# 一、名字系统及TCP/IP名字注册和名字解析

## DNS设计目标和目的

1.创建一个全球性的、可扩展的、一致性的名字空间

2.实现本地资源本地控制

3.分布式设计以避免瓶颈

4.应用的广泛性

5.支持多个底层协议

6.硬件普适性

## 域：单个对象或基于某种共性收集齐的一个对象集合

## DNS服务器支持功能

主要功能：存储和提供（通过相应来自DNS解析器的请求）名字数据

1. 与其他服务器进行交互
2. 地区管理和传输
3. 性能增强功能
4. 管理

### DNS名字服务器负载均衡

并非只能为一个DNS域名创建一条地址RR，而是可以创建多条这样的RR。这样就可以把多个IP地址与一个名字相关联，从而可以把针对一个域名的大量请求分散到多台物理IP设备上，这种做法使得DNS能够为繁忙的因特网服务器实现负载均衡

## 名字解析服务

1.标准名字解析：接受一个DNS名字作为输入并确定其对应的IP地址

2.反向名字解析：接受一个IP地址并确定与其关联的名字

3．电子邮件解析：根据报文中使用的电子邮件地址来确定应该把电子邮件报文发送到 何处。

### 名字解析器执行的功能

1．提供用户接口

2.生成并发送查询

3.处理相应

## DNS通用主文件记录格式

1. 域名
2. TTL
3. 类
4. 类型
5. 数据

### IPv6 DNS 扩展

1. 新的RR类型AAAA(IPv6地址)
2. 新的反向解析层次结构
3. 查询类型和解析过程的改动

# 二、网络文件和资源共享协议

网络文件系统（NFS）

文件传送协议（FTP）

超文本传送协议（HTTP）

## 网络文件和资源共享以及TCP/IP NFS

### 文件和资源共享协议的组件

1. 文件系统模型和体系结构
2. 资源访问方法
3. 操作集
4. 报文传送协议
5. 管理工具

### NFS专门为实现消除本地和远程文件之间差别的目标而设计

1. 研制网络文件系统（NFS）的目的是使客户机主机能够访问本地文件那样访问远程服务器上的文件。它的主要设计目标是性能、简单和跨供应商的兼容性。
2. NFS的主要组件



1. OSI模型：开放式系统互联通信参考模型
2. 通用数据交换方法(XDR):当从设备A向设备B传输关于如何访问一个文件的信息时，设备A首先将其从设备A的内部表示转换成这些数据类型的XDR表示，信息使用XDR编码跨越网络进行传输，然后设备B将其从XDR转换成自己的内部表示。
3. 使用XDR就可以在设备之间交换数据而不需要考虑每台设备使用了什么样的内部文件系统。这令NFS可以在客户机和服务器之间交换文件数据，这些客户机和服务器可能是使用完全不同的硬件和软件平台实现的。

#### 使用远程过程调用（RPC）的NFS客户机/服务器操作

##### RPC操作与运输协议用法

NFS 没有像其他大多数协议 那样采用专用报文格式。相反，客户和服务器使用RPC协议来交换文件操作请求和数据。

##### NFS中客户机和服务器的职责

NFS服务器被设计成无状态的，简言之，这意味着NFP服务器不会从一个请求到另一个请求地跟踪记录使用自己的客户机的状态。

##### 客户机和服务器高速缓存

NFS被设计成一种无状态协议，使用智能客户机和相对较哑的服务器，服务器只对请求做出相应，不维护有关那些文件正在使用的状态信息。为提高效率起见，NFS最初设计成使用UDP作为运输协议。这要求由NFS客户机负责检测丢失请求并进行重传。为能够利用TCP的可靠性和其他特色，NFSv4使用了TCP

#### NFS服务器过程和操作

#### NFS文件系统模型与装配协议

##### NFS文件系统模型

一种层次结构式的目录组织形式，目录中又包含文件和子目录。层次结构的顶端是根，根下面可以包含任意数量的文件和第一级目录，每一个目录都可以包含更多文件或其他目录，从而可以创建出任意的树状结构。

##### 装配协议

NFS版本2和版本3中没有包含用来打开或关闭某台远程服务器上的资源的过程。在这两个版本里，当NFS任务能够成功完成之前，首先必须利用专门的装配协议来装配一个文件系统，并创建一个文件句柄以便在句柄上访问中国文件，当文件系统不需要时装配协议也被用来装配一个文件系统，装配协议的实现方法与NFS自己的实现方法相似。定义了一系列使用RPC的XDR的过程。在NFSv4中装配协议已经不再需要，因为它所执行的任务已经作为NFSv4操作实现了。

# 三、主机配置与TCP/IP主机配置协议

## 主机配置概念、问题和动机

### 主机配置的目的

在TCP/IP网络中，必须为每台设备分配一个IP地址。除此之外，对一个TCP/IP网络来说，我们可能希望被告知每台主机下面的一些参数：

1. 本地网络上默认路由器的地址
2. 主机应该使用的网络掩码
3. 为主机提供特定服务的服务器的地址，例如邮件服务器或域名系统（DNS）名字服务器
4. 本地网络的最大传输单元（MTU）
5. 应该给IP数据报使用什么样的寿命（TTL，TIME TO LIVE）值

### 主机人工配置存在的问题

1. 远程配置
2. 移动设备配置
3. 哑主机配置
4. 地址共享

### 使配置过程自动化：主机配置协议

主机配置协议使管理员能够将主机设置为由主机自动确定自己的地址和其他的一些重要参数。主机配置协议之所以有用不仅因为他们节省了人工配置所需要的大量工作，而且因为它们支持远程设备、无存储设备或移动设备的自动设置。

### 主机配置协议在TCP/IP中起的作用

主机配置驻留在高层的有点：

1. 协议的操作不依赖于其上运行的硬件，从而令协议更为通用。
2. 能够在网络之间传送主机配置报文，而使用一个运行在本地网络上的低层协议则不可能做到这一点

## TCP/IP引导协议（BOOTP）

BOOTP是动态主机配置协议（DHCP）的前身。

### BOOTP概述、历史和标准

#### BOOTP：客服RARP的缺陷

反向地址解析协议（RARP）是第一个试图解决这种引导问题的尝试。

RARP能够向一台无盘设备提供其IP地址

RARP的困难在于它有太多的局限，它使用硬件广播方式运行在相当低的层次，因此他要求调整以适应不同的硬件类型。

BOOTP用来客服RARP的确定：

1. BOOTP仍基于客户机/服务器交换模式，只是作为一种高层软件协议实现，采用用户数据包协议（UDP）进行报文传输。它不像RARP那样依赖于特定的网络硬件。
2. 除了IP地址之外它还支持向客户机发送额外的配置信息，额外信息通畅可以放在一个报文中发送以提高效率。
3. 它能够处理客户机和服务器位于同一个互联网络的不同网络的情况。这使得对提供IP地址的服务器的管理能够更加集中，节省了费用同时也节省了管理时间和麻烦。

首个广泛应用于TCP/IP网络的主机配置协议是引导协议（BOOTP）。该协议专门设计用来客服PAPR的诸多缺点，支持主机配置。BOOTP计划在无存储器设备两阶段引导过程中的第一个阶段中使用，在利用BOOTP获得IP地址和其他配置参数以后，设备江勇诸如TFTP这样的协议来下载为在网络上工作所必须的软件。

#### BOOTP的修改与DHCP的研发

BOOTP的最重要的一个缺点是缺少对动态地址分配的支持。

20世纪90年代后期对动态地址分配的需求显著提高促成了动态主机配置协议（DHCP）的研发。

### BOOTP客户机/服务器报文传递和寻址

#### BOOTP报文传递和传输

BOOTP报文传递使用UDP作为自己的第四层传输协议，有以下两条原因：

1. UDP比另一个第四层运输协议即传输控制协议（TCP）要简单的多，特别适用于像BOOTP这样的简单请求/应答协议
2. 由于客户机显然不知道BOOTP服务器的地址，所以请求是在其本地网络上传播出去的。UDP支持广播，TCP则不然。

#### 丢失报文的重传

使用UDP传递BOOTP报文带来了简单性的好处，但缺点是UDP不可靠，这意味着BOOTP请求在到达服务器之前可能会丢失，或者服务器的相应可能无法返回客户机。

BOOTP使用不提供可靠特性的UDP作为传输协议，为此，BOOTP客户机必须检测自己的请求何时丢失并在必要时重传请求。

### BOOTP详细操作

#### BOOTP引导过程

1. 客户机创建请求
2. 客户机发送请求
3. 服务器收到请求对其进行处理
4. 服务器创建回答
5. 服务器发送回答
6. 客户机处理回答
7. 客户机完成引导过程

## DHCP概述与地址分配概念

DHCP包含了两种主要组件，一种是地址分配机制，另一种是允许客户机请求配置信息而服务器提供此信息的协议。DHCP以一种与BOOTP相似但又有所改进的方式实现了这两种功能。

### DHCP特色的概述

DHCP支持动态地址分配，DHCP不是使用一个将硬件地址映射到IP地址的静态表，而是使用一个IP地址池来动态分配地址。动态寻址使IP地址更有效地分配，设置可以在多个设备间共享，同时，在需要时，DHCP仍支持设备的地址的静态映射。

**要点：**DHCP是当前用于现代TCP/IP网络上的主机配置协议，它基于BOOTP，与其在许多方面相似，包括请求/回答报文交换的使用和几乎完全相同的报文格式。但是DHCP还包含了增加的功能，其中最值得注意的是动态地址分配，他允许从一个由DHCP服务器管理的共享池中给客户机分配IP地址。

### DHCP地址指派与分配机制

#### DHCP地址分配

向客户机提供IP地址是主机配置协议最基本的配置任务，DHCP标准包含了三种地址配置机制：人工、自动、和动态

#### DHCP动态分配的优点

1. 自动操作
2. 集中管理
3. 地址重用和贡献
4. 便携通用
5. 避免冲突

#### DHCP自动分配

自动分配可以看成动态分配的特例，它本质上就是客户机使用IP地址的期限（租用长度）为永远的动态分配。

**要点**：

DHCP定义了三种基本的地址分配机制。动态分配最常用的方法，它使每个客户机都从DHCP服务器租用了一个地址，并保持一段时间。服务器从共享的地址池中动态选择地址。自动分配和动态分配相似，只不过地址是永久分配而不是租用的。人工分配就和BOOTP一样，将一个地址预分配给一个特定的设备，通常只用于服务器和其他固定的重要主机。

DHCP中服务器拥有地址池中所有地址，每个客户机从服务器中租用一个地址，通常只能租用一段有限时间。

### DHCP生命周期

DHCP遵循一个租用生命周期，它通常包含以下6个阶段

1. 分配
2. 重分配
3. 正常操作
4. 更新
5. 重绑定
6. 释放

### DHCP租用地址池、范围以及地址管理

#### 地址池长度的选择

1. 客户机的数量
2. 客户机的使用情况
3. 过分配的后果

#### 租用地址范围

每个DHCP服务器维护一个地址集合，用来给客户机分配租用。它们通常是由管理员分配给服务器的连续地址块，被称为DHCP地址范围。

## DHCP配置与操作

### DHCP服务器职责

1. 地址储存与管理
2. 配置参数的存储与管理
3. 租用管理
4. 响应客户机请求
5. 管理服务

### DHCP客户机职责

1. 发起配置
2. 配置参数的管理
3. 租用管理
4. 报文重传

### DHCP租用分配、重分配和更新

#### 初始的租用分配过程

1. 客户机创建DHCPDISCOVER报文:

它自己的硬件地址，位于报文的CHAddr字段，用于标识自身。

随机的事物标识符，位于XDI字段（用于标识后继报文是同一事务的一部分）

1. 客户机发送DHCPDISCOVER报文。
2. 服务器接收并处理DHCPDISCOVER报文
3. 服务器创建DHCPOFFER报文：

分配给客户机的IP地址，位于YIAddr字段

提供的租用长度

客户机特定的配置参数

返回送给所有客户机或该客户机所在类别的通用配置参数

服务器标识符，位于DHCP服务器标识符选项

与DHCPDISCOVER报文中相同的事务标识

1. 服务器探测并/或保留提供的地址（可选）
2. 服务器发送DHCPOFFER报文
3. 客户机接收并处理DHCPOFFER报文
4. 客户机创建DHCPREQUEST报文：

被选定服务器的标识符，位于DHCP服务器标识符选项，使每个服务器都知道选中谁了。

DHCP服务器在DHCPOFFER报文中分配给客户机的IP地址，客户机将它放在请求IP地址DHCP选项中作为确认。

任何它希望的额外配置信息，位于报文的参数请求列表选项

1. 客户机发送DHCPREQUEST报文。
2. 服务器接收并处理DHCPREQUEST报文。
3. 客户机接收并处理DHCPACK或DHCPNAK报文。
4. 客户机检查该地址是否未被使用。
5. 客户机完成租用分配。

### 非DHCP地址的客户机参数配置过程

1. 客户机创建DHCPINFORM报文
2. 客户机发送DHCPINFORM报文
3. 服务器接收并处理DHCPINFORM报文
4. 服务器生成DHCPACK报文
5. 服务器发送DHCPACK报文
6. 客户机接收并处理DHCPACK报文

**要点**：不适用DHCP获取IP地址的设备仍然可以使用DHCP的其他配置能力，客户机能够广播DHCPINFOM报文。以请求任何一个可用的服务器向他发送参数，以便它可以使用该网络。DHCP服务器将请求的参数和/或默认参数放在DHCPINFORM报文的DHCP选项中返回给客户机。

## DHCP报文传递、报文类型和格式

### 报文传输

**要点**：来自BOOTP客户机的请求通常以广播方式发送，以到达任何可用的DHCP服务器。但是也有例外，比如租用更新时，请求会直接发送到已知服务器。DHCP可以以广播方式把它们的回答发送到DHCP客户机保留的特定端口号，或者以单播方式通过第2层交付。DHCP标准规定要尽可能使用第2层交付，以避免不必要的广播流量。

### 丢失报文的重传

类似于BOOTP，DHCP也使用了UDP传输，这种 不提供任何可靠性特征。当发送了请求但没有收到相应时，DHCP客户机必须察觉到，并定期重传请求。在网络环境不好的情况下，必须使用特殊的逻辑以防发送过多的请求。

## DHCP客户机/服务器的实现、特性和IPv6支持

### DHCP自配置/自动专用IP寻址（APIPA）

客户机可能无法获得租用，或者重启后不能重新得到租用，也可能无法更新已有的租用。下面几种原因可能会导致这种情况的发生：

1. DHCP服务器可能出现了故障或者离线维护
2. 客户机本地网络上的中继代理出现了故障
3. 其他硬件故障或者电源问题导致无法通信
4. 网络耗尽了可分配的地址

### APIPA操作

任何DHCP租用过程失败时，APIPA从专用地址块中随机选择一个地址，而不是直接停下来发送一条差错报文。（它的地址范围是 B 类地址块169.254.0.0~169.254.255.255）

### APIPA的限制

具有专用IP地址存在的所有限制，包括不能再英特网上使用这些地址。而且APIPA不能提供客户机需要从DHCP服务器获得的其他配置参数，最后APIPA不能喝代理APR一起工作，因为代理对所有的专用地址都会相应，这样他们看起来似乎都被占用了。

### DHCP安全性担忧

1. 未授权的DHCP服务器
2. 未授权的DHCP客户机

### IPv6中两种自配置方法

1. 无状态自配置：一种允许主机配置自身而不需要任何其他设备帮助的方法
2. 状态自配置：一种由服务器给客户机提供配置信息的技术

# 四、TCP/IP网络管理框架和协议

## TCP/IP英特网标准管理框架概述

简单网络管理协议（Simple Network Management Protocol,SNMP）

### SNMP的设计目标

简单网络管理协议（SNMP）定义了一套允许网络管理员远端监视和操作TCP/IP网络设备的技术。术语SNMP不仅指一个具体的通信协议（有时成为SNMP协议），而且指英特网管理的整个框架（SNMP框架）

### SNMP设备类型

SNMP包含的总体思想是允许网络管理需要的信息通过TCP/IP进行交换。定义了两种不同基本类型的硬件设备：

**被管节点**：网络中那些装配了软件以允许通过SNMP来管理他们的常规节点。通常来说，这些是常规的TCP/IP设备。他们有时也被称为被管节点。

**网络管理站**：（NMS）运行特殊的软件来管理上面提到的常规被管节点的指定的网络设备。网络中必须存在一个或多个NMS，因为这些是真正运行的SNMP的设备

### SNMP实体

1. 被管理节点实体：

SNMP代理：是指一个实现SNMP协议，运行被管节点为NMS提供信息并从NMS哪里获得指令的软件程序

SNMP管理信息库（MIB）：MIB定义了存储的有关节点为NMS提供信息并从NMS那里获得指令的软件程序。

1. 网络管理站实体

一个NMS的SNMP实体由以下部分组成：

SNMP管理者：实现SNMP协议的软件程序，他允许NMS从被管节点收集信息，并向它们发送指令

SNMP应用程序：允许网络管理员使用SNMP来管理网络的一个或多个管理程序。

### TCP/IP因特网标准管理框架的体系结构和协议组件

#### SNMP框架组件

1. 管理信息结构
2. 管理信息库（MIB）
3. 简单网络管理协议（SNMP）
4. 安全性和管理

## TCP/IP SMI和MIB

### TCP/IP SMI和MIB概述

#### SNMP的面向信息设计

不像大多数面向命令的协议，SNMP是面向信息的。SNMP操作。SNMP操作是通过使用被管设备维护的称为变量的对象来实现的。网络管理站通过读变量来检测设备的状态。通过改变（写）变量来控制设备的操作，而不是发出命令。

#### MIB和MIB对象

被管设备中的管理数据变量是在一个称为管理信息库（MIB）的逻辑集合中加以维护的。MIB中的对象通常称为MIB对象，它们通常被收集到一个称为MIB模块的集合中。

#### 定义MIB对象：SMI

管理信息结构（SMI）标准是负责定义MIB对象构造、描述和组织的规则。通过确保对所有管理信息使用通用数据描述，SMI允许不相似的设备通信。

### TCP/IP SNMP的概念的操作

SNMP框架的第三个主要部分是实际的简单网络管理协议（SNMP），它主要负责在设备之间传送管理信息。

SNMP报文由一组包装数据元素（称为协议数据单元或PDU）的字段组成。在有些情况下，尽管术语报文和PDU在技术上是不一样的，它们可以互换使用，SNMP的PUD根据它们的功能而被分为不同类别。

### SNMP协议操作

#### 使用GetRequest和（Get）Response报文的基本请求/响应信息轮询

1. SNMP管理者创建GetRequest-PDU
2. SNMP管理者发送GetRequest-PDU
3. SNMP代理接收并处理GetRequest-PDU
4. SNMP代理创建Response-PDU
5. SNMP代理发送Response-PDU
6. SNMP管理者处理Response-PDU

在SNMP，通信最基本类型是信息轮询，它允许NMS使用一个简单的请求/回答报文交换从被管节点读一个或多个MIB对象。

# 五、/IP应用层寻址和应用程序分类

统一资源标识符（URI）：包括统一资源定位符（URL）和统一资源名（URN）

## TCP/IP应用层寻址：URI、URL和URN

### URL概述和标准

#### URI的类别：URL和URN

统一资源定位符（URL）：URL是通过将协议或访问机制与具体的资源位置想结合来引用资源的一种URI。URL由用于访问资源的协议名开始，包含足够的信息以指出如何获得该资源。

统一资源名（URN）：URN也是一种URI，它提供了一种唯一命名资源而不需要指定访问协议或机制的方法，它不要指定一个特定的位置。

URL和URN的区别在于前者更具体，是面向如何访问资源的，而后者更抽象，被更多地用来标识资源是什么而不是如何获得它。

任何互联网都需要某种机制以允许标识和访问资源（如文件、目录和程序）。在TCP/IP中，URI用于这种“应用层寻址”。URI的两种类型是URL和URN，URL指定如何使用访问方法和位置相结合来访问一个对象，URN通过名字来标识一个对象，但不知处如何访问它。

#### URL的通用语法

URL是最广泛使用的URI类型。