

Release Note

AR Series Router Software Release 1.9.3

Introduction	2
Operation	2
HTTP Client and Server	2
Downloading Files Using HTTP	6
Aliases	8
Fast Buffers on PowerPC Models	9
User Authentication Database	9
Interfaces	10
Point-to-Point Protocol (PPP)	14
PPP Over Ethernet	14
PPP Link Management	19
Integrated Services Digital Network (ISDN)	22
X.25	22
LAPB (Layer 2)	23
X.25 DCE Mode (Layer 3)	23
Internet Protocol (IP)	27
Configuring IP Interfaces with DHCP	28
Support for a Secondary Nameserver	29
Relaying DNS Requests	29
Support for a Secondary Nameserver	32
Open Shortest Path First (OSPF)	32
Bridging	34
Firewall	35
IP Security (IPsec)	40
Other Changes	43
Other Enhancements	43
Availability	43
Installation	44

Introduction

Allied Telesyn International announces the release of Software Release 1.9.3 for the AR series of multiprotocol routers. This release note describes the new features and enhancements to the AR Router for Software Release 1.9.3, and should be read in conjunction with the *AR Series Router Reference Manual for Software Release 1.9* (Document Number C613-03016-00 REV C).

WARNING: Information in this release note 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 the document and the features and changes described are accurate, Allied Telesyn International can not accept any type of liability for errors in, or omissions arising from the use of this information.

The most significant enhancements in Software Release 1.9.3 are:

- Enhancements to the router's advanced Internet security features with the addition of a fully RFC-compliant IPsec (IP Security) implementation.
- Support for PPP over Ethernet services, both as a PPPoE host and a PPPoE access concentrator.
- An HTTP client and server for serving HTML pages out of FLASH memory, supporting web-based configuration tools and downloading files to the router from an HTTP server.
- Nemesis firewall support for dynamic interfaces.

Operation

A number of features have been added in Software Release to improve the manageability of the router, including:

- An HTTP client and server.
- The ability to download files to the router from a web server using HTTP.
- The use of aliases to shorten repetitive commands.
- Enhancements to the User Authentication Database.

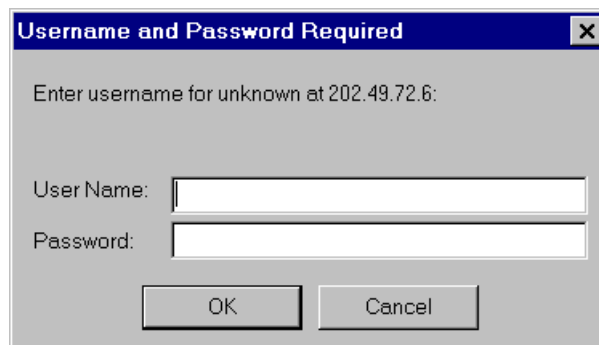
HTTP Client and Server

The router now provides a built-in HTTP client and server. The HTTP server is compatible with any HTTP/1.1-compliant browser and allows the router to serve HTML pages out of FLASH memory to a remote web browser. The HTTP server is enabled by default. To disable the HTTP server, or to enable the HTTP server after it has been disabled, use the commands:

```
DISABLE HTTP SERVER
```

```
ENABLE HTTP SERVER
```

When a user attempts to access the router via a web browser, the HTTP server will request authentication from the browser. The browser will prompt the user for a username and password (Figure 1 on page 3).

Figure 1: Logging in to the router from a web browser.

The username and password entered by the user must match a user defined in the User Authentication Database.

When the HTTP server receives a request for a URL, it uses the following procedure to resolve the URL:

- If the URL matches the name of a file stored in the router's FLASH memory, the file will be loaded and sent to the browser.
- If the URL does not match the name of a file stored in FLASH, and a web-based GUI is installed on the router, the HTTP server searches a list of dynamically generated HTML pages for a match. If a match is found the page is generated and sent to the browser.
- If the URL does not match the name of a file stored in FLASH or the name of a dynamically generated HTML page, the HTTP server will return the HTML error 404, indicating the URL could not be found.

By default, the router's home page is homepage.htm. This is the page the HTTP server returns when it receives a request that does not specify a particular page, and when no web-based GUI is installed on the router. If there is a web-based GUI, the router will return the GUI home page when a request does not specify a page. To change the home page to another file stored in the router's FLASH memory, use the command:

```
SET HTTP SERVER HOMEPAGE=filename.htm
```

All GET, configure and monitor requests, and authorisation failures are logged to the Logging Facility. Debugging can be enabled or disabled using the commands:

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

Debug messages display authorisation attempts, HTTP GET and POST requests and responses, and TCP state changes. The command:

```
SHOW HTTP DEBUG
```

displays the currently enabled debugging options for the HTTP server (Figure 2 on page 3, Figure 1 on page 4).

Figure 2: Example output from the SHOW HTTP DEBUG command.

```
Enabled Debug Modes
-----
AUTH,MSG
-----
```

Table 1: Parameters displayed in the output of the SHOW HTTP DEBUG command.

Parameter	Meaning
Enabled Debug Modes	The debugging modes currently enabled for the HTTP server; one or more of "NONE", "AUTH", "MSG", "SESSION" or "ALL".

The command:

```
RESET HTTP SERVER
```

restarts the HTTP server, disables debugging and clears all counters. The command:

```
SHOW HTTP SERVER
```

displays the current configuration and status of the HTTP server (Figure 3 on page 4, Figure 2 on page 4).

Figure 3: Example output from the SHOW HTTP SERVER command.

```

HTTP Server
-----
  Status ..... Enabled
  Homepage ..... homepage.htm
  Listen port ..... Open

  Sessions opened ..... 0
  Sessions closed ..... 0
  Received requests ..... 0
  Unknown requests ..... 0
  Transmitted replies ..... 0
  Authorisation replies ..... 0
  Authorisation sucesses ..... 0
  Authorisation failures ..... 0
-----

```

Table 2: Parameters displayed in the output of the SHOW HTTP SERVER command.

Parameter	Meaning
Status	The status of the HTTP server, one of "Enabled" or "Disabled".
Homepage	The homepage returned by the router when it receives a request that does not specify a page, and when there is no web-based GUI installed.
Listen port	Whether or not the HTTP server's TCP listen port is open: one of "Open" or "Closed".
Sessions opened	The number of HTTP server sessions that have been started.
Sessions closed	The number of HTTP server sessions that have been closed.
Received requests	The number of HTTP GET and POST requests received by the server.
Unknown requests	The number of unrecognised HTTP requests received by the server
Transmitted replies	The number of HTTP responses transmitted by the server.
Authorisation successes	The number of successful authentication attempts received by the server.

Table 2: Parameters displayed in the output of the SHOW HTTP SERVER command.

Parameter	Meaning
Authorisation failures	The number of authentication failures incurred during login attempts. Authentication failures occur when users fail to enter a user name or password when prompted by the browser, or enter an invalid user name or password

The command:

```
SHOW HTTP SESSION
```

displays TCP session information for the HTTP server (Figure 4 on page 5, Figure 3 on page 5).

Figure 4: Example output from the SHOW HTTP SESSION command.

Session	In Use	Type	TCP State	Activations
Session1	TRUE	Server	-	32
Session2	TRUE	Server	-	15
Session3	TRUE	Server	-	7
Session4	TRUE	Server	-	2
Session5	TRUE	Server	-	1
Session6	FALSE	None	-	0
Session7	FALSE	None	-	0
Session8	FALSE	None	-	0
..				
Session29	FALSE	None	-	0
Session30	FALSE	None	-	0

Table 3: Parameters in the output of the SHOW HTTP SESSION command.

Parameter	Meaning
Session	The session ID for a session. A maximum of 30 sessions can be active at any one time.
In Use	Whether or not the session is active; one of "TRUE" or "FALSE."
Type	The type of session; one of "None" (no active session), "Client" (the session is an outgoing connection from the router's HTTP client to a remote HTTP server), or "Server" (the session is an incoming connection from a client to the router's HTTP server).
TCP State	The current status of the TCP state machine; one of "FREE", "CLOSED", "LISTEN", "SYNSENT", "SYNRECEIVED", "ESTABLISHED", "FINWAIT1", "FINWAIT2", "CLOSEWAIT", "LASTACK", "CLOSING", "TIMEWAIT", OR "DELETE".
Activations	The number of times the session has been activated.

The HTTP client enables the router to act as a browser by sending HTTP GET or POST requests to another HTTP server. The HTTP client is used by the Configuration Wizard in a GUI to download updates from a support web site. The command:

```
SHOW HTTP CLIENT
```

displays the current state of the HTTP client (Figure 5 on page 6, Figure 4 on page 6).

Figure 5: Example output from the SHOW HTTP CLIENT command.

```

HTTP Client
-----
Sessions opened ..... 1
Sessions closed ..... 1
Transmitted requests ..... 1
Received replies ..... 1
-----

```

Table 4: Parameters displayed in the output of the SHOW HTTP CLIENT command.

Parameter	Meaning
Sessions opened	The number of HTTP client sessions that have been started.
Sessions closed	The number of HTTP client sessions that have been closed.
Transmitted requests	The number of HTTP GET and POST requests transmitted by the client.
Received replies	The number of HTTP responses received by the client.

Downloading Files Using HTTP

Files can now be downloaded into the router's FLASH memory or NVS (*non-volatile storage*) from a web server using HTTP (*HyperText Transfer Protocol*). The LOAD and SET LOADER commands have been modified to support this new functionality:

```

LOAD [METHOD={HTTP|WEB|WWW}] [DELAY=delay]
    [DESTINATION={FLASH|NVS}] [FILE=filename]
    [HTTPPROXY={hostname|ipadd} [PROXYPORT=1..65535]]
    [SERVER={hostname|ipadd}]

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

LOAD [METHOD=ZMODEM] [DELAY=delay] [DESTINATION={FLASH|NVS}]
    [FILE=filename] [PORT=port]

LOAD [METHOD=NONE] [DELAY=delay] [DESTINATION={FLASH|NVS}]
    [FILE=filename] [PORT=port]

SET LOADER [DELAY=delay] [DESTINATION={FLASH|NVS}]
    [FILE=filename] [HTTPPROXY={hostname|ipadd}]
    [METHOD={HTTP|TFTP|WEB|WWW|ZMODEM|NONE}] [PORT=port]
    [PROXYPORT=1..65535] [SERVER={hostname|ipadd}]

```

The METHOD parameter now supports a new option, HTTP. The options WEB and WWW are synonyms for HTTP. The default for METHOD is TFTP.

When METHOD is set to HTTP, the FILE parameter specifies the URL of the file to load (excluding the server name), and the SERVER parameter specifies the fully qualified domain name or IP address of the HTTP server.

If the HTTP server address is a fully qualified domain name, and a name server has been configured, the router will perform a DNS lookup of the server address. If a name server is not configured, then the SERVER parameter must specify the IP address of the HTTP server.

If access to the HTTP server is via a proxy server, the HTTPPROXY and PROXYPORT parameters can be used to specify the fully qualified domain

name or IP address of the proxy server, and the port to which proxy requests are sent. If the proxy server address is a fully qualified domain name, and a name server has been configured, the router will perform a DNS lookup of the proxy server address. If a name server is not configured, then the HTTPPROXY parameter must specify the IP address of the proxy server. The default for PROXYPORT is 80.

The default for DESTINATION is now FLASH.

The following are valid commands for loading the file /netupdates/new.cfg from the web server intranet.company.com (IP address 192.168.1.1):

```
load method=http destination=flash file=/netupdates/new.cfg
server=intranet.company.com

load method=http destination=flash file=/netupdates/new.cfg
server=192.168.1.1
```

The following are valid commands for loading the file /netupdates/new.cfg from the web server intranet.company.com (IP address 192.168.1.1) via proxy port 8001 on the proxy server proxy.company.com (IP address 192.168.10.5):

```
load method=http destination=flash file=/netupdates/new.cfg
server=intranet.company.com httpproxy=proxy.company.com
proxyport=8001

load method=http destination=flash file=/netupdates/new.cfg
server=192.168.1.1 httpproxy=192.168.10.5 proxyport=8001
```

The SHOW LOADER command has been modified to display the new parameters. Three new fields, *Method*, *HTTP Proxy* and *Proxy Port*, have been added (Figure 6 on page 7, Table 5 on page 8).

Figure 6: Example output from the SHOW LOADER command.

```
Loader Information
-----
Defaults:
Method..... HTTP
File ..... /netupdates/new.cfg
Server ..... intranet.company.com
HTTP Proxy ..... proxy.company.com (192.168.10.5)
Proxy Port ..... 8001
Port ..... -
Destination ..... Flash
Delay (sec) ..... 0

Current Load:
Method..... HTTP
File ..... /netupdates/8-200gui.rez
Server ..... intranet.company.com (192.168.1.1)
TCP Port ..... 8001
Destination ..... Flash
Delay (sec) ..... 0
Status ..... Loading
Load Level ..... 0%
-----
```

Table 5: New fields in the output of the SHOW LOADER command.

Parameter	Meaning
Method	The method used to load files; one of "TFTP", "HTTP", "WEB", "WWW", "ZMODEM" or "NONE".
HTTP Proxy	The IP address or host name of the proxy server when METHOD is set to HTTP and access is via a proxy server.
Proxy Port	The port on the proxy server when METHOD is set to HTTP and access is via a proxy server.

Aliases

The command line interface has been enhanced to support aliases. An alias is a short name for an often-used longer character sequence. When the user presses [Enter] to execute the command line, the command processor first checks the command line for aliases and substitutes the replacement text. The command line is then parsed and processed normally. Alias substitution is not recursive—the command line is scanned only once for aliases.

Aliases are created and destroyed using the commands:

```
ADD ALIAS=name STRING=substitution
DELETE ALIAS=name
```

where *name* and *substitution* are character strings 1 to 132 characters in length. Valid characters are any printable character. If *substitution* contains spaces it must be enclosed in double quotes.

The command:

```
SHOW ALIAS
```

displays the currently defined aliases (Figure 7 on page 8, Table 6 on page 8).

Figure 7: Example output from the SHOW ALIAS command.

```
Alias ..... df
String .... delete file=1-193.rez

Alias ..... ii
String .... ip interface
```

Table 6: Parameters displayed in the output of the SHOW ALIAS command.

Parameter	Meaning
Alias	The name of the alias.
String	The string substituted for the alias when it appears in a command line.

An alias may represent either part of a command, or a complete command. For example, assuming the following aliases are created:

```
add alias=df string="delete file=1-193.rez"
add alias=ii string="ip interface"
```

then the following commands are equivalent:

```
df
```

```

del file=1-193.rez

as are:

sh ii

show ip interface

```

Fast Buffers on PowerPC Models

PowerPC-based routers such as the AR720 and AR740 support a new class of memory buffer called “fast” buffers. Fast buffers are used for program data storage, not packet storage, and their contents are cached by the CPU. Two new fields, *Free fast buffers* and *Total fast buffers*, have been added to the output of the SHOW BUFFER command (Figure 8 on page 9, Table 7 on page 9).

Figure 8: Example output from the SHOW BUFFER command on a PowerPC-based router with fast buffers.

```

Memory ( DRAM ) ..... 1638 kB
Free Memory ..... 48 %
Free fast buffers ..... 1799
Total fast buffers ..... 1802
Free buffers ..... 4013
Total buffers ..... 4096
Buffer level 3 ..... 125 (don't process input frames)
Buffer level 2 ..... 250 (don't do monitor or command output)
Buffer level 1 ..... 500 (don't buffer up log messages)

```

Table 7: New fields in the output of the SHOW BUFFER command.

Parameter	Meaning
Free fast buffers	The number of free (unused) fast memory buffers. Fast buffer memory is cached by the CPU and is available only for program variable storage. It cannot be used for packet buffers.
Total fast buffers	The total number of fast memory buffers.

User Authentication Database

A new parameter, CALLINGNUMBER, has been added to the User Authentication Database (UAF). The ADD USER and SET USER commands have been modified to support this new option:

```

ADD USER=login-name PASSWORD=password [CALLINGNUMBER=number]
[other-options...]

SET USER=login-name [CALLINGNUMBER=number] [other-options...]

```

The CALLINGNUMBER parameter specifies the calling number to be used to authenticate incoming calls from L2TP and ISDN services that provide caller ID information. If an incoming call provides a calling number, then the username, password and calling number must match the entry in the UAF for the call to be successfully authenticated. The calling number is only checked if both the incoming call provides a calling number and the UAF entry has CALLINGNUMBER set. The number is checked from right to left and the check completes whenever a digit does not match or the end of one of the strings is reached.

The SHOW USER command has been modified to display the new CALLING NUMBER parameter. A new field, *Calling number*, has been added (Figure 9 on page 10, Table 8 on page 10).

Figure 9: Example output from the SHOW USER command.

```

Number of logged in Security Officers currently active ...1

User Authentication Database
-----
Username: dave ()
  Status: enabled      Privilege: user      Telnet: no
  Ip address: 192.168.1.1  Netmask: 255.255.255.0  Mtu: 1500
  Logins: 0           Fails: 0           Sent: 0           Rcvd: 0
Username: manager (Manager Account)
  Status: enabled      Privilege: manager  Telnet: yes
  Logins: 2           Fails: 1           Sent: 0           Rcvd: 0
Username: tony ()
  Status: enabled      Privilege: Sec Off   Telnet: no
  Callback number: 0061393546786  Calling number: 5554491
  Logins: 1           Fails: 0           Sent: 0           Rcvd: 0
-----

```

Table 8: New fields in the output of the SHOW USER command.

Parameter	Meaning
Calling number	The number to check against the incoming calling number of an L2TP or ISDN call, if the call provides caller ID information.

Interfaces

Software Release 1.9.3 adds support for control over the modem control signals of a synchronous interface. Prior to Software Release 1.9.3 there was no manual control over the modem control signals of a synchronous interface. The signals were asserted when a layer 2 module attached to the synchronous interface and the interface was enabled, and deasserted when either the layer 2 module detached or the interface was disabled. There are, however, some situations where control of the signals is necessary and this releases addresses these situations in a flexible and consistent manner.

The signals are paired off into RTS/CTS and DTR/DSR for RS-232/V.35 and C/I for X.21 to allow the output signal of each pair to follow the input signal, or to set the output permanently ON or OFF. Changing from DTE mode to DCE mode by changing the transition cable alters which signal of the pair is the input and which is the output. It is now possible to independently control the signals for each mode and to control CD in RS-232/V.35 DCE mode.

New log messages have been added to record modem control signal transitions (Table 9 on page 11). The most important control signal transitions are CD for RS-232 and V.35 DTE and I for X.21 DTE. These log messages have a higher priority and appear in the log by default. When the number of transitions exceeds 10 within a 10 minute period the number of transitions is reported in a single log message at the end of each 10 minute period.

Table 9: New log messages for synchronous modem control signals.

Type/SubType	Severity	Message Format/Description
PINT/WARN	URGENT	<p>syn<n>: <signal> modem control input change to <state></p> <p>A change in the modem control input that would normally indicate whether or not the NTU is seeing carrier from the remote NTU. This may indicate that the link will go down or up. <signal> is one of "CD" or "I". <state> is one of "ON" or "OFF".</p>
PINT/WARN	DETAIL	<p>syn<n>: <signal> modem control <direction> change to <state></p> <p>A non-critical modem control signal has changed state. This message will not appear in the log by default. <signal> is one of "RTS", "CTS", "DTR", "DSR", "CD", "I" or "C". <direction> is one of "input" or "output". <state> is one of "ON" or "OFF".</p>
PINT/WARN	URGENT	<p>syn<n>: <signal> modem control input changed <count> times in last 10 minutes</p> <p>A critical modem control input has changed state more than 10 times within 10 minutes. <signal> is one of "CD" or "I". <count> is the number of signal changes and includes the first 10 which will also generate log messages. The following changes will not generate log messages. The modem control input referred to is that which would normally indicate whether the NTU is seeing carrier from the remote NTU or not. This may indicate that the link has been going up and down.</p>
PINT/WARN	NOTICE	<p>syn<n>: <signal> modem control <direction> changes <count> times in last 10 minutes</p> <p>A modem control signal has changed state more than 10 times within 10 minutes. <signal> is one of "RTS", "CTS", "DTR", "DSR", "CD", "I" or "C". <direction> is one of "input" or "output". <number> is the number of signal changes and includes the first 10 which will also generate log messages. The following changes will not generate log messages. This message will appear in the log by default.</p>

The SET SYN command has been modified to support the control of modem control signals on synchronous interfaces:

```
SET SYN=n [C={ON|OFF|I}] [CD={ON|OFF|DTR}] [CTS={ON|OFF|RTS}]
[DSR={ON|OFF|DTR}] [DTR={ON|OFF|DSR}] [I={ON|OFF|C}]
[MAXOQLEN=max-queue] [MINTXINT=min-interval]
[RTS={ON|OFF|CTS}] [SPEED=speed]
```

The C parameter specifies the mode of operation for the X.21 modem control signal output called "C". This applies to the situation where an X.21-DTE cable is installed, the value of this parameter has no effect if any other transition cable is used. If ON is specified then the output will always be on when the interface is active and if OFF is specified then the output will always be off when the interface is active. If I is specified then when the interface is active C will be on when the modem control input signal I is on and C will be off when I is off. An interface is active when there is a layer 2 module attached and the interface is enabled. If the layer 2 module takes control of this output then the setting of this parameter is ignored. The default parameter value is ON.

The CD parameter specifies the mode of operation for the RS-232/V.35 modem control signal output called "CD". This applies to the situation where an RS-232 DCE or V.35 DCE cable is installed, the value of this parameter has no effect if any other transition cable is used. If ON is specified then the output will always be on when the interface is active and if OFF is specified then the output will always be off when the interface is active. If DTR is specified then when the interface is active CD will be on when the modem control input signal DTR is on and CD will be off when DTR is off. An interface is active when there is a layer 2 module attached and the interface is enabled. If the layer 2 module takes control of this output then the setting of this parameter is ignored. The default parameter value is ON.

The CTS parameter specifies the mode of operation for the RS-232/V.35 modem control signal output called "CTS". This applies to the situation where an RS-232 DCE or V.35 DCE cable is installed, the value of this parameter has no effect if any other transition cable is used. If ON is specified then the output will always be on when the interface is active and if OFF is specified then the output will always be off when the interface is active. If RTS is specified then when the interface is active CTS will be on when the modem control input signal RTS is on and CTS will be off when RTS is off. An interface is active when there is a layer 2 module attached and the interface is enabled. If the layer 2 module takes control of this output then the setting of this parameter is ignored. The default parameter value is ON.

The DSR parameter specifies the mode of operation for the RS-232/V.35 modem control signal output called "DSR". This applies to the situation where an RS-232 DCE or V.35 DCE cable is installed, the value of this parameter has no effect if any other transition cable is used. If ON is specified then the output will always be on when the interface is active and if OFF is specified then the output will always be off when the interface is active. If DTR is specified then when the interface is active DSR will be on when the modem control input signal DTR is on and DSR will be off when DTR is off. An interface is active when there is a layer 2 module attached and the interface is enabled. If the layer 2 module takes control of this output then the setting of this parameter is ignored. The default parameter value is ON.

The DTR parameter specifies the mode of operation for the RS-232/V.35 modem control signal output called "DTR". This applies to the situation where an RS-232 DTE or V.35 DTE cable is installed, the value of this parameter has no effect if any other transition cable is used. If ON is specified then the output will always be on when the interface is active and if OFF is specified then the output will always be off when the interface is active. If DSR is specified then when the interface is active DTR will be on when the modem control input signal DSR is on and DTR will be off when DSR is off. An interface is active when there is a layer 2 module attached and the interface is enabled. If the layer 2 module takes control of this output then the setting of this parameter is ignored. The default parameter value is ON.

The I parameter specifies the mode of operation for the X.21 modem control signal output called "I". This applies to the situation where an X.21-DCE cable is installed, the value of this parameter has no effect if any other transition cable is used. If ON is specified then the output will always be on when the interface is active and if OFF is specified then the output will always be off when the interface is active. If C is specified then when the interface is active I will be on when the modem control input signal C is on and I will be off when C is off. An interface is active when there is a layer 2 module attached and the interface is enabled. If the layer 2 module takes control of this output then the setting of this parameter is ignored. The default parameter value is ON.

The RTS parameter specifies the mode of operation for the RS-232/V.35 modem control signal output called "RTS". This applies to the situation where an RS-232 DTE or V.35 DTE cable is installed, the value of this parameter has no effect if any other transition cable is used. If ON is specified then the output will always be on when the interface is active and if OFF is specified then the output will always be off when the interface is active. If CTS is specified then when the interface is active RTS will be on when the modem control input signal CTS is on and RTS will be off when CTS is off. An interface is active when there is a layer 2 module attached and the interface is enabled. If the layer 2 module takes control of this output then the setting of this parameter is ignored. The default parameter value is ON.

All outputs will continue to be unconditionally OFF when there is no module attached or the interface is disabled.

NOTE: A new version of the RS-232 and V.35 DCE transition cables is required as the current cables do not allow the CTS, DSR and CD outputs to be individually controlled.

The actual modem control outputs that are present and may be configured depends upon the transition cable installed (Table 10 on page 13).

Table 10: Modem control signals available for each transition cable type.

Transition Cable	Modem Control Outputs	Modem Control Inputs
RS-232 DTE	RTS, DTR	CTS, DSR
V.35 DTE	RTS, DTR	CTS, DSR
X.21 DTE	C	I
RS-232 DCE	CTS, DSR, CD	RTS, DTR
V.35 DCE	CTS, DSR, CD	RTS, DTR
X.21 DCE	I	C

The output of the SHOW SYN command has been modified to display information about the control of modem control signals on synchronous interfaces. One new field, *Output mode*, has been added (Figure 10 on page 14, Table 11 on page 14).

Figure 10: Example output from the SHOW SYN command.

```

SYN instance 1:          3088 seconds   Last change at:          0 seconds

Module ..... PPP
State ..... enabled
Active ..... yes
Interface type ..... RS-232 DTE
Clocks ..... receive
Actual baud rate ..... determined externally
Configured baud rate ..... 48000
Max output queue length ... 100
Min interframe delay ..... no delay
Data sense ..... normal
Tx clock edge ..... rising
Hardware type ..... 68302
Debug ..... on
Control signals          State          Output mode          Transitions
  CTS (in) ..... off                    8
  DCD (in) ..... off                    2
  DSR (in) ..... off                    6
  RTS (out) ..... off                    follow CTS          6
  DTR (out) ..... off                    layer 2 control     6
  RL (out) ..... off                    4

```

Table 11: New fields in the output of the SHOW SYN command.

Parameter	Meaning
Output mode	The control mode for modem control output signals; one of "always off", "always on", "layer 2 control" and "follow XXX" where "XXX" is the name of the paired modem control input signal.

Point-to-Point Protocol (PPP)

Software Release 1.9.3 adds support for PPP links over Ethernet, and link management features for users wanting to control costs on PPP links using charged services such as ISP connections to the Internet.

PPP Over Ethernet

Software Release 1.9.3 adds support for the encapsulation and transmission of PPP packets over Ethernet as defined in RFC 2516 "A Method of Transmitting PPP Over Ethernet". The router can be configured to behave either as a host or as an access concentrator, as defined in RFC 2516.

PPP over Ethernet (PPPoE) provides the ability to connect a network of hosts over an access device to a remote *Access Concentrator*. An Access Concentrator may offer multiple services. A PPP over Ethernet link is a point-to-point connection between a host and a single service on an Access Concentrator.

PPP Over Ethernet has two distinct stages. In the *Discovery Stage*, the host discovers all the available Access Concentrators that offer the required service and then selects one. The host broadcasts an *Initiation* packet specifying the name of the service to which the host wants to connect. Access Concentrators which support the requested service respond with *Offer* packets which specify

the Access Concentrator's unicast Ethernet address. The host then selects an Access Concentrator and sends a *Discovery Request* packet specifying the name of the service to which the host wants to connect. The Access Concentrator responds with a *Discovery Session Confirmation* packet. When the Discovery Stage is complete the host and the selected Access Concentrator have all the information they need to create the point-to-point connection over Ethernet. In the *Session Stage* the host and the Access Concentrator exchange PPP packets.

When the router is configured as a PPPoE host, it acts as the gateway for hosts on the local LAN to establish PPP links over a broadband link (e.g. an xDSL modem) to an ISP or another remote office LAN. The router establishes each link using PPPoE active discovery with the service name of the ISP or remote office. When the router is configured as an access concentrator it offers one or more services to which hosts may connect. These services may represent connections to an ISP or a remote office. Whenever a host requests a service a dynamic PPPoE interface is created for that service. Multiple services and multiple sessions for each service are supported.

The ADD PPP, CREATE PPP and SET PPP commands have been modified to enable a PPP over Ethernet service to be specified as the physical interface for a PPP interface:

```
ADD PPP=ppp-interface OVER=physical-interface
    [other-ppp-options] ...

CREATE PPP=ppp-interface OVER=physical-interface
    [other-ppp-options] ...

SET PPP=ppp-interface OVER=physical-interface
    [other-ppp-options] ...
```

where *ppp-interface* is the PPP interface number and *physical-interface* is the name of the physical interface in the format SYN*n*, ISDN-*callname*, ACC-*callname*, MIOX*n*-*circuitname*, TNL-*callname*, TDM-*groupname* or ETH*n*-*servicename*. Service names may be up to 18 characters in length. Service names will normally be supplied by the ISP. If no service name is provided, use the special service name "ANY" to match any service.

A new PPPOE option has been added to PPP debugging commands to allow debugging PPPoE discovery packets received and transmitted, and PPPoE state transitions:

```
ENABLE PPP=ppp-interface
    DEBUG={ALL|AUTH|BAPPKT|BAPSTATE|CALLBACK|DEMAND|ENCO|LCP|
    NCP|PKT|PPPOE|UTILISATION} [, ...] [PORT=port-number]
    [TIMEOUT={NONE|1..4000000000}]
    [NUMPKTS={CONT|1..4000000000}]

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

DISABLE PPP=ppp-interface
    DEBUG={ALL|AUTH|BAPPKT|BAPSTATE|CALLBACK|DEMAND|ENCO|LCP|
    NCP|PKT|PPPOE|UTILISATION} [, ...]

DISABLE PPP TEMPLATE=template
    DEBUG={ALL|AUTH|BAPPKT|BAPSTATE|CALLBACK|DEMAND|ENCO|LCP|
    NCP|PKT|PPPOE|UTILISATION} [, ...]
```

By default, access concentrator mode is disabled. In this state the router can act as a PPPoE host simply by creating a PPP interface over a PPPoE service physical interface. To configure the router as an access concentrator, access

concentrator mode must be enabled and PPPoE services must be defined. Access concentrator mode can be enabled or disabled using the commands:

```
ENABLE PPP ACCESSCONCENTRATOR
DISABLE PPP ACCESSCONCENTRATOR
```

PPPoE services are added using the command:

```
ADD PPP ACSERVICE=service-name TEMPLATE=ppp-template
[ACRADIUS={OFF|ON}] [MAXSESSIONS=1..512]
```

The ACSERVICE parameter specifies the name of the PPPoE service. The TEMPLATE parameter specifies the PPP template to use when creating a dynamic PPP over Ethernet interface. The MAXSESSIONS parameter specifies the maximum number of PPPoE sessions that are allowed to simultaneously provide the PPPoE service. The default is 1. The ACRADIUS parameter specifies whether or not PPPoE hosts are authenticated by a RADIUS server using the hosts MAC address.

PPPoE services can be modified or deleted using the commands:

```
SET PPP ACSERVICE=service-name [ACRADIUS={OFF|ON}]
[MAXSESSIONS=1..512] [TEMPLATE=ppp-template]
DELETE PPP ACSERVICE=service-name
```

The command:

```
SHOW PPP PPPOE
```

displays information about the PPPoE interfaces and services that have been configured (Figure 11 on page 16, Table 12 on page 17).

Figure 11: Example output from the SHOW PPP PPPOE command.

```
PPPOE
-----
PPP1:
  Service Name ..... bob
  Peer Mac Address ..... 00-00-cd-00-ab-a3
  Session ID ..... ala3

  Access Concentrator Mode ..... Enabled

Services:
  bob
    Max sessions ..... 2
    Current Sessions ..... 1
    Template ..... 1
    MAC RADIUS Authentication ... YES
  ethel
    Max sessions ..... 5
    Current Sessions ..... 0
    Template ..... 1
    MAC RADIUS Authentication ... YES

PPPOE Counters:
  Rejected PADI packets ..... 0
  Rejected PADO packets ..... 0
  Rejected PADR packets ..... 0
  Rejected PADS packets ..... 0
  Rejected PADT packets ..... 0
-----
```

Table 12: Parameters displayed in the output of the SHOW PPP PPPOE command

Parameter	Meaning
Service Name	The name of the service either that the PPPoE interface is offering (if the interface is in access concentrator mode) or that the PPPoE interface is requesting/using (if the interface is not in access concentrator mode).
Peer Mac Address	The MAC address of the PPPoE peer.
Session ID	The ID of the current session.
Access Concentrator Mode	Enabled indicates that the router is acting as a PPPoE Access Concentrator. Disabled indicates that it is acting as a PPPoE client.
Services	The list of PPPoE services that the router can offer. This list is only displayed when the router is in Access Concentrator mode.
Max Session	The maximum number of simultaneous instances of the service that are permitted.
Current Sessions	The number of instances of the service currently in use.
Template	The number of the PPP template used to make PPP sessions that run over the service.
MAC RADIUS Authentication	On indicates that if RADIUS User Authentication is in use, the MAC address of the PPPoE peer will be sent with the username and password. Off indicates that the peer MAC address will not be sent.
Rejected PADI packets	The number of PPPoE PADI packets rejected because the requested service name was not available.
Rejected PADO packets	The number of PPPoE PADO packets rejected because no PPPoE interface was expecting a PADO or the PADO was not matched with a PPPoE interface.
Rejected PADR packets	The number of PPPoE PADR packets rejected because the PADR packet was not matched with a PPPoE interface.
Rejected PADS packets	The number of PPPoE PADS packets rejected because the PADS packet was not matched with a PPPoE interface.
Rejected PADT packets	The number of PPPoE PADT packets rejected because the PADT packet was not matched with a PPPoE interface.

The SHOW PPP has been modified to display the service name as the physical interface (Figure 12 on page 17).

Figure 12: Example output from the SHOW PPP command for PPP over Ethernet.

Name	Enabled	ifIndex	Over	CP	State
ppp0	YES	04	eth0-aardvark	IPCP LCP	OPENED OPENED

The SHOW PPP CONFIG command has been modified to display information about PPP over Ethernet. Two new fields, *Session ID* and *MAC Address of Peer*, have been added (Figure 13 on page 18, Table 13 on page 18).

Figure 13: Example output from the SHOW PPP CONFIG command for PPP over Ethernet.

Interface - description	Configured	Negotiated	
Parameter			

ppp0		Local	Peer
Bandwidth Allocation Protocol	ON		
Bandwidth Allocation Call Mode	CALL		
Multilink Fragmentation	OFF		
Acceptable Fragment Overhead (%)	5		
Null Fragment Timer (seconds)	3		
Session Timer (seconds)	OFF		
Idle Timer (seconds)	OFF		
Maximum Receive Unit (bytes)	1656	NONE	NONE
Compression	OFF	OFF	OFF
Username	NOT SET		
Password	NOT SET		
Bundle Endpoint Discr Class	0		
Bundle Endpoint Discr Value	[]		
Bundle Username	NOT SET		
eth0-aardvark			
Type	primary		
Modem Control	OFF		
Restart Timer (seconds)	3		
Max-Configure	continuous		
Max-Terminate	2		
Echo Request Timer (seconds)	OFF		
Callback Mode	OFF		
Link Compression	OFF	OFF	OFF
LQR Timer (seconds)	60	OFF	OFF
Magic Number	ON	OFF	OFF
Link Discriminator	0000	OFF	OFF
Link Endpoint Discr Class	0		
Link Endpoint Discr Value			
Authentication	NONE	NONE	NONE
Authentication Mode	INOUT		
Utilisation (%)	0		
PPPoE			
Session ID		4B5C	4B5C
MAC Address of Peer		00-00-cd-00-5e-65	
Service Name	aardvark		
Debug			
Maximum packet bytes to display	32		

Table 13: New fields in the output of the SHOW PPP CONFIG command for PPP over Ethernet.

Parameter	Meaning
Session ID	The value, in hexadecimal, of the session ID number for the current PPP over Ethernet session. The number is allocated by the Access Concentrator, which is the local router if the router is acting as an access concentrator, or the remote peer.
MAC Address of Peer	The MAC address of the peer to which the router is currently connected via the PPP over Ethernet session.
Service Name	The name of the Ethernet service that the PPP interface is using, of "ANY" if the special service name ANY was specified when configuring the PPP interface.

A new PPPOE option has been added to the SHOW PPP COUNT command to display PPPoE counters:

```
SHOW PPP [=ppp-interface]
COUNT [= { INTERFACE | LCP | MULTILINK | NCP | PPPOE }]
```

If PPPOE is specified, counters for PPPoE active discovery packets that have been sent and received are displayed (Figure 14 on page 19, Table 14 on page 19).

Figure 14: Example output from the SHOW PPP COUNT=PPPOE command.

ppp0	1519 seconds	Last change at:	974 seconds
PPPoE Counters			
PADIs Rx	1	PADIs Tx	0
PADOs Rx	0	PADOs Tx	1
PADRs Rx	1	PADRs Tx	0
PADsS Rx	0	PADsS Tx	1
PADTs Rx	0	PADTs Tx	0

Table 14: Parameters displayed in the output of the SHOW PPP COUNT=PPPOE command.

Parameter	Meaning
PADIs Rx	The number of PADI packets received.
PADIs Tx	The number of PADI packets transmitted.
PADOs Rx	The number of PADO packets received.
PADOs Tx	The number of PADO packets transmitted.
PADRs Rx	The number of PADR packets received.
PADRs Tx	The number of PADR packets transmitted.
PADsS Rx	The number of PADS packets received.
PADsS Tx	The number of PADS packets transmitted.
PADT Rx	The number of PADT packets received.
PADT Tx	The number of PADT packets transmitted.

PPP Link Management

Link management has been added to PPP interfaces to allow users to control the connection time and/or data throughput for a PPP interface. For example, a user with an Internet connection via an Internet Service Provider (ISP) can limit the amount of data transmitted over the PPP interface, or the total connection time, to prevent their ISP bill from exceeding some threshold they have set for themselves.

Counters record cumulative input and output data throughput, and up-time, for each PPP link. The user can set thresholds for these parameters, and if any of the thresholds are exceeded, the link is closed and prevented from reopening until the counters are cleared, the threshold limits increased, or the threshold limits are disabled. On AR100 Series routers the *Call Alert* LED will flash when the thresholds are exceeded.

The router writes the accumulated counters to FLASH memory every five minutes and every time the PPP link is brought down. If the router is restarted, the counters are restored from FLASH.

New log messages have been added to record when thresholds are exceeded, and when attempts are made to open the PPP connection after a threshold has been exceeded (Table 15 on page 20).

Table 15: New log messages for PPP link management .

Type/SubType	Severity	Message Format/Description
VINT/DOWN	INFO	ppp<n>: link closed due to <limit> being exceeded. The specified limit ("ONLINELIMIT", "INDATALIMIT", "OUTDATALIMIT" or "TOTALDATALIMIT") for the PPP interface has been exceeded and the PPP connection has been closed.
VINT/ERROR	NOTICE	ppp<n>: open attempt rejected due to on-line or data limit thresholds being exceeded. An attempt was made to open the PPP connection after one of the thresholds has been exceeded. The attempt was rejected.

The CREATE PPP, CREATE PPP TEMPLATE, SET PPP and SET PPP TEMPLATE commands have been modified to support link management:

```
CREATE PPP=ppp-interface OVER=physical-interface
  [INDATALIMIT={NONE|1..65535}]
  [ONLINELIMIT={NONE|1..65535}]
  [OUTDATALIMIT={NONE|1..65535}]
  [TOTALDATALIMIT={NONE|1..65535}] [other-options]...

SET PPP [=ppp-interface] [INDATALIMIT={NONE|1..65535}]
  [ONLINELIMIT={NONE|1..65535}]
  [OUTDATALIMIT={NONE|1..65535}]
  [TOTALDATALIMIT={NONE|1..65535}] [other-options]...

CREATE PPP TEMPLATE=template [INDATALIMIT={NONE|1..65535}]
  [ONLINELIMIT={NONE|1..65535}]
  [OUTDATALIMIT={NONE|1..65535}]
  [TOTALDATALIMIT={NONE|1..65535}] [other-options]...

SET PPP TEMPLATE=template [INDATALIMIT={NONE|1..65535}]
  [ONLINELIMIT={NONE|1..65535}]
  [OUTDATALIMIT={NONE|1..65535}]
  [TOTALDATALIMIT={NONE|1..65535}] [other-options]...
```

The ONLINELIMIT parameter specifies the up-time threshold, in hours, for the PPP interface. Once the interface's cumulative up-time counter has exceeded this limit, the link is closed and any further attempts to open this connection will fail. If the up-time counter for the interface is cleared the link can be re-opened. The default is NONE which sets no threshold.

The INDATALIMIT parameter specifies the input data threshold, in megabytes, for the PPP interface. Once the interface's cumulative input data counter has exceeded this limit, the link is closed and any further attempts to open this connection will fail. If the input data counter for the interface is cleared the link can be re-opened. The default is NONE which sets no threshold.

The OUTDATALIMIT parameter specifies the output data threshold, in megabytes, for the PPP interface. Once the interface's cumulative output data counter has exceeded this limit, the link is closed and any further attempts to open this connection will fail. If the output data counter for the interface is cleared the link can be re-opened. The default is NONE which sets no threshold.

The TOTALDATALIMIT parameter specifies the total data throughput threshold, in megabytes, for the PPP interface. Once the interface's cumulative total data counter has exceeded this limit, the link is closed and any further attempts to open this connection will fail. If the total data counter for the interface is cleared the link can be re-opened. The default is NONE which sets no threshold.

The RESET PPP command has been modified to allow the cumulative input data, output data up-time counters to be reset to zero (0):

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

A new command:

```
SHOW PPP [=ppp-interface] LIMITS
```

has been added to display the cumulative counters and the thresholds (Figure 15 on page 21, Table 16 on page 21)

Figure 15: Example output from the SHOW PPP LIMITS command.

Name		Current	Limit	Remaining

ppp0	Up Time	16:12	25 hrs	08:47
	In Data	EXCEEDED	50 MB	0.0 MB
	Out Data	21.5 MB	Unlimited	--
	Total Data	71.5 MB	Unlimited	--

Table 16: Parameters displayed in the output of the SHOW PPP LIMITS command.

Parameter	Meaning
Name	The name of the PPP interface.
Up-Time	The up-time information, in hours, for the interface.
In Data	The input data throughput information, in megabytes, for the interface.
Out Data	The output data throughput information, in megabytes, for the interface.
Total Data	The total data throughput information, in megabytes, for the interface.
Current	The current value of the cumulative counter, or "EXCEEDED" if the counter has exceeded the corresponding threshold limits.
Limit	The threshold limits for the interface, or "Unlimited" if no limit has been set.
Remaining	The remaining time or data throughput allowed before the limit is exceeded and the link closed.

Integrated Services Digital Network (ISDN)

The command:

```
SHOW BRI STATE
```

now displays the f the higher layer module(s) using the B1 and B2 channels, and for non-voice calls, the protocol in use (HDLC or transparent). The *B1/B2 enabled* field has been replaced by the *B1/B2 channel user* field (Figure 16 on page 22, Table 17 on page 22).

Figure 16: Example output from the SHOW BRI STATE command.

```
State for BRI instance 0:

Interface type ..... TE
State ..... Activated
Rx INFO ..... INFO 4
Tx INFO ..... INFO 3
Activate request ... no
Activated ..... yes
Synchronised ..... yes
Activation mode .... normal
Mode ..... mixed
ISDN slots ..... B1
TDM slots ..... B2
D channel class .... high
B1 channel user..... PBX
B2 channel user..... PPP HDLC
B1, B2 aggregated... no
Rx multiframing .... no
Transceiver mask .. 55
```

Table 17: Changed fields in the output of the SHOW BRI STATE command.

Parameter	Meaning
B1/B2 channel user	The name of the higher layer module using the channel (or "none" if no higher layer module is using the channel), and for non-voice calls the layer 1 protocol in use (one of "HDLC" or "transparent").

X.25

Software Release 1.9.3 adds enhancements to both LAPB and DCE mode operation, including:

- A maximum Layer 2 (LAPB) frame size of 4099 bytes.
- A new range for the Layer 2 (LAPB) T1 timer of 500ms to 10000ms.
- A maximum Layer 3 (X.25) packet size of 4096 bytes.
- The ability to set the Layer 3 (X.25) default through-put class, default packet size and default window size.
- Options for selecting logical channels for incoming, outgoing and two-way calls.
- Options for negotiating through-put class, packet size and window size.

LAPB (Layer 2)

LAPB now supports a maximum frame length of 4099 bytes (32792 bits) and an additional T1 timer range of 500–10000ms. The CREATE LAPB and SET LAPB commands have been modified to support these new features:

```
CREATE LAPB=lapb-interface OVER={SYNn|ISDN-callname}
  [DOD={ON|OFF|YES|NO}] [MODULUS={8|128}] [ROLE={DCE|DTE}]
  [MAXDATA=1080..32792] [WINDOW=1..127]
  [T1={1..120|500..10000}] [T3=3..120] [N2=1..40]

SET LAPB=lapb-interface [MODULUS={8|128}] [ROLE={DCE|DTE}]
  [MAXDATA=1080..32792] [WINDOW=1..127]
  [T1={1..120|500..10000}] [T3=3..120] [N2=1..40]
```

The MAXDATA parameter specifies the maximum LAPB frame length, in bits, that the router will use or expect in a LAPB frame. The default value is 2072.

The T1 parameter specifies the time, in seconds or milliseconds, for the T1 timer associated with the LAPB interface. Timer T1 is used to prevent frames from being lost by the LAPB interface. The timer period should be longer than the maximum time delay between transmission of a frame and reception of its acknowledgement. When this timer expires retransmission of the unacknowledged frame will occur. If the value specified is in the range 1 to 120, it is assumed to be in units of seconds. If the value specified is in the range 500 to 10000, it is assumed to be in units of milliseconds. The default is 2000.

The T3 parameter specifies the time, in seconds, the T3 timer associated with the LAPB interface. Timer T3 is used as a watchdog to check that the line is still active after a period of T3 seconds with no frames being exchanged. The default is 40.

X.25 DCE Mode (Layer 3)

X.25 in DCE mode now supports a maximum packet length of 4096 bytes. Previously the maximum supported packet size was 1024 bytes.

The default through-put class, default packet size and default window size can now be set via the command line. The default settings must be the same on all routers in the X.25 network. A router will refuse a *Call Request* if its settings differ from those proposed by the calling router.

Prior to Software Release 1.9.3, logical channel numbers for incoming, outgoing and two-way calls were specified as single *Logical Channel Number* (LCN) in the range 0 to 4096. Logical channel numbers are now specified by a pair of numbers—a *Logical Channel Group Number* (LCGN) in the range 0 to 15, and a *Logical Channel Number* (LCN) within the LCGN in the range 0 to 128. LCN 0 is reserved and can not be used.

The router will now attempt to negotiate the through-put class, packet size, and window size.

The router will now pass through packets with the GFI field (Qbit, Dbit, Mbit) in the X.25 header set to 1. IT and IF packets are passed through, once the X.25 packet link is established.

The CREATE X25C and SET X25C commands have been modified to support these new features:

```

CREATE X25C=x25-interface OVER=LAPBn
  [DEFPKT={128|256|512|1042|2048|4096}]
  [DEFTHROUGH={75|150|300|600|1200|2400|4800|9600}]
  [DEFWIN=0..7] [INLCGN=0..15] [INLCN=0..128]
  [MAXACTIVE=0..128] [OUTLCGN=0..15] [OUTLCN=0..128]
  [PACKETSIZE={ON|OFF}] [THROUGHPUT={ON|OFF}]
  [TWOLCGN=0..15] [TWOLCN=0..128] [WINDOW={ON|OFF}]

SET X25C=x25-interface [DEFPKT={128|256|512|1042|2048|4096}]
  [DEFTHROUGH={75|150|300|600|1200|2400|4800|9600}]
  [DEFWIN=0..7] [INLCGN=0..15] [INLCN=0..128]
  [MAXACTIVE=0..128] [OUTLCGN=0..15] [OUTLCN=0..128]
  [PACKETSIZE={ON|OFF}] [THROUGHPUT={ON|OFF}]
  [TWOLCGN=0..15] [TWOLCN=0..128] [WINDOW={ON|OFF}]

```

The parameters INCOMING, OUTGOING and TWOWAY have been obsoleted and replaced by INLCGN, INLCN, OUTLCGN, OUTLCN, TWOLCGN and TWOLCN.

The INLCGN parameter specifies the Logical Channel Group Number (LCGN) for incoming calls on the X.25 DCE interface. The value must be unique; the same LCGN can not be used for outgoing or two-way calls. The default is 0.

The INLCN parameter specifies the maximum number of active channels permitted for incoming calls on the X.25 DCE interface. LCN 0 is reserved. If INLCN is set to zero, no channels are available for incoming calls. Setting INLCN to n allocates LCNs 1 to n for incoming calls.

The OUTLCGN parameter specifies the Logical Channel Group Number (LCGN) for outgoing calls on the X.25 DCE interface. The value must be unique; the same LCGN can not be used for incoming or two-way calls. The default is 0.

The OUTLCN parameter specifies the maximum number of active channels permitted for outgoing calls on the X.25 DCE interface. LCN 0 is reserved. If OUTLCN is set to zero, no channels are available for outgoing calls. Setting OUTLCN to n allocates LCNs 1 to n for outgoing calls.

The TWOLCGN parameter specifies the Logical Channel Group Number (LCGN) for two-way calls on the X.25 DCE interface. The value must be unique; the same LCGN can not be used for incoming or outgoing calls. The default is 0.

The TWOLCN parameter specifies the maximum number of active channels permitted for two-way calls on the X.25 DCE interface. LCN 0 is reserved. If TWOLCN is set to zero, no channels are available for two-way calls. Setting TWOLCN to n allocates LCNs 1 to n for two-way calls.

The DEFPKT parameter sets the default packet size for the X.25 DCE interface. The default is 128.

The DEFTHROUGH parameter sets the default through-put class for the X.25 DCE interface. The default is 9600.

The DEFWIN parameter sets the default window size for the X.25 DCE interface. The default is 2.

The PACKETSIZE parameter specifies whether or not packet size negotiation is enabled or disabled. The default is OFF.

The THROUGHPUT parameter specifies whether or not through-put class negotiation is enabled or disabled. The default is OFF.

The WINDOW parameter specifies whether or not window size negotiation is enabled or disabled. The default is OFF.

The SHOW X25C command has been modified to display the new parameters (Figure 17 on page 25, Table 18 on page 25).

Figure 17: Example output from the SHOW X25C command.

```

X.25 DCE Interfaces
-----
X.25 DCE interface 0
Over ..... LAPB0
Max active channels ... 24
Incoming channels
  LCGN ..... 0
  Number of channels ... 8
Two way channels
  LCGN ..... 1
  Number of channels ... 8
Outgoing channels
  LCGN ..... 2
  Number of channels ... 8
-----

```

Table 18: Parameters displayed in the output of the SHOW X25C command.

Parameter	Meaning
X.25 DCE Interface	The number of the X.25 DCE logical interface.
Over	The layer 2 entity used by this X.25 DCE interface.
Max active channels	The maximum allowed active channels for the interface.
Incoming channels	Information about channels reserved for incoming calls.
Two way channels	Information about channels reserved for two-way calls.
Outgoing channels	Information about channels reserved for outgoing calls.
LCGN	The Logical Channel Group Number for the associated incoming, two-way or outgoing calls.
Number of channels	The number of call channels reserved for the associated incoming, two-way or outgoing calls.

The command:

```
SHOW X25C=x25-interface STATE
```

has been added to display status information for the LCNs on the X25C interface (Figure 18 on page 26, Table 19 on page 26).

Figure 18: Example output from the SHOW X25C STATE command.

LCGN	LCN	State	PktSize		WinSize		Throughput	
			Tx	Rx	Tx	Rx	Tx	Rx
0	1	OPEN	4096	4096	2	2	9600	9600
0	2	CR-WAIT	-	-	-	-	-	-
1	1	CR-WAIT	-	-	-	-	-	-
1	2	OPEN	256	512	3	5	2400	4800

Table 19: Parameters displayed in the output of the SHOW X25C STATE command.

Parameter	Meaning
LCGN	The Logical Channel Group Number.
Number of channels	The Logical Channels Number.
State	The state of the X.25 DCE logical interface; one of "OPEN", "CR-WAIT", "CA-WAIT", "CQ-WAIT" or "CI-WAIT".
PktSize Tx/Rx	The maximum packet size for the transmit (Tx) and receive (Rx) directions, when the <i>State</i> field is set to "OPEN".
WinSize Tx/Rx	The window size for the transmit (Tx) and receive (Rx) directions, when the <i>State</i> field is set to "OPEN".
Throughput Tx/Rx	The through-put class for the transmit (Tx) and receive (Rx) directions, when the <i>State</i> field is set to "OPEN".

The command:

```
SHOW X25C=x25-interface COUNTER
```

has been added to display counters for the X25C interface (Figure 19 on page 26, Table 20 on page 27).

Figure 19: Example output from the SHOW X25C COUNTER command.

```

X25C-0 Counters

inSQ ..... 0      outSI ..... 0
inSF ..... 0      outSF ..... 0
inCR ..... 0      outCN ..... 0
inCA ..... 0      outCC ..... 0
inCQ ..... 0      outCI ..... 0
inCF ..... 0      outCF ..... 0
inRQ ..... 0      outRI ..... 0
inRF ..... 1      outRF ..... 0
inIT ..... 0      outIT ..... 0
inIF ..... 0      outIF ..... 0

Open Calls ..... 0      Discard Calls ..... 0
    
```

Table 20: Parameters displayed in the output of the SHOW X25C COUNTER command.

Parameter	Meaning
inSQ	The number of <i>Restart Request</i> messages received from the DTE.
inSF	The number of <i>Restart Confirmation</i> messages received from the DTE.
inCR	The number of <i>Call Request</i> messages received from the DTE.
inCA	The number of <i>Call Accepted</i> messages received from the DTE.
inCQ	The number of <i>Clear Request</i> messages received from the DTE.
inCF	The number of <i>Clear Confirmation</i> messages received from the DTE.
inRQ	The number of <i>Reset Request</i> messages received from the DTE.
inRF	The number of <i>Reset Confirmation</i> messages received from the DTE.
inIT	The number of <i>Interrupt</i> messages received from the DTE.
inIF	The number of <i>Interrupt Confirmation</i> messages received from the DTE.
outSI	The number of <i>Restart Indication</i> messages sent to the DTE.
outSF	The number of <i>Restart Confirmation</i> messages sent to the DTE.
outCN	The number of <i>Incoming Call</i> messages sent to the DTE.
outCC	The number of <i>Call Connected</i> messages sent to the DTE.
outCI	The number of <i>Clear Indication</i> messages sent to the DTE.
outCF	The number of <i>Clear Confirmation</i> messages sent to the DTE.
outRI	The number of <i>Restart Indication</i> messages sent to the DTE.
outRF	The number of <i>Restart Confirmation</i> messages sent to the DTE.
outIT	The number of <i>Interrupt</i> messages sent to the DTE.
outIF	The number of <i>Interrupt Confirmation</i> messages sent to the DTE.
Open Calls	The number of calls that were successful (reached the OPEN state).
Discard Calls	The number of calls disconnected by the router.

The commands:

```
ENABLE X25C=x25-interface DEBUG
```

```
DISABLE X25C=x25-interface DEBUG
```

have been added to enable and disable debugging on the X25C interface. When debugging is enabled for an X25C interface, packet traces for all packets sent and received on all LCNs on the interface are displayed on the terminal from which the command was entered. Debugging is disabled by default.

Internet Protocol (IP)

A number of new features have been added to IP routing, including:

- Configuring IP interfaces with DHCP
- Relaying DNS requests
- Support for a Secondary Nameserver

Configuring IP Interfaces with DHCP

The ADD IP INTERFACE and SET IP INTERFACE commands have been modified to allow IP interfaces to be configured using DHCP:

```
ADD IP INTERFACE=interface IPADDRESS={ipadd|DHCP}
[BROADCAST={0|1}] [DIRECTEDBROADCAST={YES|NO|ON|OFF}]
[FILTER={0..99|NONE}] [FRAGMENT={YES|NO}]
[GRE={0..100|NONE}] [MASK=ipadd] [METRIC=1..16]
[MULTICAST={OFF|SEND|RECEIVE|BOTH|ON}]
[OSPFMETRIC=1..65534] [POLICYFILTER={100..199|NONE}]
[PRIORITYFILTER={200..299|NONE}] [PROXYARP={ON|OFF}]
[RIPMETRIC=1..16] [SAMODE={BLOCK|PASSTHROUGH}]
[VJC={ON|OFF}]

SET IP INTERFACE=interface [BROADCAST={0|1}]
[DIRECTEDBROADCAST={YES|NO|ON|OFF}] [FILTER={0..99|NONE}]
[FRAGMENT={YES|NO}] [GRE={0..100|NONE}]
[IPADDRESS={ipadd|DHCP}] [MASK=ipadd] [METRIC=1..16]
[MULTICAST={OFF|SEND|RECEIVE|BOTH|ON}]
[OSPFMETRIC=1..65534] [POLICYFILTER={100..199|NONE}]
[PRIORITYFILTER={200..299|NONE}] [PROXYARP={ON|OFF}]
[RIPMETRIC=1..16] [SAMODE={BLOCK|PASSTHROUGH}]
[VJC={ON|OFF}]
```

The IPADDRESS parameter now accepts either a static IP address in dotted decimal notation or the keyword DHCP:

```
IPADDRESS={ipadd|DHCP}
```

If DHCP is specified, the router will act as a DHCP client and obtain the configuration of the IP interface via DHCP. Table 21 on page 28 lists the parameters from the DHCP reply used by the router.

Table 21: DHCP reply parameters used by the router for configuring IP .

DHCP Parameter	Purpose
IP address and mask	The IP address and subnet mask for the IP interface.
DNS Servers	DNS server addresses are added to the list of IP name servers. A primary name server and a secondary name server are supported. Name servers are normally added manually using the SET IP NAMESERVER and SET IP SECONDARYNAMESERVER commands.
Gateway	A default route is added over the specified interface with the next hop set to the gateway address. If a default route does already exist on the router, the gateway parameter in the DHCP reply is ignored.

If an IP interface is set to use DHCP to obtain its configuration, the interface will not take part in IP routing until the IP address has been set by DHCP.

There is no change to the output of the SHOW IP INTERFACE command. For an interface configured using DHCP, the IP Address and Network Mask fields will show the values assigned by DHCP, or 0.0.0.0 if a DHCP reply has not yet been received.

NOTE: Remote address assignment must be enabled using the ENABLE IP REMOTEASSIGN command before IP interfaces will accept addresses remotely assigned by DHCP.

Support for a Secondary Nameserver

Support has been added for a secondary name server. The primary name server is specified using the command:

```
SET IP NAMESERVER=ipadd
```

A new command has been added to allow a secondary name server to be specified:

```
SET IP SECONDARYNAMESERVER=ipadd
```

When the router performs a DNS lookup, it firsts sends the request to the primary name server. If a response is not received within 20 seconds the request is sent to the secondary name server.

The SHOW IP command has been modified to display the primary and secondary name servers. One field, *Secondary Name Server*, has been added (Figure 21 on page 31, Table 22 on page 31).

Relaying DNS Requests

A DNS relay facility has been added to enable the router to receive DNS requests from hosts and forward them on to the router's own configured DNS server.

A typical application is configuring PCs on the local LAN using DHCP. The PCs are configured to use DHCP to obtain their IP address, subnet mask, DNS server address and gateway address. The router is configured as a DHCP server and specifies its own IP address as the DNS server address. DNS relay is enabled and DNS requests from the local PCs are relayed to the router's own DNS server.

DNS relay is disabled by default, and can be explicitly enabled or disabled using the commands:

```
ENABLE IP DNSRELAY
```

```
DISABLE IP DNSRELAY
```

DNS requests are forwarded to the router's own DNS server. The DNS server's address can be set using the command:

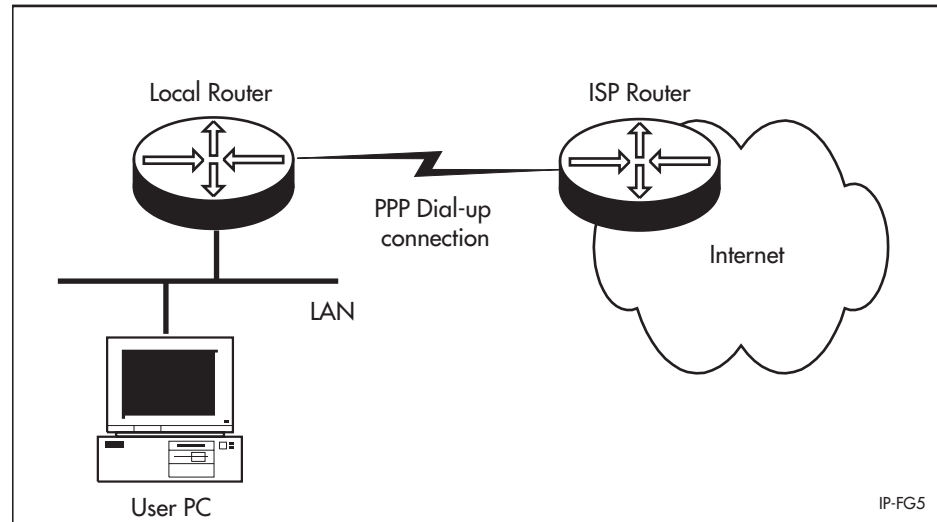
```
SET IP NAMESERVER=ipadd
```

If a DNS server has not been set using the SET IP NAMESERVER command, the router can learn the address of a remote DNS server using PPP IPCP negotiation. The command:

```
SET IP DNSRELAY INTERFACE={interface|NONE}
```

specifies the PPP interface used to learn the DNS server address. Typically this PPP interface would be a dial-up connection to an ISP that provides the DNS name server PPP option. For example, a local router acting as a DNS relay for connecting a PC to the Internet (see Figure 20 on page 30).

Figure 20: Local router acting as a DNS relay for an Internet connection.



If the PPP interface is already up when the DNS request is received from the host, and a DNS server address was not set during IPCP negotiation, the DNS request will be discarded. If the PPP interface is down, the interface will be activated and IPCP negotiation will be used to learn the DNS server address. If a DNS server address is learnt as a result of the IPCP negotiation, the DNS request is forwarded to that address. Otherwise the DNS request is discarded.

To disable the learning of DNS server addresses via IPCP, use the command:

```
SET IP DNSRELAY INTERFACE=NONE
```

NOTE: If a DNS server address has been statically defined using the SET IP NAMESERVER command, and a PPP interface learns a new DNS server address via IPCP negotiation, the learned DNS server address replaces the static DNS server address while the PPP interface is up. When the PPP interface goes down, the statically defined DNS server address is restored.

Note that from the ISP's point of view, the ISP router can be configured to offer a specific DNS server address to the local router using the commands:

```
SET PPP DNSPRIMARY=ipadd DNSSECONDARY=ipadd
```

The SHOW IP command has been modified to include the status of the DNS relay facility. One field, *DNS Relay*, has been added (Figure 21 on page 31, Table 22 on page 31).

Figure 21: Example output from the SHOW IP command.

```

IP Module Configuration
-----

Module Status ..... Enabled
IP Packet Forwarding ..... Enabled
IP Echo Reply ..... Enabled
Debugging ..... Disabled
IP Fragment Offset Filtering ... Enabled
Name Server ..... 192.168.11.5 (ppp0)
Secondary Name Server ..... Not Set
Source-Routed Packets ..... Discarded
Remote IP address assignment ... Disabled
DNS Relay ..... Disabled

Routing Protocols

RIP Neighbours ..... 1
EGP Status ..... Disabled
EGP Autonomous System Number ... Not Set
Transfer RIP to EGP ..... Disabled
OSPF Status ..... Disabled

Active Routes

Static ..... 0
Interface ..... 1
RIP ..... 4
EGP ..... 0
OSPF ..... 0
Other ..... 0

IP Filter Configuration

Total filters ..... 0

Dynamic Interfaces ..... 0

```

Table 22: New fields in the output of the SHOW IP command.

Parameter	Meaning
Name Server	The IP address of the primary name server, or "Not Set" if a secondary name server is not assigned. If the address was learnt using IPCP negotiation, the name of the interface used for the IPCP negotiation is also displayed.
Secondary Name Server	The IP address of the secondary name server, or "Not Set" if a secondary name server is not assigned. If the address was learnt using IPCP negotiation, the name of the interface used for the IPCP negotiation is also displayed.
DNS Relay	Whether or not the DNS relay facility is enabled; one of "Enabled" or "Disabled".

Support for a Secondary Nameserver

Support has been added for a secondary name server. The primary name server is specified using the command:

```
SET IP NAMESERVER=ipadd
```

A new command has been added to allow a secondary name server to be specified:

```
SET IP SECONDARYNAMESERVER=ipadd
```

When the router performs a DNS lookup, it firsts sends the request to the primary name server. If a response is not received within 20 seconds the request is sent to the secondary name server.

The SHOW IP command has been modified to display the primary and secondary name servers. One field, *Secondary Name Server*, has been added (Figure 21 on page 31, Table 22 on page 31).

Open Shortest Path First (OSPF)

Software Release 1.9.3 adds support for control over the creation of OSPF stub network links when numbered Point-to-Point (PTP) links are activated. The SET OSPF command has been modified to support this new feature:

```
SET OSPF [ASEXTERNAL={ON|OFF}]
        [DEFROUTE={ON|OFF|TRUE|FALSE|YES|NO} [TYPE={1|2}]
        [METRIC=0..16777215]]
        [DYNINTERFACE={STUB|ASEXTERNAL|NONE|NO|OFF|FALSE}]
        [RIP={OFF|EXPORT|IMPORT|BOTH}] [ROUTERID=ipadd]
        [PTPSTUB={ON|OFF|YES|NO|TRUE|FALSE}]
```

The PTPSTUB parameter controls the creation of stub network links. The OSPF RFC states that whenever a numbered point to point link comes up, a stub network to the other end of the link should be added. Each stub network adds an extra link to the router's LSA. The extra link has no useful purpose, but does increase the LSA size. To limit the LSA size in cases where there are many numbered point to point links, it may be desirable to stop generating stub networks. The default is TRUE, which means stub network links are created.



If PTPSTUB is set to FALSE, the router is not strictly compliant with the OSPF RFC, but the non-compliance is minor and will not cause any problems.

One new field, *PTP stub network generation*, has been added to the SHOW OSPF command to display the state of the PTPSTUB parameter (Figure 22 on page 33, Table 23 on page 33).

Figure 22: Example output from the SHOW OSPF command.

```

Router ID ..... 123.234.143.231
OSPF module status ..... Enabled
Area border router status ..... Yes
AS border router status ..... Disabled
PTP stub network generation ..... Enabled
External LSA count ..... 10234
External LSA sum of checksums ... 1002345623
New LSAs originated ..... 10345
New LSAs received ..... 34500
RIP ..... Off
Dynamic interface support ..... None
Number of active areas ..... 10
Logging ..... Disabled
Debugging ..... Disabled
AS external default route:
  Status ..... Disabled
  Type ..... 1
  Metric ..... 1

```

Table 23: New fields in the output of the SHOW OSPF command.

Parameter	Meaning
PTP stub network generation	Whether or not stub network links are created when numbered point-to-point links come up; one of "Enabled" or "Disabled".

The SHOW OSPF LSA command has been modified to display the length of each LSA. A new field, *Len*, has been added (Figure 23 on page 33, Table 24 on page 34).

Figure 23: Example output from the SHOW OSPF LSA SUMMARY command.

Type	LS ID	Router ID	Sequence	Age	Len	Csum

Area 0.0.0.0:						
Router	172.28.2.8	172.28.2.8	80000001	401	36	cd27
Summary	172.30.0.0	172.28.2.8	80000001	384	28	fcd2
Area 0.0.0.1:						
Router	172.28.2.8	172.28.2.8	800000a6	381	36	482b
Router	172.28.2.9	172.28.2.9	80000096	392	36	de4a
Router	172.28.10.4	172.28.10.4	80000093	387	36	aadc
Summary	172.28.0.0	172.28.2.8	80000024	391	28	c6ea
External:						
AsExternal	0.0.0.0	172.28.2.8	80000001	383	36	b1d4
AsExternal	172.16.0.0	172.28.2.8	80000001	383	36	4741
AsExternal	172.20.0.0	172.28.2.8	80000001	383	36	e644
AsExternal	172.21.0.0	172.28.2.8	80000001	383	36	da4f
AsExternal	172.23.0.0	172.28.2.8	80000001	383	36	ff1
AsExternal	172.24.0.0	172.28.2.8	80000001	383	36	72d9
AsExternal	172.26.0.0	172.28.2.8	80000001	383	36	218f
AsExternal	172.27.0.0	172.28.2.8	80000001	383	36	ba6d

Table 24: New fields in the output of the SHOW OSPF LSA SUMMARY command.

Parameter	Meaning
Len	The length of the LSA in bytes, including the 20 byte LSA header.

Bridging

Previous software releases have supported the filtering of frames based on information in the frame header, including source and destination address, encapsulation and frame type. Software Release 1.9.3 adds support for filtering frames based on the content of the data portion of the frame. Two new parameters, OFFSET and DATA, have been added to the ADD BRIDGE FILTER and SET BRIDGE FILTER commands:

```
ADD BRIDGE FILTER=1..99 [ENTRY=entry] [SADDRESS<sep1>macadd
[SMASK=macadd] [DADDRESS<sep1>macadd [DMASK=macadd]]
[ENCAPSULATION<sep1>{802|ETHII|SNAP|NOVELL}]
[DISCRIMINATOR<sep1>protocoltype]] [SIZE<sep2>1..65535]
[OFFSET=1..1500 DATA<sep1>datastring]
[TYPE<sep1>{UNICAST|MULTICAST|BROADCAST|ANY}]
PORTS={ALL|NONE|1..32[,1..32]...}

SET BRIDGE FILTER=1..99 ENTRY=entry [SADDRESS<sep1>macadd
[SMASK=macadd] [DADDRESS<sep1>macadd [DMASK=macadd]]
[ENCAPSULATION<sep1>{802|ETHII|SNAP|NOVELL}]
[DISCRIMINATOR<sep1>protocoltype]] [SIZE<sep2>1..65535]
[OFFSET=1..1500 DATA<sep1>datastring]
[TYPE<sep1>{UNICAST|MULTICAST|BROADCAST|ANY}]
PORTS={ALL|NONE|1..32[,1..32]...}
```

The OFFSET parameter specifies the offset into the user data portion of the frame where checking is to start. The first octet in the user data portion is at offset 1.

The DATA parameter specifies up to 16 bytes of data, as a hexadecimal string, to match against the contents of the frame, starting at the offset given by the OFFSET parameter. The operators "=" and "!=" can be used to test whether the data matches or does not match the contents of the frame.

For example, the following set of commands creates a filter for Novell broadcasts:

```
ADD BRIDGE FILTER=1 DADDR=ff-ff-ff-ff-ff-ff ENCAP=novell
OFFSET=47 DATA!=41 PORT=NONE

ADD BRIDGE FILTER=1 DADDR=ff-ff-ff-ff-ff-ff ENCAP=novell
OFFSET=45 DATA=0104 PORT=NONE

ADD BRIDGE FILTER=1 PORT=ALL

ADD BRIDGE PORT=1 INTERFACE=ETH0

SET BRIDGE PORT=1 FILTER=1
```

In this example an explicit filter has been added at the end of the list to pass all traffic, otherwise anything not found in the filter would be discarded.

The SHOW BRIDGE FILTER command has been modified to display the new filter options. Two new fields, *Data Offset* and *Data Pattern*, have been added (Figure 24 on page 35, Table 25 on page 35).

Figure 24: Example output from the SHOW BRIDGE FILTER command.

```

Bridge filters
-----
Filter ..... 1
Used by ports ..... None
Frames seen ..... 37465
Frames passed ..... 4938
Frames unmatched ... 2652
Frames dropped ..... 32527

Entry ..... 1
Source address ..... = 00-00-cd-00-00-00/ff-ff-ff-00-00-00
Dest address ..... Match any
Protocol ..... = ETHII, = 0800
Size ..... Match any
Multicast types ..... Match any
Output ports ..... 1,2
Matches ..... 4938
Entry ..... 2
Source address ..... Match any
Dest address ..... Match any
Protocol ..... = ETHII
Size ..... Match any
Multicast types ..... Match any
Data Offset ..... 27
Data Pattern ..... = 345678
Output ports ..... None
Matches ..... 29875
-----

```

Table 25: New fields in the output of the SHOW BRIDGE FILTER command.

Parameter	Meaning
Data Offset	The offset in the data field of the DATA condition specified in the Data Pattern field.
Data Pattern	The condition for the data in the data field starting at the position specified in the Data Offset field.

Firewall

Software Release 1.9.3 adds support for dynamic interfaces to the Nemesis Firewall through the use of dynamic interface templates.

In previous releases, only static interfaces could be managed by the firewall because the interfaces to be managed had to be assigned to the firewall by name, and dynamic interface names are not known in advance.

Software Release 1.9.3 adds support for dynamic interfaces through the use of dynamic interface templates. A dynamic interface template is used as a placeholder for the addition of dynamic interfaces to policies, NAT entries and rules wherever an interface name is required.

A dynamic interface template is added to or removed from a firewall policy using the commands:

```
CREATE FIREWALL POLICY=policy-name DYNAMIC=template-name
DESTROY FIREWALL POLICY=policy-name DYNAMIC=template-name
```

Users are then assigned to the dynamic interface template, either individually, using the command:

```
ADD FIREWALL POLICY=policy-name DYNAMIC=template-name
USER=username
```

or by specifying a text file containing a list of usernames, one per line:

```
ADD FIREWALL POLICY=policy-name DYNAMIC=template-name
FILE=filename.txt
```

A single username can be deleted from a dynamic interface template, or all the users specified in a file can be deleted using the commands:

```
DELETE FIREWALL POLICY=policy-name DYNAMIC=template-name
USER=username
DELETE FIREWALL POLICY=policy-name DYNAMIC=template-name
FILE=filename.txt
```

When a dynamic interface is created by an incoming call, the username used to authenticate the incoming call is checked against the usernames assigned to each dynamic interface template. If a match is found, the dynamic interface inherits all the firewall attributes, such as NATs and rules, of the corresponding dynamic interface template.

Users are globally assigned to policies and dynamic interface templates. A single username can only be assigned to one firewall dynamic interface template or policy. Two special usernames are reserved, NONE and ANY. The username NONE is used to specify dynamic interfaces that do not require authentication. The ANY username is used to match all authentication usernames. This allows the one catch-all for all authenticated usernames.

Once a dynamic interface template has been created, and usernames have been assigned to it, the dynamic interface template can be used as an interface to add interfaces to policies, NATs and rules. The value “*DYN-template-name*” is used to identify the interface as a dynamic interface template, rather than a static interface.

Dynamic interfaces are added to or removed from firewall policies using the commands:

```
ADD FIREWALL POLICY=policy-name INTERFACE=dyn-template-name
TYPE={PRIVATE|PUBLIC} [METHOD={DYNAMIC|PASSALL}]
DELETE FIREWALL POLICY=policy-name
INTERFACE=dyn-template-name
```

Dynamic interfaces are added to or removed from rules using the commands:

```
ADD FIREWALL POLICY=policy-name RULE=rule-id
INTERFACE=dyn-template-name other-options...
DELETE FIREWALL POLICY=policy-name RULE=rule-id
```

Dynamic interfaces are added to or removed from NATs using the commands:

```
ADD FIREWALL POLICY=policy-name NAT={ ENHANCED | STANDARD }
    INTERFACE=dyn-template-name [IP=ipadd]
    GBLINTERFACE=interface [GBLIP=ipadd[-ipadd]]

DELETE FIREWALL POLICY=policy-name NAT={ ENHANCED | STANDARD }
    INTERFACE=dyn-template-name GBLINTERFACE=interface
    [IP=ipadd]
```

NOTE: A dynamic interface template can not be added to a global interface in a NAT definition because a dynamic interface is never directly assigned an IP address. A global interface must have a global address, which must be a real globally unique Internet address.

The SHOW FIREWALL POLICY command has been modified to display the dynamic interface templates that have been created for a policy, and the interfaces, NATs and rules using the dynamic interface templates. One new field, *Dynamic Template*, has been added (Figure 25 on page 38, Table 26 on page 38).

Figure 25: Example output from the SHOW FIREWALL POLICY command.

```

Policy : test
  Accounting ..... enabled
  Enabled Logging Options ..... allow denydump
  Enabled Debug Options ..... none
  Enabled IP options ..... none
  Enabled ICMP forwarding ..... ping
  Receive of ICMP PINGS ..... enabled
  Number of Notifications ..... 0
  Number of Deny Events ..... 0
  Number of Allow Events ..... 2
  Number of Active TCP Opens ..... 0
  Number of Active Sessions ..... 2
  Cache Hits ..... 13
  Discarded ICMP Packets ..... 0
  Dynamic Template : accl
  Private Interface : eth0
    Rule ..... 1
      Action ..... allow
      Protocol ..... TCP
      Port ..... 21
      Global Port ..... all
      Days ..... all
  Private Interface : dyn-accl
  Public Interface : ppp0
    Method ..... dynamic
    NAT ..... enhanced
      Method ..... enhanced dynamic
      Private Interface ..... eth0
      Global IP ..... 192.168.15.2
    NAT ..... enhanced
      Method ..... enhanced interface
      Private Interface ..... dyn-accl
      Global IP ..... 192.168.15.2
    Rule ..... 2
      Action ..... allow
      IP ..... 192.168.14.4
      Protocol ..... TCP
      Port ..... 21
      Global IP ..... 192.168.15.2
      Global Port ..... 21
      Days ..... all

```

Table 26: New fields in the output of the SHOW FIREWALL POLICY command.

Parameter	Meaning
Dynamic Template	The name of a dynamic interface template associated with the policy.

Two new optional parameters, DYNAMIC and USER, have been added to the SHOW FIREWALL POLICY command to display the usernames assigned to a dynamic interface template or policy. The command:

```
SHOW FIREWALL POLICY=policy-name DYNAMIC[=template-name]
```

displays a list of the usernames assigned to the specified dynamic interface template or all dynamic interface templates in a policy (Figure 26 on page 39, Table 27 on page 39).

Figure 26: Example output from the SHOW FIREWALL POLICY DYNAMIC command.

```

Policy : test

Dynamic template : acc1
  Filename : fire.txt
    Users : user$qwerty user-jim user-very-long-name usera1
           usera10 usera2

Users : graeme tony

```

Table 27: Parameters displayed in the output of the SHOW FIREWALL POLICY DYNAMIC command.

Parameter	Meaning
Policy	The name of a policy.
Dynamic Template	The name of a dynamic interface template associated with the policy.
File name/Users	The name of a file containing a list of usernames added using the ADD FIREWALL POLICY DYNAMIC FILE command, and the usernames read from the file.
Users	A list of usernames added using the ADD FIREWALL POLICY DYNAMIC USER command.

The command:

```
SHOW FIREWALL POLICY=policy-name USER=[username]
```

displays the specified username or all usernames and the dynamic interface template(s) to which the username(s) are assigned (Figure 27 on page 39, Table 28 on page 39).

Figure 27: Example output from the SHOW FIREWALL POLICY USER command.

```

Policy : test

Dynamic template : acc1
  User : graeme

```

Table 28: Parameters displayed in the output of the SHOW FIREWALL POLICY USER command.

Parameter	Meaning
Policy	The name of a policy.
Dynamic Template	The name of a dynamic interface template associated with the policy.
Users	A list of usernames added using the ADD FIREWALL POLICY DYNAMIC USER command.

IP Security (IPsec)

Software release 1.9.3 adds support for the following IPsec features:

- ISAKMP Extended Authentication (XAUTH), as a means of authenticating remote peers using legacy authentication methods such as RADIUS.
- Processing of ISAKMP Configuration exchanges used by ISAKMP extended authentication to transport authentication information.
- Processing of ISAKMP Informational exchanges, as defined in RFCs 2408 and 2409. Informational exchanges are used to transport *Notify* and *Delete* payloads to ISAKMP peers.
- Process ISAKMP Aggressive exchanges, as defined in RFCs 2408 and 2409. ISAKMP Aggressive Mode is an alternative to ISAKMP Main Mode that requires fewer exchanges.
- Perform RSA signature authentication in Main and Aggressive modes, as defined in RFCs 2408 and 2409.

A number of ISAKMP commands have been modified or added to support these new features.

The ENABLE ISAKMP command has been modified to allow the router to be enabled as a policy server for VPN clients and to allow the UDP port on which ISAKMP sends and receives messages to be specified:

```
ENABLE ISAKMP [LOCALRSAKEY=key-id]  
              [POLICYSERVERENABLED={TRUE | FALSE}]  
              [POLICYFILENAME=filename] [UDPPORT=port]
```

The POLICYSERVERENABLED parameter specifies whether the router will act as a security policy server. If set to TRUE, the router will listen for security policy requests from remote ISAKMP peers. The router will respond by sending the security policy specified by the POLICYFILENAME parameter. The POLICYFILENAME parameter is required and an ISAKMP POLICY for the peer must exist. The default for this parameter is FALSE. This feature is designed for use with the ATI VPN Client for Windows.

POLICYFILENAME parameter specifies the security policy to be sent to remote ISAKMP peers when requested. This parameter must be specified if the POLICYSERVERENABLED parameter is set to TRUE. This feature is designed for use with the ATI VPN Client for Windows.

The UDPPORT parameter specifies the UDP port number on which ISAKMP sends and receives messages. The default is 500.

The CREATE ISAKMP POLICY command has been modified to support the new ISAKMP features, and a new SET ISAKMP POLICY command has been added to allow existing ISAKMP policies to be modified:

```

CREATE ISAKMP POLICY=name PEER={ipadd|ANY}
  [AUTHTYPE={PRESHARED|RSAENCR|RSASIG}]
  [ENCALG={3DES2KEY|3DESINNER|3DESOUTER|DES}]
  [EXPIRYKBYTES=kbytes] [EXPIRYSECONDS=seconds]
  [GROUP={1|2}] [HASHALG={SHA|MD5}] [HYBRIDXAUTH={ON|OFF}]
  [KEY=key-id] [LOCALRSAKEY=key-id] [MODE={MAIN|AGGRESSIVE}]
  [MSGRETRYLIMIT=retry-limit] [MSGTIMEOUT=seconds]
  [PHASE2XCHGLIMIT={NONE|xchg-limit}]
  [PRENEGOTIATE={TRUE|FALSE}] [SENDDELETES={TRUE|FALSE}]
  [SENDNOTIFY={TRUE|FALSE}] [SETCOMMITBIT={TRUE|FALSE}]
  [SRCINTERFACE=interface] [XAUTH={CLIENT|SERVER|NONE}]
  [XAUTHNAME=username] [XAUTHPASSWORD=password]
  [XAUTHTYPE={GENERIC|RADIUS}]

SET ISAKMP POLICY=name [AUTHTYPE={PRESHARED|RSAENCR|RSASIG}]
  [ENCALG={3DES2KEY|3DESINNER|3DESOUTER|DES}]
  [EXPIRYKBYTES=kbytes] [EXPIRYSECONDS=seconds]
  [GROUP={1|2}] [HASHALG={SHA|MD5}] [HYBRIDXAUTH={ON|OFF}]
  [KEY=key-id] [LOCALRSAKEY=key-id] [MODE={MAIN|AGGRESSIVE}]
  [MSGRETRYLIMIT=retry-limit] [MSGTIMEOUT=seconds]
  [PHASE2XCHGLIMIT={NONE|xchg-limit}]
  [PRENEGOTIATE={TRUE|FALSE}] [SENDDELETES={TRUE|FALSE}]
  [SENDNOTIFY={TRUE|FALSE}] [SETCOMMITBIT={TRUE|FALSE}]
  [SRCINTERFACE=interface] [XAUTH={CLIENT|SERVER|NONE}]
  [XAUTHNAME=username] [XAUTHPASSWORD=password]
  [XAUTHTYPE={GENERIC|RADIUS}]

```

The AUTHTYPE parameter specifies the method used to authenticate the ISAKMP peer. If PRESHARED is specified, shared keys will be used. If RSAENCR is specified, RSA encryption will be used. If RSASIG is specified, RSA signatures will be used. The default is PRESHARED.

The ENCALG parameter specifies the ISAKMP encryption algorithm to be used. The default is DES.

The EXPIRYKBYTES parameter specifies the number of kilobytes of data that can be processed by the ISAKMP SA created from this policy before the SA expires and must be re-negotiated. The default is 1000.

The EXPIRYSECONDS parameter specifies the maximum lifetime, in seconds, of the ISAKMP SA created from this policy before the SA expires and must be re-created. The default is 86400.

The GROUP parameter specifies which Diffie-Hellman group is to be used when negotiating session keys. The default is 1.

The HASHALG parameter specifies the ISAKMP hash algorithm to be used. The default is SHA.

The HYBRIDXAUTH parameter specifies whether the hybrid form of extended authentication is to be used. This only applies if the AUTHTYPE parameter is set to RSASIG. The default is OFF.

The LOCALRSAKEY parameter specifies the key identification number of the ENCO Private RSA key to be used to authenticate the local router to the peer. This is only used for authentication types RSAENCR and RSASIG. If no value is specified then the default key specified in the ENABLE ISAKMP command is used.

The MODE parameter specifies whether MAIN or AGGRESSIVE mode is to be used for phase 1. The default is MAIN.

The MSGRETRYLIMIT parameter specifies the number of times an ISAKMP message is retransmitted. The default is 5.

The MSGTIMEOUT parameter specifies the number of seconds between the initial transmission of an ISAKMP message and the first retransmission. Subsequent retransmissions of the message occur at longer intervals. The default is 10 seconds.

The PEER parameter specifies the IP address of the ISAKMP peer. If the ANY parameter is specified then connections from any IPADDRESS will be accepted. If the value ANY is specified for this parameter then connections from any IPADDRESS will be accepted.

The PHASE2XCHGLIMIT parameter specifies the maximum number of phase2 exchanges allowed over an ISAKMP SA created from this policy. The default is NONE.

The POLICY parameter specifies the name of the policy to modify. A policy with the specified name must already exist.

The PRENEGOTIATE parameter specifies whether or not the ISAKMP SA is to be negotiated at startup when the ENABLE ISAKMP command is issued. The default is FALSE.

The SENDDELETES parameter specifies whether delete messages are to be sent. The default is FALSE.

The SENDNOTIFY parameter specifies whether notify status and error messages are to be sent. The default is FALSE.

The SETCOMMITBIT parameter specifies whether the commit bit is to be set when negotiating an ISAKMP SA. The default is FALSE.

The XAUTH parameter specifies whether extended authentication is to be used. If the value SERVER is specified for this parameter the router will initiate the XAUTH exchange. If the value CLIENT is specified then the router will expect an XAUTH request from the remote server. The default is NONE, specifying that extended authentication is not to be used.

The XAUTHNAME parameter specifies the username to be used for extended authentication when acting as the client.

The XAUTHPASSWORD parameter specifies the password to be used for extended authentication when acting as the client.

The XAUTHTYPE parameter specifies what type of authentication is to be used in the extended authentication exchange. The default is GENERIC.

The KEY parameter specifies the key identification number of the ENCO key to be used for authentication of the peer. If AUTHTYPE is set to SHAREDKEY this parameter specifies a GENERAL key shared by both ISAKMP peers. If AUTHTYPE is set to RSAENCR or RSASIG this parameter specifies the RSA Public key of the ISAKMP peer. If no value is specified and AUTHTYPE is set to RSAENCR then a key matching the IPADDRESS of the peer is searched for in the ENCO key database.

The LOCALRSAKEY parameter specifies the key identification number of the private RSA key to be used to authenticate the local router to the peer. This is

only used for authentication types RSAENCR and RSASIG. If no value is specified the default key specified in the ENABLE ISAKMP command is used.

The SRCINTERFACE parameter specifies the local interface to which the policy is attached.

Other Changes

The SET IPSEC POLICY command no longer allows the interface to which the policy is attached to be changed. The INTERFACE parameter is no longer supported:

```
SET IPSEC POLICY=name [ACTION={DENY|IPSEC|PERMIT}]
[BUNDLESPECIFICATION=bundlespecification-id]
[DFBIT={SET|COPY|CLEAR}] [GROUP={1|2}]
[IPROUTETEMPLATE=template-name]
[ISAKMPPOLICY=isakmp-policy-name]
[LADDRESS={ANY|ipadd[-ipadd]}] [LMASK=ipadd]
[LNAME={ANY|system-name}] [LPORT={ANY|OPAQUE|port}]
[PEERADDRESS={ipadd|ANY|DYNAMIC}] [POSITION=pos]
[RADDRESS={ANY|ipadd[-ipadd]}] [RMASK=ipadd]
[RNAME={ANY|system-name}] [RPORT={ANY|port|OPAQUE}]
[TRANSPORTPROTOCOL={ANY|EGP|ESP|GRE|ICMP|OPAQUE|OSPF|RSVP
|TCP|UDP|protocol}] [USEPFSKEY={TRUE|FALSE}]
```

To change the interface to which an IPsec policy is attached, the IPsec policy must be destroyed and then re-created.

The XAUTHNAME and XAUTHPASSWORD parameters of the CREATE ISAKMP POLICY and SET ISAKMP POLICY commands now support usernames and passwords up to 64 characters long.

Other Enhancements

- The maximum number of PPP interfaces, ISDN calls and IP interfaces that can be configured has been increased to 512.
- On AR300 Series and AR100 Series routers with voice ports, the B1 and B2 channel LEDs on the front panel are lit when a voice call is using the respective B channel.

Availability

Software Release 1.9.3 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 (<http://www.alliedtelesyn.co.nz/support/updates/patches.html>).

Software releases must be licenced and require a password to activate. To obtain a licence and password, download a Software Upgrade request form from the Software Updates area of the Allied Telesyn web site (<http://www.alliedtelesyn.co.nz/support/updates/patches.html>), complete the form and fax it along with a company purchase order to Allied Telesyn Sales on +64-3-377 8870, or call Teltrend Customer Service on 0800 808 909.

Software Release 1.9.3 will not be available as an EPROM upgrade.

Installation

There are no issues upgrading from Software Release 1.8.1 to Software Release 1.9.3.