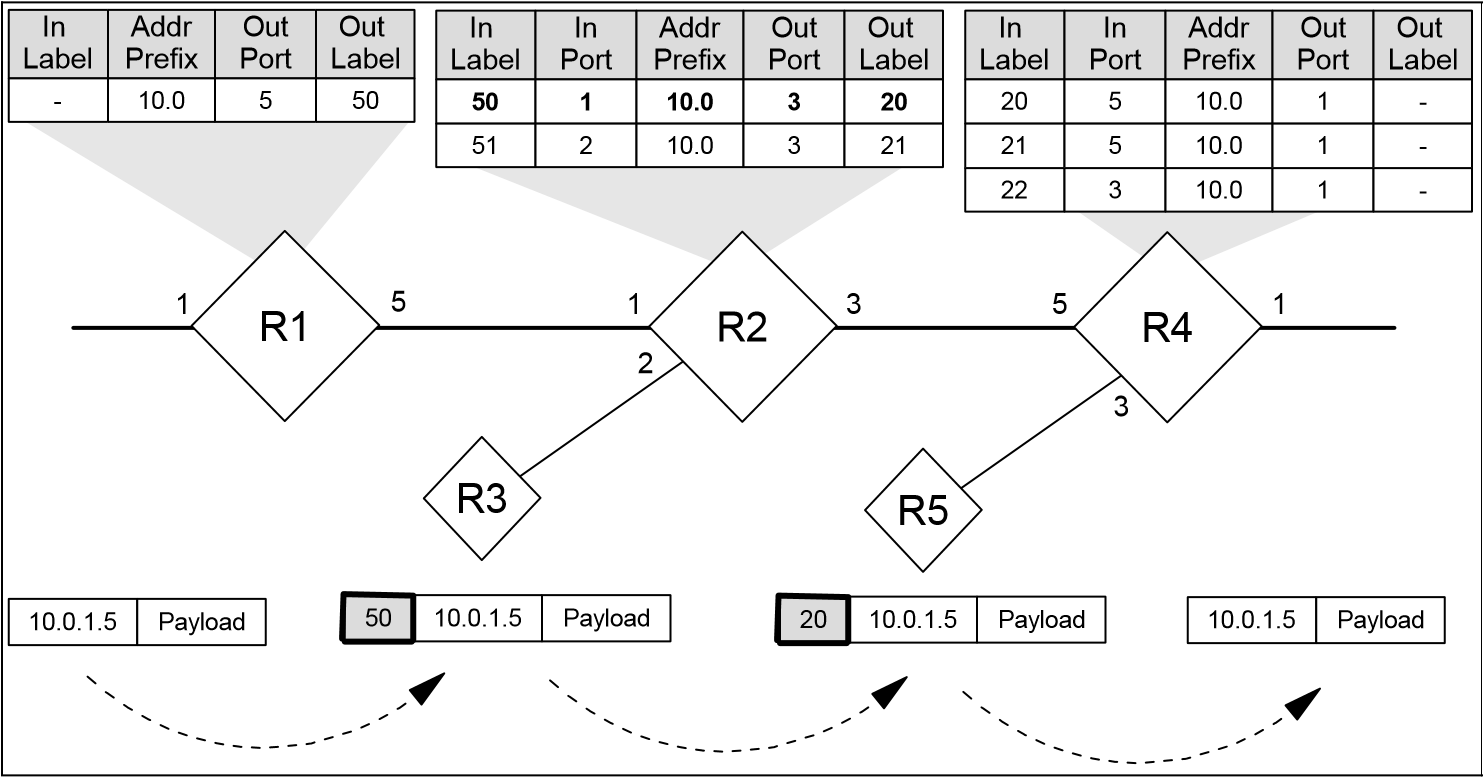
##### Forwarding a labeled packet

An MPLS node examines the label at the top of the stack of an incoming packet. It uses the ILM to map the label to an NHLFE. The NHLFE indicates where to forward the packet and the operation to perform on the label stack. Using this information, the node encodes a new label stack and forwards the resulting packet.

##### Forwarding an unlabeled packet

An MPLS node examines the network layer header and any other pertinent information required to determine an FEC. The node uses the FTN to map the FEC to an NHLFE. Processing is now identical to a labeled packet. The NHLFE indicates where to forward the packet and the operation to perform on the label stack. Using this information, the node encodes a new label stack and forwards the resulting packet.

Figure A-2 depicts label swapping in an MPLS environment.



*Figure A-2 Label swapping in an MPLS environment*

**Note:** In a label swapping environment, the next hop router is always determined from MPLS information. This might cause the packet to traverse a different path than the one obtained using conventional routing algorithms.

##### Penultimate hop popping

This is the ability to pop an MPLS label at the penultimate node rather than at the egress node. From an architectural perspective, this type of processing is permitted. The purpose of a label is to forward a packet through the network to the egress node. After the penultimate node has decided to send the packet to the egress node, the label no longer has any function. It does not need to be included in the packet.

The penultimate node pops the stack and forwards the packet based on the next hop address obtained from the NHLFE. When the egress node receives the packet, one of two activities occur:

The packet contains a label. This occurs when the penultimate node processed a packet with at least two labels. In this scenario, the label now at the top of the stack is the label the egress node needs to process to make a forwarding decision.

The packet does not contain a label. In this scenario, the LSP egress receives a standard network layer packet. The node uses the local IP routing table to make a forwarding decision.

#### A.2.2 Label switched path (LSP)

An LSP represents a set of MPLS nodes traversed by packets belonging to a specific FEC. The set is an ordered, unidirectional list. Traffic flows from the node at the head-end of the list toward the node at the tail-end of the list. The LSP for the traffic flow shown in Figure A-2 on page 933 is <R1, R2, R4>.

In an MPLS network, LSPs can be established in one of two ways:

Independent LSP control: Each LSR makes an independent decision to bind a label to an FEC. It then distributes the label to its peer nodes. This is similar to conventional IP routing; each node makes an independent decision as to how to forward a packet.

Ordered LSP control: An LSR binds a label to a particular FEC only if it is the egress LSR for that FEC, or if it has already received a label binding for that FEC from its next hop for that FEC. In an environment implementing traffic engineering policies, ordered LSP control is used to ensure that traffic in a particular FEC follows a specific path.

Section A.2.5, “Label distribution protocols” on page 938 describes the procedures used to exchange label information in an MPLS environment.

#### A.2.3 Label stack and label hierarchies

A label stack (FILO) is used in tunneling between the two MPLS nodes. The tunnel is implemented as an LSP and label switching is used to forward traffic through the tunnel.

The set of traffic sent through the tunnel constitutes an FEC. Each LSR in the tunnel must assign a label to that FEC.

To send a packet through the tunnel, the tunnel ingress node pushes a label understood by the tunnel egress node onto the label stack. The tunnel ingress node then pushes a label understood by the next hop node and forwards the data packet through the tunnel.

For example, a network might contain an LSP <R1, R2, R3, R4>. In this example, R2 and R3 are not directly connected, but are peers endpoints of an LSP tunnel. The actual sequence of LSRs traversed through the network is <R1, R2, R21, R22, R3, R4>. Figure A-3 shows this configuration.

*Figure A-3 LSP tunnels*

R1

R2

R21

R22

R3

R4

Level 1

Level 2

l

LSP Tunne

**Lb**

La

IP hdr

Payload

**Lc**

La

IP hdr

Payload

La

IP hdr

Payload

A packet traversing this network travels along a level-1 LSP: <R1, R2, R3, R4>. Then, when traveling from R2 to R3, uses a level-2 LSP: <R2, R21, R22, R3>. From the perspective of the level-1 LSP, R2’s peer devices are R1 and R3. From the level-2 perspective, R2’s peer device is R21.

Using this diagram, the following actions occur when a packet is sent through the LSP tunnel:

1. R2 receives a labeled packet from R1. The packet contains a single label. The depth of the label stack is one.
2. R2 pops this label and pushes a label understood by R3. This label is called La.
3. R2 must also include a label understood by R21. R2 pushes the label on top of the existing level-1 label. This label is called Lb. The label stack contains two entries.
4. R2 forwards the packet to R21.
5. R21 pops the level-2 label (Lb) appended by R2 and pushes a level-2 label understood by R22. This label is called Lc. R21 does not process the level-1 label. The label stack contains two entries.

1. R21 forwards the packet to R22.
2. R22 reviews the level-2 label appended by R21 and realizes it is the penultimate hop in the R2-R3 tunnel. R22 pops the level-2 label (Lc) and forwards the packet to R3. The label stack contains one entry.

#### A.2.4 MPLS stacks in a BGP environment

The network shown in Figure A-4 shows three autonomous systems. The environment contains two classes of IP routing:

Each autonomous system runs an IGP to maintain connectivity within the AS. For example, R2, R21, R22, and R3 use OSPF to maintain routes within AS 2.

Each autonomous systems runs BGP to maintain connectivity between autonomous systems. For example, border routers R1, R2, R3, and R4 use BGP to exchange inter-AS routing information.

**L3**

L1

IP hdr

Payload

AS 1

AS 2

AS 3

**L2**

L1

IP hdr

Payload

L1

IP hdr

Payload

EBGP

EBGP

IBGP

R1

IGP

R4

IGP

R21

R2

R3

R22

*Figure A-4 Connecting autonomous systems in an MPLS environment*

In this sample network, it is desirable to avoid distributing BGP-learned routes to devices which are not BGP border routers (for example, R21, R22). This minimizes the CPU processing required to maintain the IP routing table on these devices. It also eliminates the need to run a BGP routing algorithm on these devices.

An MPLS LSP stack can be used to implement this environment. In this configuration, BGP routes are distributed only to BGP peers, and not to interior

routers that lie along the hop-by-hop path between peers. LSP tunnels are configured so that:

Each peer distributes a label for each address prefix that it distributes through BGP. These labels are distributed to peers within the same AS.

The IGP maintains a host route for each BGP border router. Each interior router distributes a label for the host route to each IGP neighbor.

Consider a situation where R2 receives an unlabeled packet destined for a network connected through AS 3. The packet might have originated from a LAN segment locally connected to R2 or another LAN segment within AS 2. The packet would have been previously labeled if it had originated in AS1.

1. R2 searches the local IP forwarding table to determine the most specific route for the required destination address. The route will have be learned through BGP. The BGP next hop will be R3.
2. R3 has previously bound a label for the longest match and distributed this label to R2. This label is called L1.
3. Because all devices within AS 2 participate in the IGP, a route to R3 appears in the routing table of all devices within AS 2:
   * R22 has previously bound a label for R3 and distributed this label to R21. This label is called L2.
   * R21 has previously bound a label for R3 and distributed this label to R2. This label is called L3.
4. R2 prepares the data packet destined for AS 3 by creating a label stack. The initial entry on the stack is created by pushing the L1 label. The top entry on the stack is created by pushing the L3 label. The labeled packet is then sent to the next hop, R21.
5. R21 receives the labeled packet and reviews the top entry in the stack. Using the information in the NHLFE, R21 replaces the L3 label in the stack with the L2 label. The labeled packet is then sent to the next hop, R22.
6. R22 receives the labeled packet and reviews the top entry. Because R22 is the penultimate hop on the R2-R3 tunnel, R22 pops the L2 label on the stack and forwards the data packet to R3. The label stack now contains a single entry as it is forwarded to R3.
7. R3 receives the labeled data packet and reviews the L1 label on the stack. Using information in the NHLFE, R3 replaces the old label with a label bound by R4 and forwards the packet.

**Note:** Whenever an MPLS node pushes a label on to an already labeled packet, the new label must correspond to an FEC whose LSP egress is the node that assigned the new label.

#### A.2.5 Label distribution protocols

A label distribution protocol is a set of procedures that allows one MPLS node to distribute labels to other peer nodes. This specification is used by an LSR to notify another LSR of an assigned label and its associated meaning. This exchange establishes a common agreement between peers.

Each MPLS node participates in a local IGP to determine the network topology and populate the routing table. Label distribution protocols use this information to establish labels. After a distribution protocol has run in each node, the entire MPLS network has a complete set of paths and associated labels.

Label distribution protocols also encompass any negotiations between peers needed to learn the MPLS capabilities of each peer.

##### Types of label distribution protocols

The MPLS architecture does not specify a required distribution protocol nor does it assume there is only a single protocol. Because of this, there are a number of different standards under development. These standards can be placed into one of two categories.

###### Extensions to existing protocols

Proposals have been made to existing protocols so that label distribution information is included within existing data flows. Two examples of this are:

BGP extensions: In many cases, FECs are used to identify address prefixes distributed by BGP peers. It might be advantageous to have these same devices distribute MPLS labels. Further, the use of BGP route reflectors to distribute labels can provide significant scalability enhancements.

RSVP extensions: This proposal enhances the RSVP standard to include support for establishing and distributing LSP information. This enables the allocation of resources along the end-to-end path.

###### Development of new protocols

New protocols are also being developed with the sole purpose of distributing labels. These stand-alone protocols do not rely on the presence of specific routing protocols at every hop along the path. This is useful in situations in which an LSP must traverse nodes that do not support one of the existing protocols that has been extended to include label distribution functions.

##### Label distribution methods

There are two methods to initiate communication between MPLS nodes to exchange label information:

Downstream-on-demand: An LSR can request a label binding for a particular

FEC. The request is made to the next hop MPLS node for that FEC.

Unsolicited downstream: An LSR can distribute bindings to LSRs that have not explicitly requested the information.

Both of these distribution techniques can be used in the same network at the same time. For a given set of peers, the upstream LSR and the downstream LSR must agree on the technique to be used.

#### A.2.6 Stream merge

Stream merge is the aggregation of a large number of data flows into a single downstream flow. The device performing the merge consolidates the individual streams so that they are treated as a single stream by subsequent MPLS nodes. The merged stream is represented by a single label. After the merged packets are transmitted, any information that the packets arrived with different incoming labels is lost.

Stream merge is a major component of MPLS scalability.

### A.3 Emulating Ethernet over MPLS networks

As MPLS gaining popularity, there is a trend to carry non-IP traffic over MPLS network directly. One example is the encapsulation method for transport of Ethernet over MPLS networks.

Instead of using Ethernet cable or switch, we use MPLS as the underlying transport. The Ethernet service operates on top of the MPLS network layer as illustrated in Figure A-5 on page 940.

Emulated

Ethernet

MUX

MPLS

Emulated

Ethernet

MUX

MPLS

Physical

Packet

Tunnne

l

Etherne

t

service

*Figure A-5 Encapsulation of Ethernet over MPLS*

When emulating Ethernet over MPLS networks:

The Label Distribution Protocol (LDP) sets up a pseudo wire (as opposed to a real Ethernet cable wire, or a Ethernet switch) on MPLS.

The Ethernet pseudo wire carries the Ethernet/802.3 protocol data units (PDUs) over MPLS.

The pseudo wire emulation consists of the destination address, source address, length/type, MAC client data, and padding extracted from a MAC frame as a concatenated octet sequence in their original order.

Usually, only point-to-point Ethernet connections are emulated as the broadcast operation in a real Ethernet.

The emulation can provide multiplexing and demultiplexing at the consumer edge routers so that aggregrated traffic is between provider edge MPLS routers.

An Ethernet PW operates in one of two modes, raw mode or tagged mode:

In tagged mode, each frame *must* contain at least one 802.1Q Virtual LAN tag, a

1. Some of these protocols can be described as impractical at best. For instance, RFC 1149 (dated 1990 April 1) describes the transmission of IP datagrams by carrier pigeon and RFC 1437 (dated 1993 April 1) describes the transmission of people by electronic mail. [↑](#footnote-ref-1)
2. RFC 1771 uses uppercase to name BGP messages. The same convention is used in this section. [↑](#footnote-ref-2)
3. At the time of writing, there were 13 root servers. [↑](#footnote-ref-3)
4. Note that all of the fields are byte-aligned. The alignment of the Type field on a 4-byte boundary is for example purposes and is not required by the format. [↑](#footnote-ref-4)
5. A MIB view is a subset of the set of all instances of all object types defined according to SMI. [↑](#footnote-ref-5)
6. snmpEventID.i is an SNMPv2 manager-to-manager MIB object that shows the authoritative identification of an event. [↑](#footnote-ref-6)
7. ASN.1 BER specifies the Basic Encoding Rules for OSI Abstract Syntax Notation One, according to ISO 8825. [↑](#footnote-ref-7)