

Release Note

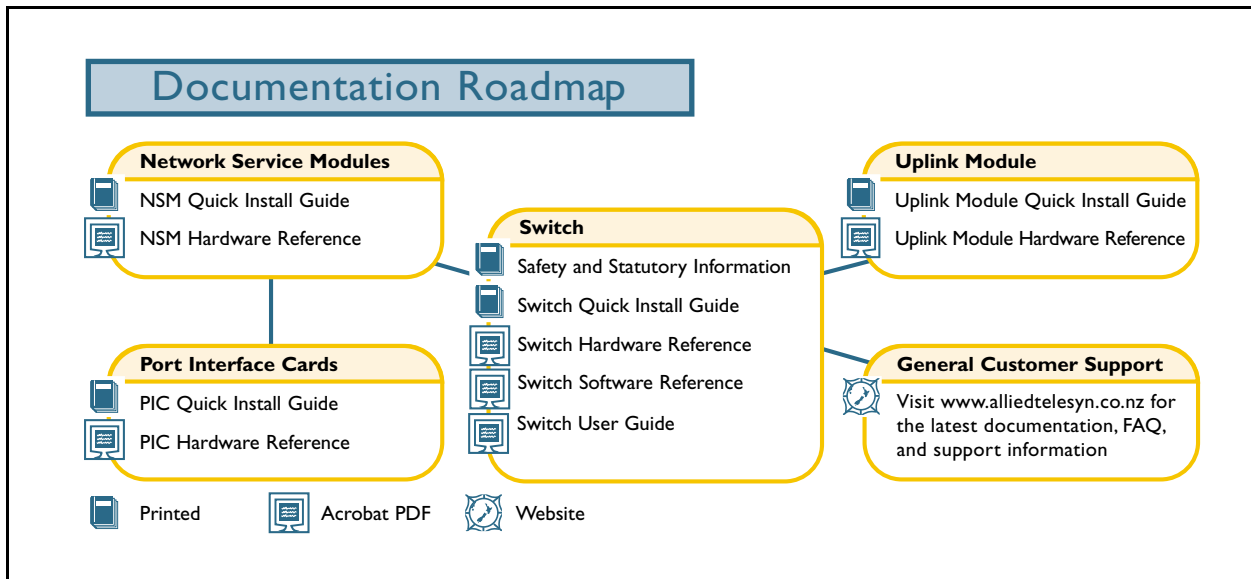
Software Release 2.1.5 for Rapier Switches and AR800 Series Modular Switching Routers

Contents

Contents	1
Introduction	2
Hardware Platforms	3
Support for Uplink Modules	3
The AT-A39/T 1-port 1000BASE-T Uplink Module	3
AT-A39/T Uplink Module LEDs	4
Port, Connector, and Cable Combinations	4
Software Release 2.1.5	4
New Software Features	4
VLAN Relay	4
Disabling CHAP Re-challenge	9
Resolved Issues	10
E1/T1 PIC Card	10
Firewall	10
Interfaces	10
Switch	11
Spanning Tree Protocol (STP)	11
Availability	11
Installation	12

Introduction

Allied Telesyn International announces the release of Software Release 2.1.5 on existing models of Layer 3 managed switches and switching routers. This release note describes the new features and enhancements to the AR800 Series Modular Switching Router, and the Rapier Layer 3 switches in Software Release 2.1.5. It should be read in conjunction with the Quick Install Guide, Hardware Reference, User Guide and Software Reference for your switch. These documents can be found on the Documentation and Tools CD-ROM packaged with your switch, or on the support site for your switch: www.alliedtelesyn.co.nz/support/rapier/ or www.alliedtelesyn.co.nz/support/ar800/.



Software Release 2.1.5 contains two significant new features:

- VLAN relay, which allows the passage of a range of non-routed protocol types between Virtual Local Area Networks on the switch.
- The CHAP re-challenge parameter, which gives the user control over the frequency with which the Challenge-Handshake Authentication Protocol sends out re-challenge messages, and allows the user to disable re-challenge messages if required.

A number of minor issues are also resolved in this release.



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 this 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.

Hardware Platforms

Rapier Layer 3 switches and AR800 Series switching routers deliver wire speed Layer 2 and Layer 3 switching with low-latency high-bandwidth traffic capabilities. The range of models allows the user to choose the port connectors, expansion options and advanced features required for their network.

Software Release 2.1.5 supports the following switch and switching router models, with access via the command line interface, SNMP and the Graphical User Interface (GUI):

- Rapier 24
- Rapier 16F/SC
- Rapier 16F/MT
- Rapier 8/8SC
- Rapier 8/8MT
- Rapier G6
- Rapier G6F/LX
- Rapier G6F/SX
- Rapier G6F/MT
- AR824
- AR816F/SC
- AR816F/MT

Support for Uplink Modules

Uplink modules allow you to connect switches together and to add extra gigabit ports and port types to the switch.

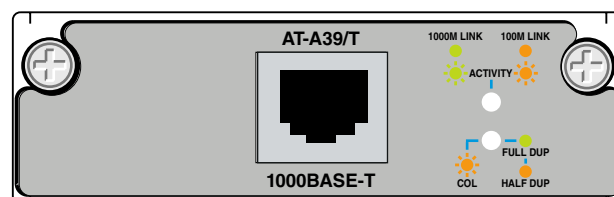
The following uplink modules are currently available:

- AT-A35/SX 1-port 1000BASE-SX (SC fibre connector)
- AT-A35/LX 1-port 1000BASE-LX (SC fibre connector)

The AT-A39/T 1-port 1000BASE-T Uplink Module

Software Release 2.1.5 will also support the upcoming AT-A39/T Uplink Module, which will include one 1 gigabit port and will use an RJ-45 copper connector. This module will make the speed and functionality of the gigabit uplink modules available to network sections using CAT5 and CAT5E cables.

Figure 1: AT-A39/T Uplink Module.



For more information about any of these Uplink Modules, ask your Authorised Allied Telesyn distributor or reseller, or visit www.alliedtelesyn.co.nz.

AT-A39/T Uplink Module LEDs

These LEDs will be on the face-plate of the Uplink Module, and will provide information on how the module is functioning. This information will be useful for diagnosing possible operational faults. Further information can be found in the Uplink Module Hardware Reference, the latest version of which is available at www.alliedtelesyn.co.nz/support/support.html.

Table 2: Uplink Module LEDs (AT-A39/T).

LED	State	Function
Full Dup/Half Dup/Col	Green	The port is operating at full-duplex
	Amber	The port is operating at half-duplex
	Flashing amber	Collisions are occurring
	Off	No link is present
Activity	Green	A 1000 Mbps link is open
	Flashing green	1000 Mbps activity is occurring
	Amber	A 100 Mbps link is open
	Flashing Amber	100 Mbps activity is occurring
	Off	No link is present

Port, Connector, and Cable Combinations

Table 3: Port, connector, and cable combinations for the AT-A39/T.

Model	Port Type	Connector Type	Cable Type ¹	Maximum Cable Length
AT-A39/T	100/	RJ-45	CAT5	100 to 150m
	1000BASE-T		CAT5E	(328 to 492ft) 200m (656ft)

1. Refer to the IEEE 802.3 Standards for further cable information.

Software Release 2.1.5

New Software Features

VLAN Relay

VLAN relaying allows the passage of traffic between the VLANs on one switch, for protocols which are not processed by the switch's routing functions. Particular protocols or protocol groups can be specified, and filtering will occur on the basis of protocol identification number. VLAN relaying is similar to the bridging function of an Allied Telesyn router.

Protocol names have been predefined for many protocol types. Those protocols that are transferred by VLAN relay and that have predefined names are given in Table 4, with their associated protocol identification numbers. Other protocols can be specified by entering their protocol identification numbers. Protocols that are routed by the switch, including IP, IPX, AppleTalk, STP and GARP, cannot be VLAN relayed.

Table 4: Predefined protocol types implemented by VLAN relay.

Protocol Name	Protocol Number	Encapsulation
All802	all SAP protocols	SAP
Netbeui	F0	SAP
SNA Path Control	04	SAP
PROWAY-LAN	0E	SAP
EIA-RS	4E	SAP
PROWAY	8E	SAP
ISO CLNS IS	FE	SAP
AllEthII	all EthII protocols	EthII
XEROX PUP	0200	EthII
PUP Addr Trans	0201	EthII
XEROX NS IDP	0600	EthII
X.75 Internet	0801	EthII
NBS Internet	0802	EthII
ECMA Internet	0803	EthII
Chaosnet	0804	EthII
X.25 Level 3	0805	EthII
XNS Compat	0807	EthII
Banyan Systems	0BAD	EthII
BBN Simnet	5208	EthII
DEC MOP Dump/Ld	6001	EthII
DEC MOP Rem Cons	6002	EthII
DEC LAT	6004	EthII
DEC Diagnostic	6005	EthII
DEC Customer	6006	EthII
DEC LAVC	6007	EthII
RARP	8035	EthII
DEC LANBridge	8038	EthII
DEC Encryption	803D	EthII
IBM SNA	80D5	EthII
SNMP	814C	EthII
AllSNAP	all SNAP protocols	SNAP

VLAN relaying operates in three stages:

1. The user creates one or more VLAN relay entities and adds the required VLANs and protocols to each entity.

2. The VLAN relay entity attaches to each specified VLAN and receives traffic. If more than one VLAN relay entity is attached to the same VLAN for the same protocol type, an intermediate attachment level will receive the packet, duplicate it and send it to the separate VLAN relay entities as required.
3. The VLAN relay entity sends the packet to the appropriate destination VLAN. Destination addresses are determined from the switch's learned address tables. If the destination address cannot be found, the packet is sent to all ports on all VLANs which are part of the VLAN relay entity. If the packet is destined for the VLAN on which it was received, the relaying entity will not send it to that VLAN, because the packet will have caused a destination lookup failure, and therefore the switch itself will have sent the packet to all the ports in the VLAN.

To configure VLAN relaying on the switch, first create a VLAN relay entity and give it a unique name, using the command:

```
CREATE VLANRELAY=name
```

where *name* is a unique name for the VLAN relay entity, 1 to 15 characters in length. Valid characters are uppercase letters (A-Z), lowercase letters (a-z), digits (0-9), the underscore character ("_"), and the hyphen character ("-").

The VLAN relay entity will be enabled by default.

The VLANRELAY parameter specifies the unique identifier for the VLAN relay entity. No VLAN relay entity with this name may already exist. Comparisons of VLAN relay entity names are done without regard to the case of letters, although the case of letters is preserved in order to improve readability. For example, "relayone" and "RelayOne" are treated as the same VLAN relay entity name.

In many networks, only one VLAN relay entity will be required. The following configurations are examples of situations when more than one VLAN relay entity may be used.

- If a number of protocols and VLANs will be part of VLAN relaying, but not all protocols on all VLANs, then setting up a number of VLAN relay entities allows only the relevant protocols and VLANs to be part of relaying.
- If traffic is to be relayed between certain VLANs but not others (for example, between VLAN 1 and VLAN 2, and between VLAN 1 and VLAN 3, but not between VLAN 2 and VLAN 3), then separate VLAN relay entities are required.

An existing VLAN relay entity can be disabled or destroyed using the commands:

```
DISABLE VLANRELAY=name
```

```
DESTROY VLANRELAY=name
```

If a VLAN relay entity is destroyed, packet relaying as configured in that entity immediately stops.

A disabled VLAN relay entity can be re-enabled using the command:

```
ENABLE VLANRELAY=name
```

To initiate relaying, add the VLANs which packets are to be sent between, and the desired protocols, to the VLAN relay entity, using the command:

```
ADD VLANRELAY=name [PROTOCOL=protocoltype]
[VLAN={vlaname|1..4094}]
```

where:

- *protocoltype* is either a valid protocol number in hexadecimal notation, or a recognised protocol name. A protocol number will be 1 byte for SAP, 2 bytes for ETHII or 5 bytes for an 802.2 SNAP type packet.
- *vlaname* is a unique name for the VLAN, 1 to 15 characters in length. Valid characters are uppercase letters (A-Z), lowercase letters (a-z), digits (0-9) the underscore character (" _"), and the hyphen character (-). The *vlaname* cannot be a number or ALL.

This command adds a protocol number and/or a VLAN to a VLAN relay entity. At least one protocol and two VLANs must be added to a VLAN relay entity before the entity can begin relaying packets.

The VLANRELAY parameter specifies the unique identifier for the VLAN relay entity. A VLAN relay entity with this name must already exist.

The PROTOCOL parameter specifies an Ethernet protocol number for packets which are to be relayed. A predefined list of common protocols is provided in Table 4 on page 5. To relay one of these protocols, specify the protocol name as the value for the PROTOCOL parameter. There is also the option of relaying all protocols of a given encapsulation type by use of the keywords "ALL802", "ALLETHII" and "ALLSNAP".



Use of the "ALL802", "ALLETHII" and "ALLSNAP" protocols can cause traffic to be unexpectedly relayed where it is not desired. It is more desirable to explicitly enter the identification numbers of the protocols to be relayed.

The VLAN parameter specifies the name or VLAN identifier of a VLAN to add to the VLAN relay entity. Adding a VLAN allows packets from that VLAN to be received and relayed, and packets from other VLANs to be relayed to that VLAN. The VLAN must already exist, and must be a static VLAN.

VLANs and/or protocols can be removed from an existing VLAN relay entity using the command:

```
DELETE VLANRELAY=name [PROTOCOL=protocoltype]
VLAN= [{vlaname|1..4094}]
```

The relay entity must still contain at least one protocol and two VLANs in order to relay packets.

A count of the packets relayed by the VLAN relay entity or entities, which shows the packets relayed from and to each VLAN, can be displayed using the command:

```
SHOW VLANRELAY [=name]
```

The VLANRELAY parameter specifies the name of the VLAN relay entity for which to show information. If the name is not given, information about all VLAN relay entities is displayed.

Figure 1: Example output from the SHOW VLANRELAY command.

```

VLAN relay entities
-----
Name ..... SNARelay
Enabled ..... Yes
Debugging ..... No
Protocol ..... 00
Protocol ..... 04
VLAN ..... 2 (Accounts)
VLAN ..... 5 (Admin)
VLAN ..... 16 (Sales)
Packet counters:
  VLAN 2 to VLAN 5 ..... 2345
    VLAN 16 ..... 148
  VLAN 5 to VLAN 2 ..... 2567
    VLAN 16 ..... 754
  VLAN 16 to VLAN 2 ..... 174
    VLAN 5 ..... 802
-----

```

Table 5: Parameters displayed in the output of the SHOW VLANRELAY command.

Parameter	Meaning
Name	The name of the VLAN relay entity.
Enabled	Whether the VLAN relay entity is enabled or not.
Debugging	Whether packet debugging for the VLAN relay entity is enabled or not.
Protocol	The protocol number of each protocol that is relayed by the VLAN relay entity.
VLAN	The numerical VLAN Identifier and name of each VLAN that has been added to the VLAN relay entity.
Packet counters	The number of packets that have been relayed between VLANs by this VLAN relay entity.

The traffic being relayed, including the source and destination VLANs and the relevant VLAN relay entity, can be displayed using the command:

```
ENABLE VLANRELAY [=name] DEBUG
```

The format of the output messages from packet debugging is as follows:

```
VR: 2->3: 0000cd001234 0000cd004321 040403060708090560403
```

The first part of the output shows which VLANs the packet is being relayed between. The second part shows the packet, with destination and source MAC addresses separated from the payload of the packet.

VLAN relay debugging can be disabled using the command:

```
DISABLE VLANRELAY [=name] DEBUG
```

Debugging is disabled by default. It can be enabled for one specified VLAN relay entity, and can be disabled for all entities, or for a specified entity.

Disabling CHAP Re-challenge

The Challenge-Handshake Authentication Protocol (CHAP) provides for both authentication during the Link Establishment phase and verification at random intervals during the Network-Layer Protocol phase.

CHAP is controlled by the authenticator, which sends a *challenge* message containing an identifier and a unique challenge value to the peer. The peer responds with a user name and value calculated by applying a *one-way hash function* (MD5) to a string created by concatenating the identifier, the password for the user name and the challenge value. The authenticator compares the response against its own computation of the function, using the user name to look up the password in the User Authentication Database. If the values match, the authentication is acknowledged, otherwise the link is terminated.

The challenge is repeated at intervals during the Network-Layer Protocol phase to ensure that there has been no change to the link. Each challenge uses a different identifier and challenge value. The identifier value changes in a predictable way (typically the value of a regularly incremented counter), but the challenge value is a unique and random value. By default, the interval between challenges varies randomly between 5 and 15 minutes.

For some users, this interval may be too large. Other users may find the re-challenge feature unnecessary and therefore undesirable, because answering the message requires that the PDA terminal wakes up out of battery-save mode, and because the user may be charged for the re-challenge traffic. Also, PDA terminals running earlier versions than v1.3 of the Win96 dial-up adapter do not reply to the re-challenge message. Therefore, a new optional parameter, RECHALLENGE={ON | OFF | 360..3600} , has been added to a number of CHAP commands.

The RECHALLENGE parameter specifies if the CHAP re-challenge function is on or off, or specifies a maximum re-challenge period. PPP will calculate a random period for the CHAP re-challenge between the maximum re-challenge period and a minimum of 5 minutes. If ON is specified the CHAP re-challenges will take place with a maximum re-challenge period of 15 minutes. If OFF is specified then CHAP re-challenges will not take place, because the CHAP re-challenge is disabled. If a time is specified then this time will be used as the upper limit on the re-challenge time calculation. The default is ON.

The maximum re-challenge period is given in seconds, and is a value between 360 and 3600 seconds.

The commands which include the RECHALLENGE parameter are:

- CREATE PPP
- CREATE PPP TEMPLATE
- SET PPP
- SET PPP TEMPLATE

The maximum re-challenge period can be seen in the output of the SHOW PPP CONFIG and the SHOW PPP TEMPLATE commands, in the form:

```
CHAP rechallenge (max. period seconds)          900
```

If RECHALLENGE=OFF, "off" will be displayed instead of the number of seconds.

Resolved Issues

E1/T1 PIC Card

In the United States of America, some of the overhead bits of a T1 link are used to provide a data link (DL) for monitoring and maintenance. In Japan this DL is not used. If the DL receiver is enabled in Japan and noise occurs on these bits during link/up down, an infinitely long frame may be received. This in turn has caused a watchdog timer reboot of the router. The DL reception has been disabled for Japan and the watchdog timer reboot prevented.

Firewall

Wire-speed hardware routing will now be performed between VLANs, when applicable, as long as there is no possibility of traffic passing between public and private VLAN interfaces, or between VLAN interfaces in different policies.

Certain configurations of VLAN interfaces may still require software routing to allow the firewall to function correctly. Software routing will be necessary for a VLAN interface that has been added to the firewall policy if

- the new interface is a private interface and the same policy contains a public VLAN interface,
- the new interface is a public interface and the same policy contains a private VLAN interface, or
- a VLAN interface has been configured in another policy.

If any one of these circumstances exists, the firewall will configure software routing for all traffic on the VLANs concerned. If possible, this situation should be avoided, because of the cost in routing speed.

The firewall now correctly opens ports with passive FTP.

Some firewall log messages have been made more concise so that they will no longer be truncated.

Interfaces

For each transition cable type, one of the modem control inputs is used to determine the operational status of the interface. This status is the `ifOperStatus` object in the interface MIB for the interface and can be displayed using the `SHOW INTERFACE` command. For the `ifOperStatus` of a SYN interface to be shown as "Up" the following 3 conditions must apply:

- the SYN interface must be enabled
- a higher layer (e.g. PPP) must be attached to the SYN interface
- the relevant modem control input signal must be asserted.

The modem control input signal controlling the `ifOperStatus` for each transition cable type is given in Table 6.

Table 6: The input signal which determines the operational status of the interface for different transition cable types.

Cable type	Input signal
RS-232 DTE	CD
V.35 DTE	CD
X.21 DTE	I
RS-232 DCE	DTR
V.35 DCE	DTR
X.21 DCE	C

To avoid spurious ifOperStatus transitions due to "glitches" (changes of short duration) on the modem control input signal, the transitions are subjected to some hysteresis. The modem control signal must be asserted continuously for a period of at least one second before the ifOperStatus is changed to "Up", and the modem control signal must be negated continuously for a period of at least two seconds before the ifOperStatus is changed to "Down".

Switch

When a large number of packets originated in the CPU of a Rapier switch, or was routed by its software, occasionally a packet consisting only of bytes containing 0x55 and 0x11 would be transmitted. This packet would be followed by the retransmission of some packets that had been transmitted previously. This problem with packet transmission has been corrected so that neither the spurious packets nor the retransmissions now occur.

For the Rapier family, packets that originate on the switch or are routed by the switch's software have been assigned a Quality of Service priority of 7. To ensure that these packets are transmitted promptly, you should not assign priority 7 to a low-numbered egress queue.

Packets sent from, or routed by, the CPU to a port that has MIRROR=BOTH | TX are now correctly mirrored to the mirror port.

The gigabit Ethernet ports now consistently handle illegal runt packets correctly.

Spanning Tree Protocol (STP)

When a cable is disconnected from a port in the STP Blocking state, the SHOW SWITCH PORT command now shows that the port is in a link-down state.

Availability

Software Release 2.1.5 is available immediately as a FLASH release for upgrading existing switches and switching routers. The release file can be downloaded directly from the Allied Telesyn support site for your switch: www.alliedtelesyn.co.nz/support/rapier/ or www.alliedtelesyn.co.nz/support/ar800/.

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 at www.alliedtelesyn.co.nz/support/updates/patches.html, complete the form, and contact your authorised Allied Telesyn distributor or reseller.

Installation

There are no issues upgrading from Software Releases 2.1.1, 2.1.2, 2.1.3 or 2.1.4 to Software Release 2.1.5.