

YD

中华人民共和国通信行业标准

YD/T 1358-2005

路由器设备安全技术要求 ——中低端路由器(基于 IPv4)

Security requirements of medium-end and low-end router

2005-06-21 发布

2005-11-01 实施

中华人民共和国信息产业部 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 符号和缩略语	3
5 概述	5
6 数据转发平面安全	6
6.1 安全威胁	6
6.2 安全功能	6
7 控制平面安全	8
7.1 安全威胁	8
7.2 安全功能	8
8 管理平面安全	11
8.1 安全威胁	11
8.2 安全功能	11
附录 A (资料性附录) 硬件系统和操作系统的安全要求	14
参考文献	15

前 言

本标准是“支持 IPv4 的路由器”系列标准之一，本系列的结构和标准名称预计如下：

1. YD/T 1096-2001 路由器设备技术规范——低端路由器；
2. YD/T 1098-2001 路由器测试规范——低端路由器；
3. YD/T 1097-2001 路由器设备技术规范——高端路由器；
4. YD/T 1156-2001 路由器测试规范——高端路由器；
5. 《路由器设备安全技术要求——中低端路由器（基于 IPv4）》；
6. 《中低端路由器安全测试方法》；
7. 《路由器设备安全技术要求——高端路由器（基于 IPv4）》；
8. 《高端路由器安全测试方法》。

随着技术发展，将制定后续标准。

本标准与《中低端路由器安全测试方法》配套使用。

本标准的附录 A 为资料性附录。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中兴通讯股份有限公司

华为技术有限公司

国家计算机网络与信息安全管理中心

中国电信集团公司

本标准主要起草人：苗福友 冯 伟 孟宪民 许志军 黄元飞 史 凡

路由器设备安全技术要求

——中低端路由器（基于 IPv4）

1 范围

本标准规定了支持IPv4协议的单播应用的中低端路由器设备的安全技术要求，包括数据转发平面安全、控制平面安全、管理平面安全等。

本标准适用于支持IPv4协议的单播应用的中低端路由器设备，不适用于支持IPv4协议的组播应用的中低端路由器设备。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 18336-2001	信息技术安全性评估准则
YD/T 1096-2001	路由器设备技术规范——低端路由器
YD/T 1098-2001	路由器测试规范——低端路由器

3 术语和定义

下列术语和定义适用于本标准。

3.1

访问控制 Access Control

防止未经授权使用资源。

3.2

授权 Authorization

授予权限，包括根据访问权进行访问的权限。

3.3

密钥管理 Key Management

根据安全策略产生、分发、存储、使用、更换、销毁和恢复密钥。

3.4

安全审计 Security Audit

对系统的记录及活动独立的复查与检查，以便检测系统控制是否充分，确保系统控制与现行策略和操作系统保持一致、探测违背安全性的行为，并介绍控制、策略和程序中所显示的任何变化。

3.5

数字签名 Digital Signature

附在数据单元后面的数据，或对数据单元进行密码变换得到的数据。允许数据的接收者证明数据的来源和完整性，保护数据不被伪造，并保证数据的不可否认性。

3.6

否认 Repudiation

参与通信的实体否认参加了全部或部分的通信过程。

3.7

可用性 Availability

根据需要，信息允许有权实体访问和使用的特性。

3.8

保密性 Confidentiality

信息对非授权个人、实体或进程是不可知、不可用的特性。

3.9

数据完整性 Data Integrity

数据免遭非法更改或破坏的特性。

3.10

安全服务 Security Service

由通信系统提供的，对系统或数据传递提供充分安全保障的一种服务。

3.11

安全策略 Security Policy

提供安全服务的一套规则。

3.12

安全机制 Security Mechanism

实现安全服务的过程。

3.13

拒绝服务 Denial of Service

阻止授权访问资源或延迟时间敏感操作。

3.14

防重放 Anti-Replay

防止对数据的重放攻击。

3.15

信息泄露 Information Disclosure

指信息被泄漏或透露给非授权的个人或实体。

3.16

完整性破坏 Integrity Compromise(damage)

数据的一致性通过对数据进行非授权的增加、修改、重排序或伪造而受到损害。

3.17

非法使用 Illegal Use

资源被非授权的实体或者授权的实体以非授权的方式或错误的方式使用。

4 符号和缩略语

下列符号和缩略语适用于标准。

3DES	Triple Data Encryption Standard	三重数据加密标准
ACL	Access Control List	访问控制列表
AES	Advanced Encryption Standard	先进加密标准
ARP	Address Resolution Protocol	地址解析协议
ASIC	Application-Specific Integrated Circuit	专用集成电路
BGP	Border Gateway Protocol	边界网关协议
BGP4	Border Gateway Protocol version 4	边界网关协议版本4
CAR	Committed Access Rate	承诺接入速率
CBC	Cipher Block Chaining	密码块链
CHAP	Challenge-Handshake Authentication Protocol	质询握手认证协议
CoS	Class of Service	业务类别
CPU	Central Processing Unit	中央处理器
CR-LDP	Constraint-based Routing Label Distribution Protocol	基于约束路由的标记分发协议
DNS	Domain Name Service	域名服务
DoS	Denial of Service	拒绝服务
DSS	Digital Signature Standard	数字签名标准
EGP	Exterior Gateway Protocol	外部网关协议
FTP	File Transfer Protocol	文件传输协议
HMAC	Hashed Message Authentication Code	散列消息认证码
HTTP	Hyper Text Transport Protocol	超文本传输协议
ICMP	Internet Control Messages Protocol	因特网报文控制协议
IDEA	International Data Encryption Algorithm	国际数据加密算法
IGP	Interior Gateway Protocol	内部网关协议
IKE	Internet Key Exchange	因特网密钥交换
IP	Internet Protocol	因特网协议
IPSec	Internet Protocol Security	因特网协议安全
IS-IS	Intermediate System to Intermediate System Protocol	中间系统到中间系统协议
L2TP	Layer 2 Tunneling Protocol	二层隧道协议
LAC	L2TP Access Concentrator	L2TP接入集中器
LDP	Label Distribution Protocol	标记分发协议
LNS	L2TP Network Server	L2TP网络服务器
LSP	Label Switched Path	标记交换路径
LSR	Label Switch Router	标记交换路由器
MAC	Media Access Control	媒介访问控制

MD5	Message Digest version 5	消息摘要版本5
MODP	Modular Exponentiation Group	模求幂组
MPLS	Multi-Protocol Label Switching	多协议标记交换
NAT	Network Address Translation	网络地址转换
NAPT	Network Address Port Translation	网络地址端口转换
NTP	Network Time Protocol	网络时间协议
OAM&P	Operation, Administration, Maintenance and Provisioning	操作、管理、维护和配置
OSPF	Open Shortest Path First	开放最短路径优先协议
PAP	Password Authentication Protocol	口令认证协议
PFS	Perfect Forward Secrecy	完美前向保密
RIP	Routing Information Protocol	路由信息协议
RIPv2	Routing Information Protocol version 2	路由信息协议版本2
RSVP	Resource Reservation Protocol	资源预留协议
RSVP-TE	Extension to RSVP for LSP Tunnels	用于LSP隧道的RSVP扩展
PPP	Point-to-Point Protocol	点到点协议
RSA	Rivest, Shamir and Adleman Algorithm	RSA算法
SHA	Secure Hash Algorithm	安全散列算法
SHA-1	Secure Hash Algorithm 1	安全散列算法版本1
SNMP	Simple Network Management Protocol	简单网络管理协议
SNMPv1	SNMP version 1	SNMP版本1
SNMPv2c	SNMP version 2c	SNMP版本2c
SNMPv3	SNMP version 3	SNMP版本3
SSH	Secure Shell	安全外壳
SSHv1	Secure Shell version 1	SSH版本1
SSHv2	Secure Shell version 2	SSH版本2
SSL	Secure Socket Layer	安全套接层
TCP	Transmission Control Protocol	传输控制协议
TFTP	Trivial File Transfer Protocol	简单文件传输协议
TLS	Transport Layer Security	传输层安全
ToS	Type of Service	服务类型
UDP	User Datagram Protocol	用户数据报协议
URPF	Unicast Reverse Path Forwarding	单播反向路径转发
USM	User-based Security Model	基于用户的安全模型
VLAN	Virtual Local Area Network	虚拟局域网
VPN	Virtual Private Network	虚拟专用网
VRF	VPN Routing and Forwarding	VPN路由和转发

5 概述

中低端路由器通常位于网络边缘，用作接入边缘网路由器，对中低端路由器的定义和使用范围参见 YD/T 1096-2001《路由器设备技术规范——低端路由器》。

中低端路由器处于网络边缘，往往是专用网络和骨干网络的接入点，所以它是网络攻击[从专用网络攻击外部网络（包括骨干网络和其他专用网络）或者利用外部网络攻击专用网络]的必经之路，在接入网络解决安全问题是整个网络安全体系的重要组成部分。

路由器功能在逻辑上可以划分为数据转发平面、控制平面和管理平面3个功能平面。

（1）数据转发平面主要指为用户访问和利用网络而提供的功能，如数据转发等。

（2）控制平面也可以称为信令平面，主要包括路由协议、ICMP协议等，以及与建立会话连接、控制转发路径等有关的功能。

（3）管理平面主要指与OAM&P有关的功能，如SNMP、管理用户Telnet登录、日志等，支持FCAPS（Fault、Capacity、Administration、Provisioning and Security）功能。管理平面消息的传送方式有带内和带外两种。

为了防范不安全事件的发生，中低端路由器应提供一定的安全功能。本标准引用 GB/T 18336-2001 中定义的安全功能类并应用到中低端路由器，这些安全功能类包括：

—鉴别和认证，确认用户的身份及其真实性；

—用户数据保护，保护用户数据相关的安全功能和安全策略；

—系统功能保护，安全数据（完成安全功能所需要的数据，如用户身份和口令）的保护能力；

—资源分配，对用户使用的资源进行控制，不允许用户过量占用资源造成的拒绝服务；

—安全审计，能够提供日志等审计记录，这些记录可以用来分析安全威胁活动和对策；

—安全管理，安全功能、数据和安全属性的管理能力；

—可信信道/路径，中低端路由器之间以及中低端路由器同其他设备之间通信的信道/路径要求可信，

对于传送敏感数据的通信要同传送其他数据的通信隔离开来；

—系统访问，本安全功能类要求控制用户会话的建立。

—路由器安全框架如图 1 所示。

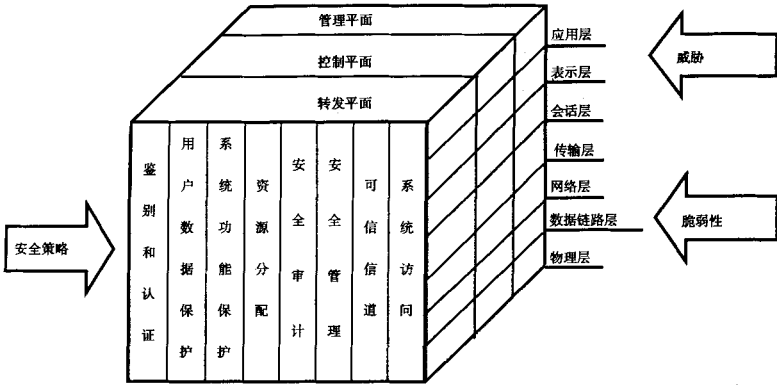


图1 路由器安全框架

硬件系统和操作系统是中低端路由器本身安全的重要因素，对硬件系统和操作系统的要求参见附录A。

6 数据转发平面安全

6.1 安全威胁

对数据转发平面的安全威胁主要有以下方面，但并不局限于这些方面：

- 对数据流的流量分析，从而获得敏感信息；
- 未授权观察、修改、插入和删除数据流；
- 拒绝服务攻击，降低设备的转发性能。

6.2 安全功能

6.2.1 鉴别和认证

中低端路由器位于网络边缘，需要对接入网络的数据源进行检查和确认，保证报文来自可信/合法的用户或设备。

6.2.2 用户数据保护

6.2.2.1 IPSec 功能

IPSec在IP层上提供数据保密性、数据源认证、数据完整性和抗重放等安全服务，由AH、ESP和IKE等协议组成。

中低端路由器支持IPSec协议，对IPSec的特性要求如下：

- 应支持手工密钥管理和IKE自动密钥管理；
- 应支持AH和ESP协议，对于这两种协议，应支持隧道和传送两种封装模式，建议支持AH和ESP协议的嵌套封装；

—AH和ESP协议应支持HMAC-MD5-96和HMAC-SHA1-96认证算法，ESP协议应支持国家相关部门规定的加密算法，以及DES-CBC、3DES-CBC和AES等加密算法，应支持空加密算法和空认证算法，但两者不应同时使用。

对 IKE 的特性要求如下:

- 第一阶段应支持主模式和野蛮模式;
- 第二阶段应支持快速模式;
- 应支持情报模式;
- 应支持预共享密钥认证方式, 建议实现 RSA 加密 Nonce 验证和数字证书认证方式;
- 应支持HMAC-MD5-96和HMAC-SHA1-96认证算法, 支持MD5和SHA1散列算法, 应支持国家相关部门规定的加密算法, 以及DES-CBC、3DES-CBC和AES等加密算法;
- 密钥交换应支持MODP-Group1、MODP-Group2等Diffie-Hellman组;
- 对于快速模式, 支持PFS。

6.2.3 系统功能保护

对于用户的安全数据, 系统要提供妥善的保护手段, 包括对访问安全数据的用户进行标识和鉴别。

6.2.4 资源分配

6.2.4.1 流量控制

常见的流量攻击是通过大量的某种流量实施的。对该种流量进行控制, 限制其进入网络的容量, 可以缓解这种攻击。中低端路由器应在其端口上支持采用CAR策略, 结合ACL和CoS, 控制某种类型的流量使用网络资源。

6.2.5 安全审计

对于用户流量, 中低端路由器要求能够提供流量日志能力, 相关要求参见 8.2.5 节有关规定。

6.2.6 安全管理

能够提供对本章提供的安全功能和管理能力, 管理方式包括但不限于控制台、远程连接或网络管理接口/系统等方式。

6.2.7 可信信道/路径

中低端路由器之间以及中低端路由器同其他设备间通信的信道/路径要求可信, 对于传送敏感数据的通信要同传送其他数据的通信隔离开来。

VPN能够将VPN内的用户数据同VPN外部或其他VPN的数据隔离开来, 能够提供可信的通信信道/路径, 对VPN功能的要求参见6.2.8.3节。

6.2.8 系统访问

6.2.8.1 过滤功能

应支持RFC 1858和RFC 3128规定的IP分片包过滤, 以及RFC 2827和RFC 3704规定的包过滤器。

6.2.8.2 访问控制列表

访问控制列表是基于报文的内容, 如MAC地址、IP地址、协议和端口等, 指定的安全规则表对每个进出路由器的报文通过与这些规则匹配, 确定对其处理的动作。

建议实现基于源MAC地址的访问控制列表, 降低系统的无谓开销。

应支持基于源地址、目的地址、协议类型、源端口号、目的端口号的访问控制列表, 建议支持基于IP头部的ToS域的访问控制列表, 以及在指定时间有效的访问控制列表, 应支持对报文匹配情况进行统计和产生日志等。中低端路由器应支持同时配置2000项以上的访问控制列表规则, 而不使性能明显下降。

6.2.8.3 VPN 功能

VPN利用公共网络资源，建立虚拟专用网络，利用VPN可以实现不同专用网络用户流量的隔离。中低端路由器支持利用以下技术实现VPN。

(1) L2TP隧道

应支持通过L2TP隧道技术实现VPN，应支持LAC和LNS功能，支持CHAP鉴别协议。

(2) IPSec隧道

宜支持通过IPSec隧道技术实现VPN，对IPSec的要求见6.2.2.1节。

(3) MPLS LSP

可基于MPLS LSP实现MPLS VPN，对MPLS VPN的要求如下：

—不管是L2 VPN还是L3 VPN，数据应严格基于标签沿着LSP转发。除非需要，一个VPN的数据不应被发送到该VPN之外，一个VPN的数据不应进入到另一个VPN。

—当同时支持VPN服务和因特网服务时，特别是在同一个物理接口上通过不同的逻辑接口支持VPN服务和因特网服务时，可基于逻辑接口对接入速率进行限制。

6.2.8.4 NAT

NAT的初衷是为了解决IP地址资源匮乏，但NAT可以实现内网和外网的隔离，内网可以正常地访问外网，同时可以隐藏内网的编址方案和网络结构，保证了内网的安全。

中低端路由器应支持NAT功能，对NAT的功能特性要求如下：

- 应支持NAPT；
- 应支持HTTP、FTP、DNS、H.323等应用协议；
- 应支持5 000以上的并发连接数；
- 支持输出NAT日志记录。

6.2.8.5 防火墙功能

中低端路由器宜支持防火墙功能，除包过滤、访问控制列表、NAT外，可支持应用代理功能，只允许被保护的网访问允许的网应用。

状态检测不仅检查网层和传输层的信息，还检查应用层协议的信息，实时维护这些TCP或UDP的状态信息。使用这些状态信息确定访问控制，中低端路由器可支持基于状态检测的包过滤功能。

7 控制平面安全

7.1 安全威胁

控制平面的安全威胁主要有以下几个方面，但并不局限于这些方面：

- 对协议流进行探测或者进行流量分析，从而获得转发路径信息。
- 获得设备服务的控制权，暴露转发路径信息，包括将转发路径信息暴露给非授权设备，一个VPN转发路径信息暴露给另一个VPN等。
- 利用协议流实施的拒绝服务攻击，如利用ICMP协议的Smurf攻击；利用路由协议的拒绝服务攻击；利用面向连接协议的半连接攻击等。
- 非法设备进行身份哄骗，建立路由协议的信任关系，非法获得转发路径信息。
- 针对路由协议转发路径信息的欺骗。

7.2 安全功能

7.2.1 鉴别和认证

7.2.1.1 PPP 用户认证

PPP作为数据链路层协议，本身并不具备完善的安全能力。其认证阶段应选用CHAP协议，而不能选用明文口令的PAP协议，以避免用户口令被侦听。

7.2.1.2 路由认证

路由安全是路由器执行正常功能的重要基础。动态路由协议可以分为IGP和EGP两类。对于中低端路由器，目前广泛采用的IGP有OSPF和IS-IS协议，EGP主要是BGP协议。其中：

—RIPv2、OSPFv2应支持明文认证和MD5加密认证；

—IS-IS应支持明文认证和MD5加密认证；

—BGP-4应支持MD5加密认证。

对于MPLS，用于建立LSP的标记分配协议主要有RSVP-TE和LDP/CR-LDP两种：

—LDP/CR-LDP

发现交换过程使用的消息由UDP协议承载。对于基本Hello消息，中低端路由器应只接受与可信LSR直接相连的接口上的基本Hello消息，忽略地址不是到该子网组播组的所有路由器的基本Hello消息；对于扩展Hello消息，可利用访问列表控制只接受允许的源发送来的扩展Hello消息。LDP会话过程使用的消息由TCP协议承载，应通过TCP MD5签名选项对会话消息进行真实性和完整性认证。

—RSVP-TE

应通过加密的散列算法支持实体认证，从而实现逐跳认证机制，应支持 HMAC-MD5 算法和 HMAC-SHA1 算法。

7.2.2 用户数据保护

7.2.2.1 路由认证

路由认证往往使用加密散列算法，在提供数据源认证的同时，也提供了数据完整性认证，路由认证功能参见7.2.1.2节。

7.2.3 系统功能保护

安全数据应得到妥善保护。

7.2.4 资源分配

7.2.4.1 抗常见网络攻击

7.2.4.1.1 URPF

URPF是通过在转发表中查找收到分组的源IP地址和接口，只转发源IP地址在IP路由表中存在分组的一种技术，这种技术可以缓解基于IP地址哄骗的网络攻击。中低端路由器应支持URPF功能。

7.2.4.1.2 禁止定向广播报文转发

Smurf攻击是一种利用定向广播报文实施的DoS攻击，中低端路由器应在端口禁止定向广播报文转发。

7.2.4.2 关闭一些 IP 服务

7.2.4.2.1 ICMP 协议

ICMP用于网络操作和排除故障，中低端路由器需要实现ICMP协议的一些功能，但设备应具有关闭这些功能的能力。这些ICMP消息类型包括：

—Type = 0 回显应答；

—Type = 3 目的地不可达；

- Type = 5 重定向;
- Type = 8 回显请求;
- Type = 11 超时。

7.2.4.2.2 代理 ARP

代理ARP是一台主机（常常是路由器）代替另一台主机应答ARP请求。该主机负责将分组转发到最终目的地的一种技术，代理ARP能够帮助一个子网的主机不用配置路由或默认网关到达远端子网。中低端路由器如果支持该功能，应具有关闭代理ARP的能力。

7.2.4.2.3 IP 源路由选项

IP 源路由选项取消了报文传输路径中各个设备的中间转发过程，而不管转发接口的工作状态，可能被恶意攻击者利用，刺探网络结构。中低端路由器如果支持该功能，应提供关闭 IP 源路由选项功能。

7.2.4.2.4 其他服务

对于下列 TCP 和 UDP 小端口服务，应缺省关闭这些服务，或者不提供这些服务：

- Echo;
- Chargen;
- Finger;
- NTP。

7.2.4.3 MPLS VPN

可实现 MPLS VPN 使用的路由器资源（如 CPU、内存等）的相互隔离，防止因一个 VPN 独占资源而造成对其他 VPN 的 DoS 攻击。

7.2.5 安全审计

对控制平面的信息要提供日志记录功能，特别是对设备的路由表等重要数据以及有影响的控制数据。关于日志可以参考 8.2.5 节。

7.2.6 安全管理

7.2.6.1 口令管理

中低端路由器涉及的口令长度应不少于 8 个字符，并且应由数字、字符或特殊符号组成。中低端路由器可提供检查机制，保证每个口令至少是由前述 3 类符号中的两类组成。

7.2.7 可信信道/路径

中低端路由器之间以及中低端路由器同其他设备之间的控制信息通信的信道/路径要求可信，对于传送敏感数据的通信要同传送其他数据的通信隔离开来。

7.2.8 系统访问

7.2.8.1 路由过滤

路由过滤可以控制路由协议对路由信息的发布和接受，可以只发布某些指定的路由，也可以只接收符合某些条件的路由。这样可以在满足需要的前提下减少路由器的资源消耗，达到更好的性能，避免路由攻击。在接收和发布路由信息时，应支持按 IP 地址、自治系统路径以及团体属性进行过滤。

7.2.8.2 MPLS VPN

7.2.8.2.1 L2 VPN

—VPN 之间 MAC 地址和 VLAN 信息应相互隔离，VPN 之间或 VPN 和 MPLS 骨干之间应可以复用 MAC 地址空间和 VLAN 空间。

—除非需要，VPN 之间或 VPN 和 MPLS 骨干之间的交换信息应相互隔离。

7.2.8.2.2 L3 VPN

常用的 L3 VPN 技术是 BGP/MPLS VPN。BGP/MPLS VPN 实质上是通过 BGP 协议约束路由信息分配的 MPLS，对 L3 VPN 要求如下：

—应支持静态路由算法和动态路由算法。对于动态路由算法，建议具有在接口上过滤路由更新的能力，IGP 和 EGP 路由协议都应支持 MD5 加密认证，并可基于 VRF 实例限制路由更新的速度。

—VPN 之间的拓扑和编址信息应相互隔离，一个 VPN 应可以使用所有因特网地址范围，包括 RFC 1918 定义的私有地址范围，VPN 之间或 VPN 和 MPLS 骨干之间应可以复用 IP 地址空间。

—应为每个 VPN 维持一个独立的 VRF 实例，除非需要，VPN 之间或 VPN 和 MPLS 骨干之间的路由信息及其分发和处理应相互独立，互不干扰。

7.2.8.3 防火墙功能

防火墙功能参见 6.2.8.5 节。

8 管理平面安全

8.1 安全威胁

对管理平面的安全威胁主要有以下方面，但并不局限于这些方面：

- 对数据流进行流量分析，从而获得设备有关的系统配置信息；
- 未授权观察、修改、插入、删除数据流；
- 未授权地访问管理接口，控制整个设备；
- 利用管理信息流实施拒绝服务攻击。

8.2 安全功能

8.2.1 鉴别和认证

对设备的管理用户都需要鉴别和认证。鉴别和认证是系统访问的基础，对有关 SNMP 管理、Web 管理、远程登录管理中用户认证的要求参见 8.2.8 节。

8.2.2 用户数据保护

对于中低端路由器，一般使用以下远程管理方式：

(1) SNMP

应支持 SNMPv3，支持 USM 等安全机制。

(2) 远程登录

建议支持 SSHv1 和 SSHv2，通过认证算法和加密算法实现对管理用户数据的保密性和完整性保护。

(3) Web 管理

可通过支持 SSL/TLS 安全协议，实现对管理用户数据的完整性保护。

有关这 3 种远程管理方式的详细要求参见 8.2.8.1、8.2.8.4、8.2.8.5 等节。

8.2.3 系统功能保护

与管理相关的安全数据应得到妥善保护。

8.2.4 资源分配

管理数据是系统运行的重要数据，系统要保证管理系统获得足够的运行资源，但是不能因此显著地影响控制平面和数据转发平面的正常工作。此外，通过管理平面提供的设备补丁下载功能应该得到严格的管理，不应该被用来对设备资源实施恶意占用。

8.2.5 安全审计

日志应记录过滤规则、拒绝访问、配置修改等相关安全事件，告警记录发生的安全违章事件，并可以一定的方式提示管理员。审计可对记录的安全事件进行回顾和检查，分析和报告安全信息，管理员基于该信息了解安全策略的执行情况，并据此进行修改。安全日志、安全告警等安全记录往往是安全审计的素材。

对日志的要求：

- 每个安全日志条目应包含事件主体、发生时间和事件描述等；
- 应可以保存在本地系统的缓存区内，也可以发送到专用的日志主机上作进一步处理；
- 应可以实时打印在专用打印机或连接路由器的显示终端上，以备最坏的情况下使用（如日志主机因安全危害而不能使用）；
- 应定义日志的严重程度级别，并能够根据严重程度级别过滤输出；
- 应支持和日志主机之间的接口。

对告警的要求：

- 应定义告警的严重程度级别，并根据严重程度级别确定是否以一定的方式（如声光显示）提示管理员；
- 应支持告警输出到打印机或显示终端，可根据严重程度级别输出到不同的显示终端；
- 告警应保存在本地或通过网络存储到其他主机。

8.2.6 安全管理

8.2.6.1 口令管理

口令管理要求参见 7.2.6.1 节。

8.2.7 可信信道/路径

8.2.7.1 带外管理

由于带内管理面临潜在的安全问题，中低端路由器可通过如独立的管理端口、VPN虚接口等方式支持专用管理网络，将管理通信流和其他通信流隔离。中低端路由器可提供关闭带内接口的能力，以实现只通过专用管理网络管理设备。

8.2.8 系统访问

8.2.8.1 SNMP 的安全性

SNMP 是一种应用非常广泛的网络管理协议，主要用于设备的监控和配置的更改等。目前使用的 SNMP 协议有 3 个版本，分别是 SNMPv1、SNMPv2c 和 SNMPv3。中低端路由器应支持安全性较好的 SNMPv3 作为网管协议。

此外，建议中低端路由器实现对网管站的访问控制，限定用户通过哪些 IP 地址使用 SNMP 对设备进行访问。

8.2.8.2 Telnet 访问

Telnet协议用于通过网络对设备进行远程登录。在中低端路由器中，如果为用户提供Telnet服务，则建议满足下列约定：

- 用户应提供用户名/口令才能进行后续操作，用户地址和操作应记入日志；
- 应限制同时访问的用户数；
- 在设定的时间内不进行交互，用户应自动被注销；
- 可限定用户通过哪些IP地址使用Telnet服务对设备进行访问；
- 必要时可关闭Telnet服务；

8.2.8.3 串口访问

中低端路由器如果支持串口访问功能，应提供同8.2.8.2节相同的安全保护能力。

8.2.8.4 SSH 访问

SSH是在不安全的网络上为远程登录会话和其他网络服务提供安全性的一种协议，对SSH服务的要求如下：

- 应支持 SSHv1 和 SSHv2 两个版本；
- 用户应通过身份认证才能进行后续的操作，用户地址和操作记入日志，中低端路由器应支持口令认证，建议支持公钥认证，可实现基于主机认证。
- SSH 服务器宜采用认证超时机制，在超时范围内没有通过认证应断开连接，建议限制客户端在一个会话上认证尝试的次数。
- SSHv2 应支持用于会话的加密密钥和认证密钥的动态管理，支持 Diffie-Hellman 组 14 的密钥交换，在密钥交换过程中协商密钥交换算法、对称加密算法和认证算法等，并对服务器端进行主机认证。
- 应支持 HMAC-SHA1 认证算法，建议支持 HMAC-SHA1-96 认证算法，可实现 HMAC-MD5、HMAC-MD5-96 等认证算法；
- 应支持 3DES-CBC 对称加密算法，可实现 Blowfish-CBC、IDEA-CBC、CAST128-CBC、AES256-CBC、AES128-CBC 等对称加密算法；
- 对于非对称加密算法，应支持 SSH-DSS，建议实现 SSH-RSA；
- 可限定用户通过哪些 IP 地址使用 SSH 服务对设备进行访问；
- 应支持必要时关闭 SSH 服务。

8.2.8.5 Web 管理

Web管理基于HTTP协议，中低端路由器宜支持Web管理，建议满足下列约定：

- 用户应提供用户名/口令才能进行后续的操作，用户地址和操作应记入日志；
- 可限定用户通过哪些IP地址使用HTTP对设备进行访问；
- 必要时可关闭HTTP服务；
- 应支持SSL/TLS。

8.2.8.6 软件升级

路由器一般使用FTP/TFTP协议实现设备的软件升级，软件升级包括软件版本、设备配置等，有本地和远程两种途径。软件升级通过建立FTP/TFTP服务器和客户端的连接来实现，FTP/TFTP协议应支持口令认证功能。

对于远程软件升级，建议支持SSHv2，实现文件的安全传送。

附 录 A
(资料性附录)

硬件系统和操作系统的安全要求

A.1 硬件系统

硬件系统主要包括硬件系统设计、密钥及系统程序保护设计等方面。

A.1.1 硬件系统设计

—在安全性要求比较高的场合，对与安全有关的元器件建议尽量采用具有自主知识产权的国产元器件，国内无法生产的元器件宜进行安全性测试后使用；

—建议采用模块式的硬件结构，将涉及到安全的功能模块与通用模块分割处置，部分关键模块可使用物理遮盖的方法进行保护，或者采用国家有关管理部门批准使用的安全硬件系统；

—对硬件系统的设置宜采用强身份认证机制保护；

—对于管理平面，可提供一个专用的管理接口，以用于建立专用的管理网络，实现管理和业务网络的物理隔离；

—各类安全告警信号建议使用多种标示方式，如由打印机打印，在显示终端上显示，且能用不同颜色或其他方式显示出各类安全告警信号的严重程度。

A.1.2 密钥及系统程序保护设计

—对安全性要求较高的场合，中低端路由器的密钥存储、运算和系统关键程序建议在硬件系统中单独设计，与系统其他部分物理分割，推荐使用遮盖或胶封等方法进行物理保护；

—对于以明文存储的密钥建议进行分割存储，其他密钥或证书宜加密存储，并提供单独的存储空间；

—建议提供密钥销毁功能。可通过菜单操作或某种直观的操作直接销毁硬件中存储的密钥和算法或系统的关键程序。在更进一步的安全要求下，建议提供设备开箱自毁功能，即在外力强迫打开机箱时，系统提供对密钥、算法和关键程序的销毁功能。

A.2 操作系统

—推荐使用专用的操作系统，并对操作系统进行固化，禁止一些不常用的服务和应用，采用的操作系统不应有后门，不建议使用通用操作系统；

—对加密 ASIC 所使用的驱动程序应经过国家有关管理部门的测试，并可在中低端路由器内定义到具体的内存、进程上下文；

—对命令集的结构进行缜密的设计以及对输入的参数进行全面的检查处理；

—对路由器资源的访问要能够进行权限限制和级别限制，如对管理员用户进行分级，为不同的管理员用户定义不同的管理能力，“网络管理员”用户可显示和修改配置和接口参数，而“操作员”用户只能够清除连接和计数器；

—对各个进程及使用资源进行审计，应提供基于用户的审计功能，用户审计功能应记录用户的登录行为、用户对设备的操作行为等；

—应具有备份版本、配置、日志记录等功能。

参考文献

- GB 4943-1995 信息技术设备（包括电气事务设备）的安全
- GB 9254-1998 信息技术设备的无线电骚扰限值及测量方法
- GB 9361-88 计算机场地安全要求
- GB/T 17618-1998 信息技术设备抗扰度限值及测量方法
- GB/T 18018-1999 路由器安全技术要求
- GB/T 18336-2001 信息技术 安全技术 信息技术安全性评估准则
- YD/T 849-1996 开放系统互联安全体系结构
- YD/T 968-1998 电信终端设备电磁兼容性限值及测量方法
- YD/T 1163-2001 IP网络安全技术要求——安全框架
- ISO 7498-2: 1989 信息处理系统 开放系统互连 基本参考模型第二部分：安全体系结构
- ISO/IEC 10164-7: 1992 信息技术 开放系统互连 系统管理 第七部分：安全报警报告功能
- ISO/IEC 10164-8: 1993 信息技术 开放系统互连 系统管理 第八部分：安全审计跟踪功能
- ISO/IEC 10745: 1995 信息技术 开放系统互连 上层安全模型
- ISO/IEC 11577: 1995 信息技术 开放系统互连 网络层安全协议
- ISO/IEC 11770-1 信息技术 安全技术 密钥管理 第一部分：框架
- ISO/IEC 11770-2 信息技术 安全技术 密钥管理 第二部分：使用对称技术的机制
- ISO/IEC TR 13335-1 信息技术安全管理的指导 第一部分：IT安全概念和模型
- ISO/IEC 15408-1 信息技术安全的评估准则 第一部分：引言和一般模型
- ISO/IEC 15408-2 信息技术安全的评估准则 第二部分：安全功能要求
- ISO/IEC 15408-3 信息技术安全的评估准则 第三部分：安全保证要求
- ITU-T X.805 (10/2003) 数据网络和开放系统通信 安全：提供端到端通信系统的安全体系结构
- IETF RFC 793 传输控制协议
- IETF RFC 1321 MD5消息摘要算法
- IETF RFC 1352 SNMP安全协议
- IETF RFC 1446 SNMPv2的安全协议
- IETF RFC 1700 分配号码
- IETF RFC 1704 关于因特网的认证
- IETF RFC 1858 IP分片过滤的安全考虑
- IETF RFC 1918 私有因特网的地址分配
- IETF RFC 2082 RIP-2 MD5认证
- IETF RFC 2154 使用数字签名的OSPF
- IETF RFC 2196 站点安全手册
- IETF RFC 2385 通过TCP MD5签名选项的保护BGP会话
- IETF RFC 2401 因特网协议的安全体系结构
- IETF RFC 2408 因特网安全关联和密钥管理协议

IETF RFC 2510	因特网X.509公开密钥基础设施证书管理协议
IETF RFC 2573	SNMPv3应用
IETF RFC 2644	改变路由器的默认的定向广播
IETF RFC 2827	网络入口过滤：防止使用IP源地址哄骗的拒绝服务
IETF RFC 2828	因特网安全术语表
IETF RFC 3013	建议的因特网服务提供商安全服务和程序
IETF RFC 3128	保护免受一种残片攻击的变种
IETF RFC 3567	IS-IS加密认证
IETF RFC 3704	多宿主（multihomed）网络的入口过滤
