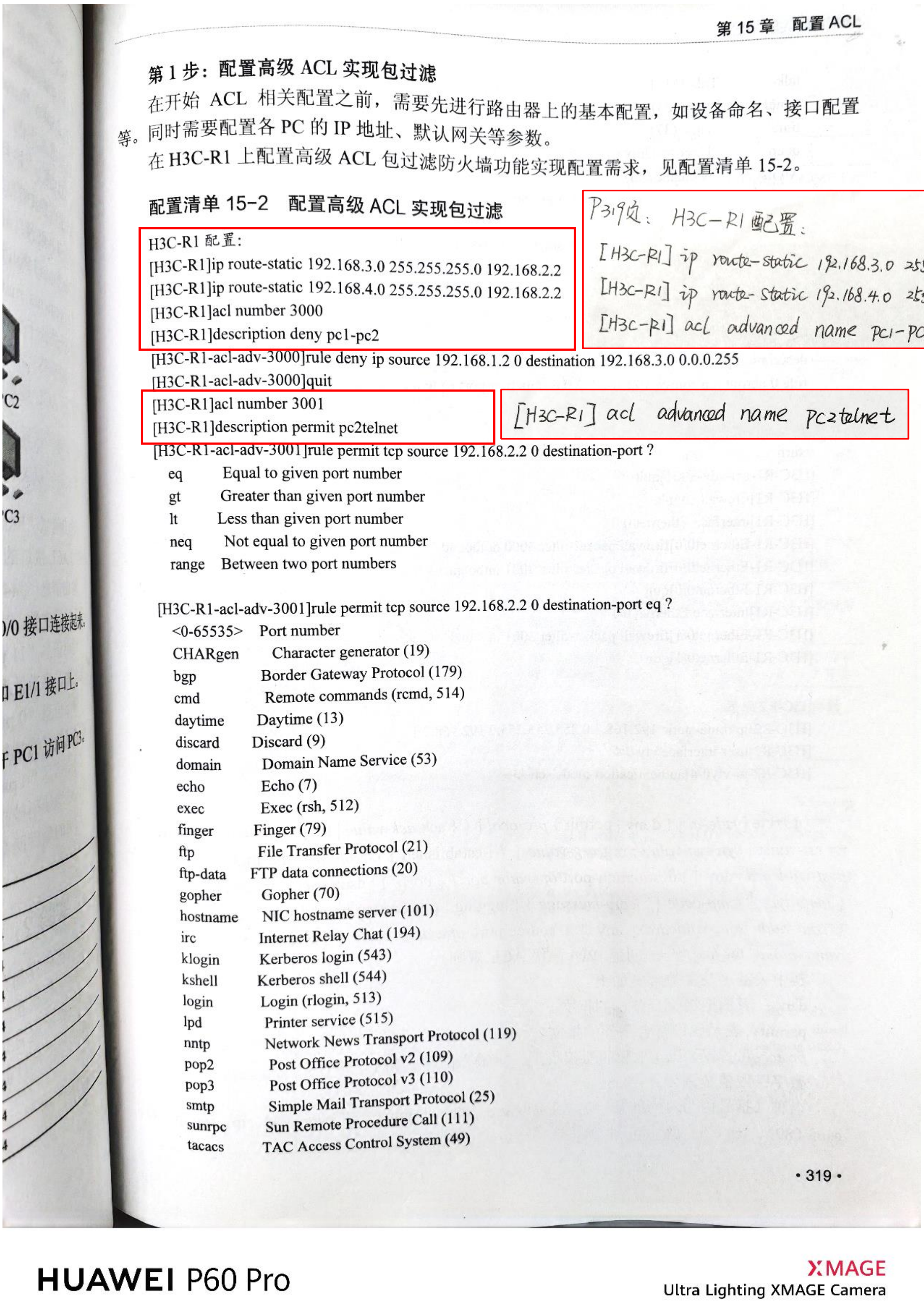

第 1 步：配置高级 ACL 实现包过滤

在开始 ACL 相关配置之前，需要先进行路由器上的基本配置，如设备命名、接口配置等。同时需要配置各 PC 的 IP 地址、默认网关等参数。

在 H3C-R1 上配置高级 ACL 包过滤防火墙功能实现配置需求，见配置清单 15-2。

配置清单 15-2　配置高级 ACL 实现包过滤

```
H3C-R1 配置：
[H3C-R1]ip route-static 192.168.3.0 255.255.255.0 192.168.2.2
[H3C-R1]ip route-static 192.168.4.0 255.255.255.0 192.168.2.2
[H3C-R1]acl number 3000
[H3C-R1]description deny pc1-pc2
[H3C-R1-acl-adv-3000]rule deny ip source 192.168.1.2 0 destination 192.168.3.0 0.0.0.255
[H3C-R1-acl-adv-3000]quit
[H3C-R1]acl number 3001
[H3C-R1]description permit pc2telnet
[H3C-R1-acl-adv-3001]rule permit tcp source 192.168.2.2 0 destination-port ?
  eq      Equal to given port number
  gt      Greater than given port number
  lt      Less than given port number
  neq     Not equal to given port number
  range   Between two port numbers

[H3C-R1-acl-adv-3001]rule permit tcp source 192.168.2.2 0 destination-port eq ?
  <0-65535>  Port number
  CHARgen    Character generator (19)
  bgp        Border Gateway Protocol (179)
  cmd        Remote commands (rcmd, 514)
  daytime    Daytime (13)
  discard    Discard (9)
  domain     Domain Name Service (53)
  echo       Echo (7)
  exec       Exec (rsh, 512)
  finger     Finger (79)
  ftp        File Transfer Protocol (21)
  ftp-data   FTP data connections (20)
  gopher     Gopher (70)
  hostname   NIC hostname server (101)
  irc        Internet Relay Chat (194)
  klogin     Kerberos login (543)
  kshell     Kerberos shell (544)
  login      Login (rlogin, 513)
  lpd        Printer service (515)
  nntp       Network News Transport Protocol (119)
  pop2       Post Office Protocol v2 (109)
  pop3       Post Office Protocol v3 (110)
  smtp       Simple Mail Transport Protocol (25)
  sunrpc     Sun Remote Procedure Call (111)
  tacacs     TAC Access Control System (49)
```

P319页：H3C-R1配置：

```
[H3C-R1] ip route-static 192.168.3.0 255.255.255.0 192.168.2.2
[H3C-R1] ip route-static 192.168.4.0 255.255.255.0 192.168.2.2
[H3C-R1] acl advanced name pc1-pc2
```

```
[H3C-R1] acl advanced name pc2telnet
```

C2

C3

/0 接口连接起来.

I E1/1 接口上.

F PC1 访问PC3.

```
talk        Talk (517)
telnet      Telnet (23)
time        Time (37)
uucp        Unix-to-Unix Copy Program (540)
whois       Nicname (43)
www         World Wide Web (HTTP, 80)

[H3C-R1-acl-adv-3001]rule permit tcp source 192.168.1.2 0 destination-port eq 23
[H3C-R1-acl-adv-3001]rule deny tcp source any destination-port eq 23
[H3C-R1-acl-adv-3001]display this
#
acl number 3001
 description pc1-pc2
 rule 0 permit tcp source 192.168.2.2 0 destination-port eq telnet
 rule 5 deny tcp destination-port eq telnet
#
return
[H3C-R1-acl-adv-3001]quit
[H3C-R1]firewall enable
[H3C-R1]interface Ethernet 0/0
[H3C-R1-Ethernet0/0]firewall packet-filter 3000 outbound
[H3C-R1-Ethernet0/0]firewall packet-filter 3001 intbound
[H3C-R1-Ethernet0/0]quit
[H3C-R1]interface Ethernet 0/1
[H3C-R1-Ethernet0/1]firewall packet-filter 3001 inbound
[H3C-R1-Ethernet0/1]quit
```

```
[H3c-R1] inter GigabitEthernet0/0
[H3c-R1-GigabitEthernet0/0] packet-filter name pc1-pc2 outbound
[H3c-R1-GigabitEthernet0/0] packet-filter name pc2telnet inbound
[H3c-R1-GigabitEthernet0/0] quit
[H3c-R1] inter GigabitEthernet0/1
[H3c-R1-GigabitEthernet0/1] packet-filter name pc2telnet inbound
[H3c-R1-GigabitEthernet0/1] quit
```

H3C-R2 配置：

```
[H3C-R2]ip route-static 192.168.1.0 255.255.255.0 192.168.2.1
[H3C-R2]user-interface vty 0 4
[H3C-R2-ui-vty0-4]authentication-mode scheme
```

（1）rule [*rule-id*] { deny | permit } *protocol* [{ { ack *ack-value* | fin *fin-value* | psh *psh-value* | rst *rst-value* | syn *syn-value* | urg *urg-value* } * | established } | counting | destination { *dest-addr dest-wildcard* | any } | destination-port *operator port1* [*port2*] | dscp *dscp* | fragment | icmp-type { *icmp-type* [*icmp-code*] | *icmp-message* } | logging | precedence *precedence* | reflective | source { *sour-addr sour-wildcard* | any } | source-port *operator port1* [*port2*] | time-range *time-range-name* | tos *tos*] *——创建 IPv4 高级 ACL 规则。

其中关键字及参数含义如下。

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

protocol：表示 IPv4 承载的协议类型，可输入的形式如下。

数字：取值范围为 0～255。

名称（括号内为对应的数字）：可选取 gre（47）、icmp（1）、igmp（2）、ip、ipinip（4）、ospf（89）、tcp（6）或 udp（17）。