

## Release Note

# Software Release 2.4.1

## For AR100 Series Internet Routers

Introduction .....	2
New Features and Enhancements .....	2
Telephony Services .....	2
Point-to-Point Protocol (PPP) .....	6
Asynchronous Port Names .....	11
Firewall .....	12
Timeouts .....	13
User Accounts .....	13
Security Mode .....	14
Basic Rate Interface (BRI) .....	15
Displaying Stack Dumps .....	15
Loader .....	16
RESET CPU UTILISATION command .....	16
COPY command .....	17
Internet Protocol (IP) .....	17
DHCP Extended ID .....	18
HTTP Server .....	18
Availability .....	18
Installation .....	19

## Introduction

Allied Telesyn announces the release of Software Release 2.4.1 for AR100 Series Internet Routers. This Release Note describes the new features in Software Release 2.4.1, since Software Release 1.9.4. Corrections to the Reference Manual that was released with Software Release 1.9.4 are described separately in an Errata for Software Release 1.9.4 (Document Number C613-06003-00 REV A). This Errata is available on the support site at [www.alliedtelesyn.co.nz/support/ar100/](http://www.alliedtelesyn.co.nz/support/ar100/).

This Release Note should be read in conjunction with the AR100 Series Internet Router Software Reference for Software Release 2.4.1, available on the support site at [www.alliedtelesyn.co.nz/support/ar100/](http://www.alliedtelesyn.co.nz/support/ar100/).



**WARNING:** Information in this document is subject to change without notice and does not represent a commitment on the part of Allied Telesyn International. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesyn International cannot accept any type of liability for errors in, or omissions arising from the use of this information.

## New Features and Enhancements

### Telephony Services

#### Ring Cadences

The number of user-settable tone cadences has been increased. Tones are used to inform the user of the progress of the call or operation. Tones are generated in the earpiece of the connected phone and are distinguished by the cadencing, or on-off time periods, of a 400Hz tone. To change a cadence, use the command:

```
SET PBX [CADENCE={BELL|RING|BUSY|DIAL|DISTINCTIVE|DTFS|DEXT|
FSET|UNAV} VALUE=cadence-values]
```

The CADENCE parameter specifies which tone cadence to change (“CADENCE parameters” on page 2).

**Table 1: CADENCE parameters**

Keyword	Meaning
BELL	The phone's ringing bell cadence.
RING	The ringing tone cadence.
BUSY	The busy tone cadence.
DIAL	The dial tone cadence.
DISTINCTIVE	The phone's distinctive ringing bell cadence (see “Japanese NTT INS Support” on page 5).
DTFS	The dial tone feature set tone cadence.
DEXT	The external dial tone cadence.
FSET	The feature set tone cadence.
UNAV	The unavailable tone cadence.

If CADENCE is specified, the VALUE parameter must also be present. The VALUE parameter specifies the ON/OFF periods for the specified cadence, as a comma-separated list of decimal numbers:

```
VALUE=on1,off1,on2,off2,on3,off3
```

## PBX Functionality

In United States of America, ISDN users can choose to purchase a range of ISDN supplemental services. A number of ISDN supplemental services and the router's PBX functions both require the telephone's recall or flash hook button. The router supports the ISDN supplemental services by default, but one or more extensions can instead be set to support the router's PBX functions that require the flash hook or recall button.

USA ISDN supplementary services that require the flash hook button:

- Call conference
- Call hold
- Call waiting
- Call transfer

PBX functions that require the flash hook button:

- Putting a call on hold
- Transferring a call
- Shuttling between two calls
- Picking up a call to one phone from another phone
- Redialing the last number dialed
- Diverting a call

To access the PBX functions instead of the ISDN supplementary services, use the RECALL=LOCAL and the EXTENSIONCALL=ON parameters in the commands:

```
CREATE PBX EXTENSION=extension_number [RECALL={LOCAL|REMOTE}]
      [EXTENSIONCALL={ON|OFF|YES|NO|TRUE|FALSE}]

SET PBX EXTENSION=extension_number [RECALL={LOCAL|REMOTE}]
   [EXTENSIONCALL={ON|OFF|YES|NO|TRUE|FALSE}]
```

If LOCAL is specified, PBX functions that require use of the recall or flash hook button are enabled. If REMOTE is specified, ISDN supplementary services that require use of the recall or flash hook button are enabled. The default is REMOTE.

All of these PBX functions, except for putting a call on hold, are accessed by dialling a PBX prefix, and require that the EXTENSIONCALL parameter be set to ON. The EXTENSIONCALL parameter specifies whether or not the extension can be used to call another extension, or access PBX functions such as call transfer, call shuttle, call pickup and call redial. If EXTENSIONCALL is set to ON, the user can call another extension by off-hooking the telephone and dialling a "\*", followed by the PBX prefix for the required function and the internal extension number. If it is set to OFF, this extension can not call another extension. The default is ON.

For instructions about using each of the PBX functions, see "PBX Functions" in your router's Software Reference.

Default prefixes for each function will exist, but can be changed, using the command:

```
SET PBX [OPEXT={extension-number|NONE}] [BUSY={prefix-number|
NONE}] [CLEAR={prefix-number|NONE}]
[EXTERNAL={prefix-number|NONE}] [GRP={prefix-number|NONE}]
[IMMEDIATE={prefix-number|NONE}] [INTERNAL={prefix-number|
NONE}] [NOANSWER={prefix-number|NONE}]
[NOREPLY={prefix-number|NONE}] [OPERATOR={prefix-number|
NONE}] [PICKUP={prefix-number|NONE}] [REDIAL={prefix-number|
NONE}]
```

## Call Diversion

Call diversion can be configured for each extension using the commands:

```
CREATE PBX EXTENSION=extension-number DIVERT={NOREPLY|BUSY|
IMMEDIATE|INS|NOANSWER|NONE} [NUMBER=phone-number]
[REBOUND={1..30|NONE}] [TRANSFER=1..30]
SET PBX EXTENSION=extension-number DIVERT={NOREPLY|BUSY|
IMMEDIATE|INS|NOANSWER|NONE} [NUMBER=phone-number]
[REBOUND={1..30|NONE}] [TRANSFER=1..30]
```

where *phone-number* is the number to which the call is to be diverted, and must include either the internal call prefix or the external call prefix.

The DIVERT parameter specifies the type of call diversion in use. The NOREPLY option will divert the call if the extension is engaged or does not answer after the transfer timer expires. The BUSY option will divert the call if the extension is engaged. The IMMEDIATE option will divert the call immediately. The INS option will divert the call if the extension does not answer after the transfer timer expires. The NOANSWER option will divert the call if the extension does not answer after the transfer timer expires. The NONE option will not divert any calls from this extension. The default is NONE.

The REBOUND parameter specifies the timer value, in seconds, for the rebound after transfer. When a call is transferred and is not answered after the rebound time period, the call will return to the transferring phone. The rebound timer can be turned off by specifying the value NONE. The default is 20.

The TRANSFER parameter specifies the timer value, in seconds, for answer functions. When an answer mode is set that uses the timer, such as “answer on no reply”, the extension will ring for the specified transfer time before diverting to the next extension. The default is 20.

## Operator Extension

The prefix to call to call the operator can be set, using the command:

```
SET PBX [OPEXT={extension-number|NONE}]
```

The OPEXT parameter specifies which extension is the operator extension. When an extension has been set as the operator, dialling the operator prefix from any other extension will cause an internal call to be made to the specified operator. If the OPEXT parameter is set to NONE then the dial operator function is disabled. The default is 0.

## Japanese NTT INS Support

An extension can be configured to support the Japanese NTT INS I-Number service, using the commands:

```
CREATE PBX EXTENSION=extension-number [INUMBER={OFF|PORT1|PORT2|
PORT3} CALLINGNUMBER=calling-number] [optional parameters]

SET PBX EXTENSION=extension-number [INUMBER={OFF|PORT1|PORT2|
PORT3} CALLINGNUMBER=calling-number] [optional parameters]
```

The INUMBER parameter specifies the port number to use for each extension with the Japanese NTT INS I-Number service. The subscriber (base) number is always port1. Therefore, if the INUMBER parameter is set to PORT1 the CALLINGNUMBER parameter must be set to the subscriber (base) number. If the INUMBER parameter is set to PORT2 or PORT3 the CALLINGNUMBER parameter must be set to the additional directory number. If OFF is specified the I-Number feature is not used. If PORT1, PORT2, or PORT3 are specified, when the extension makes a call the CALLSETUP Q931 message will include the I-Number instead of the calling number. When a call is received with an I-number in the CALLSETUP Q931 message the extension configured with the respective I-number is rung. The default is OFF.

The router can be configured to support the Japanese NTT INS Distinctive Incoming Call service which is accessed via an NTT. If a call is received from a registered number, the telephone will ring in a distinctive pattern. To configure the distinctive pattern, use the command:

```
SET PBX CADENCE=DISTINCTIVE VALUE=on1,off1,on2,off2,on3,off3
[optional parameters]
```

where the ring pattern is specified by the VALUE parameter, in units of 0.1 seconds, in the form *on1,off1,on2,off2,on3,off3*.

## Caller ID Display

When caller ID display (CID) is enabled, the telephone number of an incoming call will be displayed on a CID unit. The router supports caller ID display, when the system territory is set to Japan, USA or New Zealand. In Japan, CID units support the NTT Caller ID protocol, which displays the number before the telephone begins to ring. In the USA and New Zealand, units generally support the Bellcore Caller ID protocol, which displays the number after the first ring. The router will select the appropriate protocol, depending on the territory. Users outside Japan should be aware that the calling number may not be displayed if the phone is not allowed to ring for a second time.

For a given call, caller ID display is only available if the caller has permitted the number to be displayed. If the number could not be displayed, a message will indicate that the service was unavailable.

Caller ID display is disabled by default. To enable or disable it, use the commands:

```
CREATE PBX EXTENSION=extension-number CLID=ON
[optional parameters]

SET PBX EXTENSION=extension-number CLID=ON [optional parameters]

SET PBX EXTENSION=extension-number CLID=OFF
[optional parameters]
```

To set the system territory, use the command:

```
SET SYSTEM TERRITORY=[JAPAN|NEWZEALAND|USA]
[optional parameters]
```

To display debugging information about caller ID display, use the command:

```
ENABLE PBX DEBUG=CLID [optional parameters]
```

To stop displaying debugging information, use the command:

```
DISABLE PBX DEBUG=CLID [optional parameters]
```

## PBX Debugging

The debug option CODEC has been replaced by the option DRIVER in the commands:

```
ENABLE PBX DEBUG={ALL|COMMAND|COUNTERS|CLID|DRIVER|EVENT|
  REDIRECTEDNUMBER|TRACE} [PORT=port-number]
```

```
DISABLE PBX DEBUG={ALL|COMMAND|COUNTERS|CLID|DRIVER|EVENT|
  REDIRECTEDNUMBER|TRACE}
```

The option DRIVER enables or disables capture of the data that is read from and written to the POTS driver.

## Point-to-Point Protocol (PPP)

### Charge Management

Charge management allows users to budget data calls made using a WAN connection by tracking the time spent connected, the amount of data transferred and the fees incurred when calls are made. The WAN link is disconnected if:

- the cumulative estimated fee counter exceeds a user-defined limit, *or*
- the cumulative charged fee counter plus the current call estimated charge exceeds a user-defined limit, *or*
- the cumulative connection time exceeds a user-defined limit



*Charge management operates independently of link management. A PPP interface should not be configured for both charge management and link management.*

In addition to recording *estimated call fees* based on the connection time and user-defined charging rates, the charge management facility will also record *actual charged fees* based on the processing of Q.931 *Advice of charge* messages, where these are generated by the service provider, to maintain an accurate record of charges. Advice of charge messages are transmitted by the service provider when a call is terminated and contain confirmation of the actual charges billed to the customer's account as a result of the call. If Advice of charge messages are provided, they are used instead of the estimated call fees.

Counters for connection time, data transferred, estimated fees, and charged fees can be automatically reset to zero (0) every month on a specified day, in line with service provider billing.

To ensure the maximum use is made of charged connection time, on demand calls are kept active as long as possible without incurring extra expense by extending the idle timer mechanism. On normal dial-on-demand calls, a idle timer is started whenever data is transmitted or received over the PPP interface. If the idle timer expires, the PPP interface is deemed inactive and the call is cleared. The idle timer extension delays call clearance until just before the next charging period.

For example if the idle timer expires before the minimum charge period has elapsed, then call clearance will be delayed until the end of the minimum charge period. If the idle timer expires during an subsequent charging period, then call clearance will be delayed until the end of that charging period.

Log messages are generated and sent to the Logging Facility when the counters are reset each month, or when a charge-limiting event disables the PPP link.

Charge management can be activated and deactivated during certain hours of the day and/or week using the Trigger Facility.




---

*Charge management does not apply to voice calls using telephony services (PBX).*

---

To create a new PPP interface with charge management thresholds, use the command:

```
CREATE PPP=[ppp-interface] OVER=physical-interface
  [CHARGELIMIT={NONE|1..1000000}] [CHARGING={YES|NO|TRUE|
  FALSE|ON|OFF}] [CURRENCY=currency-string] [CURUNIT={1|10|
  100|1000|10000}] [DISCONNECTMODE={IMMEDIATE|DELAYED}]
  [MINTIME={NONE|1..65535} MINFEE={NONE|0..65535}
  INCTIME={NONE|1..65535} INCFEE={NONE|0..65535}]
  [OFFSETTIME=0..255] [RESETPERIOD={NONE|MONTHLY|WEEKLY|
  DAILY}] [RESETVALUE={1..28|SUN|MON|TUE|WED|THU|FRI|SAT}]
  [optional parameters]
```

If any one of the parameters MINTIME, MINFEE, INCTIME, and INCFEE is specified, all of the parameters must be specified. If any of the parameters is set to NONE, then the other three parameters will automatically be set to NONE as well. Once set, these parameters can be changed independently, without having to specify values for the others.

The CHARGELIMIT parameter specifies the cumulative fee threshold in fractional currency units, for example yen or dollars, for the Charge Management object. When the Charge Management object's cumulative fee exceeds this limit, the PPP link is closed and any further attempts to open the PPP link will fail. The default value is NONE, which sets no threshold.

The CHARGING parameter specifies whether or not charge management is active. The default is NO.

The CURRENCY parameter specifies the name of the currency unit for reporting purposes. The default is based on the current setting of the system territory, set using the SET SYSTEM TERRITORY command.

The CURUNIT parameter specifies the number of fractional currency units per currency unit, e.g. 1 for JPY or 100 for dollars or pounds. If fractions of yen or cents are required then 10 or 1000 can be specified. The default is based on the current setting of the system territory, set using the SET SYSTEM TERRITORY command.

The DISCONNECTMODE parameter sets the disconnect behaviour of the charge management utility. IMMEDIATE forces the charge management utility to disconnect immediately when the charge limit reaches its configured limit. No further connections are permitted when the limit is reached. DELAYED forces the charge management utility to stay connected when the charge limit reaches its limit until explicitly disconnected, at which point no further connections are permitted. The DISCONNECTMODE is only effective if charge management is active. The default is IMMEDIATE.

The INCFEE parameter specifies the incremental charging fee, in fractional currency units, e.g. yen, cents or pence. The default is NONE. If INCFEE is specified, MINTIME, MINFEE, and INCTIME must also be specified.

The INCTIME parameter specifies the incremental charging step, in seconds, for each step after a MINTIME period. The default is NONE. If INCTIME is specified, MINTIME, MINFEE, and INCFEE must also be specified.

The MINTIME parameter specifies the minimum charging period, in seconds. The default is NONE. If MINTIME is specified, MINFEE, INCTIME, and INCFEE must also be specified.

The MINFEE parameter specifies the minimum charging fee, in fractional currency units, e.g. yen, cents or pence. The default is NONE. If MINFEE is specified, MINTIME, INCTIME, and INCFEE must also be specified.

The OFFSETTIME parameter specifies the anticipated difference (in seconds) between the telephone company timing and the router timing. The default value is 1 second, meaning that the router's idle time extension will be shortened by 1 second.

The RESETPERIOD parameter specifies the frequency that the counters in the Charge Management object are automatically reset and the PPP link re-enabled if it has been disabled. The action is equivalent to the RESET PPP LIMITS=ALL command. Note that the actual reset will occur one second past midnight on the day specified using the RESETVALUE parameter. When RESETPERIOD=DAILY, any information specified with the RESETVALUE parameter will be ignored. The default value is NONE.

The RESETVALUE parameter is used in conjunction with the RESETPERIOD parameter to specify when the counters in the Charge Management object are automatically reset and the PPP link re-enabled if it has been disabled. The RESETVALUE parameter must be specified if RESETPERIOD is not equal to NONE. When RESETPERIOD=MONTHLY, the valid values for RESETVALUE are the numbers 1 to 28. When RESETPERIOD=WEEKLY, the valid values for RESETVALUE are the days of the week.

To enable charge management on an existing PPP interface, or to change the charging rates or thresholds, use the command:

```
SET PPP=ppp-interface [CHARGELIMIT={NONE|1..1000000}]
  [CHARGING={YES|NO|TRUE|FALSE|ON|OFF}] [CURRENCY=currency-
string] [CURUNIT={1|10|100|1000|10000}]
  [DISCONNECTMODE={IMMEDIATE|DELAYED}] [MINTIME={NONE|
1..65535}] MINFEE={NONE|0..65535} INCTIME={NONE|1..65535}
  INCFEE={NONE|0..65535}] [OFFSETTIME=0..255]
  [RESETPERIOD={NONE|MONTHLY|WEEKLY|DAILY}]
  [RESETVALUE={1..28|SUN|MON|TUE|WED|THU|FRI|SAT}]
  [optional parameters]
```

To reset the limits, enter the command:

```
RESET PPP=ppp-interface [COUNTERS] [LIMITS={ONLINE|INDATA|
OUTDATA|TOTALDATA|CHARGE|ALL}]
```

Many of these limits could previously be reset using the parameter LINKCOUNTERS parameter in this command. The LINKCOUNTERS parameter is still valid, but the LIMITS parameter is now the preferred syntax.

## PPP Debug expansion

Four new options have been added to the ENABLE PPP DEBUG command, which displays information that might be helpful while dealing with network configuration problems. These options are CTRLPKT (which supersedes BAPPKT), DATAPKT, DECODE and LQR. The obsolete option BAPPKT is still supported for backwards compatibility, and the synonyms PACKET and PKT are the equivalent of specifying CTRLPKT and DATAPKT at the same time. The syntax is:

```
DISABLE PPP=ppp-interface DEBUG={ALL|AUTH|BAPPKT|BAPSTATE|
CALLBACK|CTRLPKT|DATAPKT|DECODE|DEMAND|ENCO|LCP|LQR|NCP|
PACKET|PKT|UTILISATION}[ , ... ]

ENABLE PPP TEMPLATE=template DEBUG={ALL|AUTH|BAPPKT|BAPSTATE|
CALLBACK|CTRLPKT|DATAPKT|DECODE|DEMAND|ENCO|LCP|LQR|NCP|
PACKET|PKT|UTILISATION}[ , ... ] [ASYN=port-number]
[TIMEOUT={NONE|1..4000000000}] [NUMPKTS={CONT|
1..4000000000}]
```

Table 2 on page 9 lists the new debugging options and their meanings. Output is sent to the specified asynchronous port or the terminal from which the command was entered.

**Table 2: Point-to-Point Protocol (PPP) debugging options.**

Option	Description
CTRLPKT	Hexadecimal dump of PPP control packets received and transmitted on the PPP interface.
DATAPKT	Hexadecimal dump of data packets received and transmitted on the PPP interface.
DECODE	Decoded control packets. Enabling this option will also automatically enable the AUTH debug. Currently, only LCP packet decoding is supported.
LQR	Decoded LQR packets.
PACKET PKT	Hexadecimal dump of all packets received and transmitted on the PPP interface. This option has the same effect as the CTRLPKT and DATAPKT specified at the same time.

## Maximum Transmission Unit

The Maximum Transmission Unit (MTU) can now be set in a PPP template. The syntax is:

```
CREATE PPP TEMPLATE=template [MTU=value] [optional parameters]
SET PPP TEMPLATE=template [MTU=value] [optional parameters]
```

The MTU parameter specifies the value of the maximum transmission unit. The allowable MTU values for the PPP lower layers are shown in Table 3 on page 9.

**Table 3: Allowable MTU values.**

Interface	Minimum MTU	Maximum MTU	Default MTU
PPP (except over Ethernet)	256	1500	1500
PPP over Ethernet	256	1492	1492



*For normal operations do not change the default MTU values.*

## MRU

When a Point-to-Point (PPP) link is brought up, a Link Control Protocol (LCP) link request may include an Maximum Receive Unit (MRU) option, indicating to the remote endpoint the largest packet size that the sender of the option can receive from the endpoint. Transmission of the MRU option can now be disabled for PPP links, or a specific value indicated. Third-party products have been known, on the receipt of this option, to terminate the link. To allow interoperability with these products it may be necessary to disable transmission of the MRU option. If transmission of the MRU option is explicitly disabled for a PPP interface or template, all subsequent requests on that interface will omit the MRU option.

To disable or enable transmission of the MRU option when creating a PPP interface or PPP template, use the commands:

```
CREATE PPP=ppp-interface OVER=physical-interface
  [MRU={ON|OFF|256..1656}] [optional parameters]

CREATE PPP TEMPLATE=template [MRU={ON|OFF|256..1656}]
  [optional parameters]
```

To modify the MRU option on an existing PPP interface or PPP template, use the commands:

```
SET PPP[=ppp-interface] [MRU={ON|OFF|256..1656}]
  [optional parameters]

SET PPP TEMPLATE=template [MRU={ON|OFF|256..1656}]
  [optional parameters]
```

The MRU parameter specifies whether the MRU (Maximum Receive Unit) option is transmitted, and what value will be sent in LCP configuration requests while bringing up this interface. If OFF is specified, the MRU option is omitted. If a decimal value is specified, the transmitted MRU option will be set to this value. If ON is specified, the MRU is calculated normally. The default is ON.

## Maximum Links

A new parameter, MAXLINKS, has been added to the SET PPP command to modify the maximum number of dynamic links per multilink bundle on an existing dynamic PPP interface. The syntax is:

```
SET PPP[=ppp-interface] [MAXLINKS=1..64] [optional parameters]
```

The MAXLINKS parameter limits the number of dynamic PPP links that can be added to a multilink bundle as the result of incoming calls. The default value is 2. The MAXLINKS parameter is most applicable to ISDN links where the remote (receiving) end of the PPP link has a limited number of data channels. In this situation, MAXLINKS can be used to prevent a single PPP multilink bundle from monopolising all the B channels.

## Asynchronous Port Names

The router's asynchronous port was previously specified in commands using the PORT parameter. This parameter is still valid, but by default the asynchronous port is now specified using the ASYN parameter. If the router is configured using the PORT parameter and the configuration is saved using the CREATE CONFIG command, the PORT parameter will be replaced with the ASYN parameter. The following commands replace the equivalent commands with a PORT parameter:

```
CREATE LOG OUTPUT={TEMPORARY|output-id} DESTINATION={MEMORY|
  ASYN|ROUTER|SYSLOG} [ASYN=port-number] [optional
  parameters]

DISABLE ASYN=asyn-number

ENABLE ASYN=asyn-number

ENABLE PPP [DEBUG={ALL|AUTH|BAPSTATE|CALLBACK|CTRLPKT|
  DATAPKT|DECODE|DEMAND|ENCO|LCP|LQR|NCP|PACKET|PKT|
  UTILISATION}[,...] [ASYN=port-number]
  [optional parameters]

ENABLE PPP TEMPLATE=template [DEBUG={ALL|AUTH|BAPSTATE|
  CALLBACK|CTRLPKT|DATAPKT|DECODE|DEMAND|ENCO|LCP|LQR|NCP|
  PACKET|PKT|UTILISATION}[,...] [ASYN=port-number]
  [optional parameters]

LOAD [ASYN=port-number] [optional parameters]

PURGE ASYN={asyn-number|ALL}

RESET ASYN[=asyn-number]

RESET ASYN[=asyn-number] COUNTER[={DIAGNOSTIC|INTERFACE|
  RS232}]

RESET ASYN[=asyn-number] HISTORY

SET ASYN[=asyn-number] [ATTENTION={BREAK|alphabetical control
  char|^[|NONE]}] [CDCONTROL={CONNECT|IGNORE|ONLINE}]
  [DATABITS={5|6|7|8}] [DEFAULTSERVICE={ON|OFF|YES|NO|TRUE|
  FALSE}] [DTRCONTROL={CONNECT|OFF|ON}] [ECHO={ON|OFF|YES|
  NO|TRUE|FALSE}] [FLOW={CHARACTER|HARDWARE|NONE}]
  [HISTORY=0..99] [INFLOW={CHARACTER|HARDWARE|NONE}]
  [IPADDRESS={ipadd|NONE}] [IPXNETWORK=network]
  [LOGIN={ON|OFF|YES|NO|TRUE|FALSE}]
  [MAXOQLEN=0..4294967295] [MTU=40..1500] [NAME=name]
  [OUTFLOW={CHARACTER|HARDWARE|NONE}] [PAGE={4..99|OFF}]
  [PARITY={EVEN|MARK|NONE|ODD|SPACE}] [PROMPT={prompt|
  DEFAULT|OFF}] [SECURE={ON|OFF|YES|NO|TRUE|FALSE}]
  [SPEED={AUTO|75|110|134.5|150|300|600|1200|1800|2000|
  2400|4800|9600|14400|14.4K|19200|19.2K|28800|28.8K|38400|
  38.4K|57600|57.6K|115200|115.2K}] [STOPBITS={1|2}]
  [TYPE={DUMB|VT100}]

SET LOADER [ASYN={port-number|DEFAULT}] [optional parameters]

SET LOG OUTPUT={TEMPORARY|output-id} [ASYN=port-number]
  [DESTINATION={MEMORY|ASYN|ROUTER|SYSLOG}]

SHOW ASYN[=port-number|ALL] [ {COUNTER[={DIAGNOSTIC|INTERFACE|
  RS232}] | HISTORY | SUMMARY } ]

SHOW MANAGER ASYN

UPLOAD [METHOD=ZMODEM] [FILE=filename] [ASYN=port]
```

## Firewall

### Application Rule-based Policies

A new command has been added to define rules for managing application traffic between interfaces covered by the firewall policy:

```
ADD FIREWALL POLICY=policy APPRULE=app-rule-id
  ACTION={ALLOW|DENY} INTERFACE=interface
  APPLICATION={FTP|TELNET|TIME|DNS|BOOTPS|BOOTPC|TFTP|
  GOPHER|FINGER|WWW|KERBEROS|RTELNET|POP2|POP3|RTSP|
  SNMPTRAP|SNMP|VDOLIVE|REALAUDIO|REALVIDEO|CUSSEEME|XING|
  QUICKTIME} [COMMAND={GET|PUT}] [PORT=port]
```

The APPRULE parameter specifies both an identifier for the rule and the position of the rule in the list of rules for this policy. Rules are processed in order, from the lowest to the highest numbered rule. The identifier is used to refer to this rule in other commands.

The ACTION parameter specifies what the firewall should do with traffic that matches the selectors defined for this rule. If ALLOW is specified, the traffic will be permitted to pass through the firewall. If DENY is specified, the traffic will be prevented from passing through the firewall.

The APPLICATION parameter specifies the name of an application for which the session flows are to be modified by this rule. At least one of the parameters COMMAND or PORT is required.

The COMMAND parameter specifies a comma separated list of keywords, dependent on the application. Currently only GET and PUT are supported, representing the FTP STOR and RETR commands (RFC 959), respectively. The COMMAND parameter is only valid when APPLICATION is set to FTP. Application protocol packets containing these commands are either allowed through the firewall or removed from the flow, depending on the setting of the ACTION parameter.

The PORT parameter allows an alternate port to be used for the application, and for flows to the specified port to be treated as flows for that application.

To delete a rule for managing application traffic between interfaces covered by the firewall policy, use the command:

```
DELETE FIREWALL POLICY=policy APPRULE=app-rule-id
```

### Rule-based Policies

The option NONAT has been added to the ACTION parameter of the following commands:

```
ADD FIREWALL POLICY=policy RULE=rule-id
  ACTION={ALLOW|DENY|NONAT} [optional parameters]

SET FIREWALL POLICY=policy RULE=rule-id
  ACTION={ALLOW|DENY|NONAT} [optional parameters]
```

If NONAT is specified, any traffic that matches the rule will not have a NAT translation performed on it, should a NAT relationship exist for the interfaces involved.

## Timeouts

A new command allows timeouts for TCP, UDP, and other protocols to be set for a specified policy:

```
SET FIREWALL POLICY=policy [TCPTIMEOUT=seconds]
    [UDPTIMEOUT=seconds] [OTHERTIMEOUT=seconds]
```

The firewall will timeout inactive sessions after the set period. Specifying a value of 0 seconds for any of the timeout parameters will set the timeout period to 30 seconds.

The TCPTIMEOUT parameter specifies the timeout period, in seconds, for a TCP session.

The UDPTIMEOUT parameter specifies the timeout period, in seconds, for a UDP session.

The OTHERTIMEOUT parameter specifies the timeout period, in seconds, for sessions other than TCP or UDP. The default timeout for ICMP sessions is 10 minutes. The value of OTHERTIMEOUT can be set to less than 10 minutes for ICMP sessions. However, if the value of OTHERTIMEOUT is set to more than 10 minutes, it will default to 10 minutes because that is the timeout limit for ICMP sessions.

## User Accounts

A new parameter, LOGIN, has been added to the ADD USER and SET USER commands. This parameter enables managers to restrict all or a specified user's access to the command line by Telnet, and therefore to reduce the likelihood of Denial of Service attacks.

To add a user to the User Authentication Database, use the command:

```
ADD USER=login-name LOGIN={TRUE|FALSE|ON|OFF|YES|NO}
    PASSWORD=password [optional parameters]
```

To change the access rights for an existing user, use the command:

```
SET USER=login-name [LOGIN={TRUE|FALSE|ON|OFF|YES|NO}]
    [optional parameters]
```

To change the access rights for all users, use the command:

```
SET USER [LOGIN={TRUE|FALSE|ON|OFF|YES|NO}]
    [optional parameters]
```

The LOGIN parameter is used to specify whether or not users with a privilege of "user" will be able to login to the command line interface. If used without a login name, it changes all login values for user privileged users currently in the User Database. If a valid login name is specified, the login value of that specific user will be changed. FALSE means the user will be authenticated by the User Database but will not be allowed to log into the switch. TRUE enables the user to log into the switch and enter commands. The default is FALSE.

Usernames with LOGIN set to TRUE can be used both for PAP and CHAP authentication, and to login and access the command line. Usernames with LOGIN set to FALSE can only be used for PAP and CHAP authentication.

## Security Mode

The commands that a user may execute depend on the user's privilege level and the mode in which the router is operating. The router now operates in one of two modes, *normal mode* and *security mode*. By default the router operates in normal mode. To enable security mode, first create at least one user with SECURITY OFFICER privilege level, using the command:

```
ADD USER=login-name LOGIN=TRUE PASSWORD=password  
PRIVILEGE=SECURITYOFFICER [optional parameters]
```

Security mode can then be enabled, using the command:

```
ENABLE SYSTEM SECURITY_MODE
```

The router is restored to normal operating mode using the command:

```
DISABLE SYSTEM SECURITY_MODE
```

Sensitive data files can only be stored in the router's file subsystem when the router is operating in security mode.



---

*When security mode is disabled, all sensitive data files are automatically deleted.*

---

When the router is operating in security mode, only users with SECURITY OFFICER privilege can execute commands which could impact the security of the router:

- ACTIVATE SCR
- ADD IP INT
- ADD SCR
- ADD USER
- CREATE CONFIG
- CREATE PPP
- CREATE PPP TEMPLATE
- CREATE SNMP COMMUNITY
- DEACTIVATE SCR
- DELETE FILE
- DELETE SCR
- DELETE USER
- DISABLE USER
- DUMP
- EDIT
- ENABLE PPP DEBUG
- ENABLE PPP TEMPLATE DEBUG
- ENABLE SNMP
- ENABLE USER
- LOAD

- MODIFY
- PURGE USER
- RENAME FILE
- RESET ENCO
- RESET USER
- SET CONFIG
- SET INSTALL
- SET IP INT
- SET PPP
- SET PPP TEMPLATE
- SET SCR
- SET SNMP COMMUNITY
- SET USER
- SHOW CONFIG
- SHOW PPP CONFIG
- UPLOAD

## Basic Rate Interface (BRI)

A new parameter, CHANNEL, has been added to the SHOW BRI COUNTER command:

```
SHOW BRI[=instance] COUNTER[={INTERFACE|BRI}][CHANNEL={B1|B2|D|0|1|2}]
```

The CHANNEL parameter specifies which of the B1, B2, and D channels to include in the display of BRI counters. Specifying B1 or 0 displays only the B1 channel counters. Specifying B2 or 1 displays only the B2 channel counters. Specifying D or 2 displays only the D channel counters. Not specifying a channel displays the counters for all channels as well as the counters for the BRI as a whole.

## Displaying Stack Dumps

A new parameter, STACK, has been added to the SHOW DEBUG command, to limit the output to a stack dump, if one is available:

```
SHOW DEBUG [STACK]
```

If the STACK parameter is specified, the output depends on whether the last fatal condition was a hardware reset or a software reboot. After a software reboot, the output is a stack dump only. After a hardware reset, no stack dump information is available.

## Loader

Enhancements have been made to the router's file loading functionality:

- The server port can be set when loading from an HTTP server, using the `SERVPORT` parameter
- A destination file name can be specified when loading from an HTTP server, using the `DESTFILE` parameter
- A user name and password can be specified when loading from an HTTP server, using the `USERNAME` and `PASSWORD` parameters
- In the `SET LOADER` command, parameters with default settings can be returned to their defaults by specifying the option `DEFAULT`
- The parameter `SRCFILE` has been added as a synonym of the parameter `FILE`, to distinguish the source file name from the destination file name.

The command syntax for the loader commands is:

```
LOAD [METHOD={HTTP|WEB|WWW}] [DELAY=delay]
    [DESTFILE=filename] [DESTINATION=FLASH]
    [HTTPPROXY={hostname|ipadd} [PASSWORD=password]
    [PROXYPORT={1..65535}] [SERVER={hostname|ipadd}]
    [SERVPORT={1..65535|DEFAULT}] [SRCFILE|FILE=filename]
    [USERNAME=username]

LOAD [METHOD=NONE] [DELAY=delay] [DESTINATION=FLASH]
    [ASYN=port] [SRCFILE|FILE=filename]

LOAD [METHOD=TFTP] [DELAY=delay] [DESTINATION=FLASH]
    [SERVER={hostname|ipadd}] [SRCFILE|FILE=filename]

LOAD [METHOD=ZMODEM] [DELAY=delay] [DESTINATION=FLASH]
    [ASYN=port] [SRCFILE|FILE=filename]

SET LOADER [DELAY={delay|DEFAULT}] [DESTFILE=filename]
    [DESTINATION={FLASH|DEFAULT}] [HTTPPROXY={hostname|ipadd|
    DEFAULT}] [METHOD={HTTP|TFTP|WEB|WWW|ZMODEM|NONE|
    DEFAULT}] [PASSWORD=password] [ASYN={port|DEFAULT}]
    [PROXYPORT={1..65535|DEFAULT}] [SRCFILE|FILE=filename]
    [SERVER={hostname|ipadd|DEFAULT}]
    [SERVPORT={1..65535|DEFAULT}] [USERNAME=username]
```

The `SERVPORT` parameter optionally specifies the port on the HTTP server from which the file is loaded. If this is not specified (or is specified using the `DEFAULT` keyword) and no default has been explicitly set using the `SET LOADER` command, a default will be invoked according to the current load method. In this case, `SERVPORT` will take a value of 80 for HTTP.

The `DESTFILE` parameter specifies the name of the destination file in the router file system. When using the HTTP method, if `DESTFILE` is required it must be present on the command line whenever the `FILE` or `SRCFILE` parameter is present, or it will take no effect.

## RESET CPU UTILISATION command

The CPU utilisation can be reset to 0%, using the new command:

```
RESET CPU UTILISATION
```

## COPY command

A new command, COPY, can be used to copy any text file within FLASH memory:

```
COPY filename1.ext filename2.ext
```

## Internet Protocol (IP)

### Propagation of Static Routing Information

A new parameter, STATICEXPORT, has been added to the commands:

```
ADD IP RIP INTERFACE=interface [CIRCUIT=miox-circuit]
[IP=ipadd] [SEND={NONE|RIP1|RIP2|COMPATIBLE}]
[RECEIVE={NONE|RIP1|RIP2|BOTH}] [DEMAND={FALSE|NO|OFF|ON|
TRUE|YES}] [AUTH={NONE|PASSWORD|MD5}] [PASSWORD=password]
[STATICEXPORT={YES|NO}]

SET IP RIP INTERFACE=interface [CIRCUIT=miox-circuit]
[IP=ipadd] [SEND={NONE|RIP1|RIP2|COMPATIBLE}]
[RECEIVE={NONE|RIP1|RIP2|BOTH}] [DEMAND={FALSE|NO|OFF|ON|
TRUE|YES}] [AUTH={NONE|PASSWORD|MD5}] [PASSWORD=password]
[STATICEXPORT={YES|NO}]
```

The STATICEXPORT parameter specifies whether or not static routing information will be propagated from this interface. If YES is specified, static routes are included in routing exports. If NO is specified, static routes are omitted from routing exports. The default is YES.

### IP counters

The range of counters that can be displayed and reset to zero has been expanded. The command syntax is:

```
RESET IP COUNTER={ALL|ARP|ICMP|INTERFACE|IP|MULTICAST|ROUTE|
SNMP|UDP}

SHOW IP COUNTER[={ALL|ARP|ICMP|INTERFACE|IP|MULTICAST|ROUTES|
SNMP|UDP}]
```

### Displaying IP Route Information

A new parameter, FULL, has been added to the command SHOW IP ROUTE, to enable display of all routes, including those whose Layer 2 interface is down. Routes whose outgoing Layer 2 interface is down are marked with the “#” character after the layer two interface name. The command syntax is:

```
SHOW IP ROUTE[=ipadd] [{GENERAL|CACHE|COUNT|FULL}]
```

## DHCP Extended ID

A new command adds support for the extended Client ID to both the DHCP client and server. DHCP servers use the Client ID field in DHCP requests to identify remote clients. An extended client ID is used when connecting multiple router interfaces to the same DHCP server. The command syntax is:

```
SET DHCP EXTENDID={ON|OFF}
```

The EXTENDID parameter specifies whether DHCP clients will use an extended client ID when communicating with a DHCP server. If OFF is specified, the client ID value is the hardware address of the client interface. If ON is specified, the client ID value is extended to include an internal interface identifier, uniquely distinguishing different interfaces on a device. The default is OFF.

## HTTP Server

### Debugging

A new debug option, STATE, has been added:

```
DISABLE HTTP DEBUG={ALL|AUTH|MSG|SESSION|STATE}
```

```
ENABLE HTTP DEBUG={ALL|AUTH|MSG|SESSION|STATE}
```

If STATE is specified, debugging of state changes in the state machine is enabled or disabled. STATE debug shows each event that occurs, the current state and the new state.

### Displaying Server Session Information

The command:

```
SHOW HTTP SESSION
```

has been replaced with the command:

```
SHOW HTTP SERVER SESSION
```

**Figure 1-1: Example output from the SHOW HTTP SERVER SESSION command.**

Client IP	Interface	Current User	State
202.36.163.121	eth0	manager	AWAITING_REQ

## Availability

Software Release 2.4.1 is available immediately as a FLASH release for upgrading existing routers. The release file can be downloaded directly from the Software Updates area of the Allied Telesyn web site at [www.alliedtelesyn.co.nz/support/updates/patches.html](http://www.alliedtelesyn.co.nz/support/updates/patches.html) or from the support site for your router: [www.alliedtelesyn.co.nz/support/ar100/](http://www.alliedtelesyn.co.nz/support/ar100/).

## Installation

---

There are no known issues upgrading from Software Release 1.9.4 to Software Release 2.4.1.

After an upgrade is done, the LOGIN parameter is required when adding new users from the command line prompt. However, if users are added in the boot script, and the LOGIN parameter is not seen in the boot script, then the value of the login parameter for all levels of user privilege is set to TRUE. Therefore, system managers may wish to assess whether their users should be able to log in as well as being authenticated. They should then change the value of the LOGIN parameter accordingly.