Linksys One Ready Communications Solution SFE2000/SFE2000P and SGE2000/ SGE2000P

Contents

Introduction

Platforms

This document provides information on the following platforms:

- SFE2000 / SFE2000P

  24FE ports (10BASE-T/100BASE-TX)

  2 GE Copper and 2 GE additional Combo ports (Either Copper or Fiber)

  Stackable System

  PoE (only in SFE2000P)

- SGE2000 / SGE2000P

  24GE ports (10BASE-T/100BASE-TX/1000BASE-T)

  2 combo ports (Either Copper or Fiber)

  Stackable System

PoE (only in SGE2000P)

NOTE: It is recommended that these Release Notes be thoroughly reviewed prior to installing or upgrading this product.

Support

For information regarding the latest available firmware and documentation, refer to Linksys One web site.

System Specifications

System Firmware Version Details

Name of the Boot Code Image	Version No	Release Date
linksys_bp24_boot-10005.bin	1.0.0.05	27-Aug-06

Name of the Main Software Application Program Image	Version No	Release Date
linksys1_bp_fe_bx-10048.ros	1.0.0.48	4-Jan-07
linksys1_bp_ge_bx-10045.ros	1.0.0.45	4-Jan-07

Known Restrictions and Limitations

Management & System Features

Headline	Description	Reference
System->System Management->Time->System Time	The time zone setting is not applied after you upload the configuration from the TFTP server. Recommended Workaround: After you upload the configuration file, change the time zone setting in the Time Zone Offset file.	66906
System -> Admin -> File Management -> Save Configuration	There may be cases where copying a running configuration file to a start up configuration file with saved VLAN values will issue an error after an upgrade. Recommended Workaround: Verify that you are not trying to create the same value twice.	68698
System -> SNMP -> Security -> Users	Cannot add users to the SNMP via the GUI. Recommended Workaround: Create SNMP groups before adding users.	68695
System->SNMP->Security->Communities	Deleting 3 or more SNMP communities advanced entities from the table may result in an error “Request Entity Too Large”. Recommended Workaround: Delete one SNMP community entity at a time.	68090
Combo ports	MGBSX1(T) 100M SFP registers its speed as 1000M.	68440
Admin->Diagnostics->copper ports	Cable length for Fast Ethernet Copper Ports is not displayed.	69338
Admin->Diagnostics->copper ports	In a stacked configuration, running an optical test may result in traffic lost on the GE port. Recommended Workaround: Disable STP on the port.	66147
Admin->Diagnostics->copper ports	After pressing the “Test” button, the “Advance” button is not displayed. Recommended Workaround: After switching to another page and returning to this page, the cable length and the “Advance” button are displayed.	69344
System->System Mgmt->Zoom	Zoom view shows SFP ports number 1 & 2 description only. For SGE2000 Only.	65363

Headline	Description	Reference
IE 5 & above doesn't display web pages normally. In some cases not all images are loaded, in other cases "Page not found" error may appear.	In these situations, users need to verify that the IE registry does contain non standard WEB server connection settings. 1. Start Registry Editor (Regedt32.exe). 2. Locate the following key in the registry: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings 3. If the following entries exist, delete them Value name: MaxConnectionsPer1_0Server Value Name: MaxConnectionsPerServer 4. Quit Registry Editor. IE normally limits the number of simultaneous TCP/IP connections made to a single web server. Windows limits HTTP 1.1 connections to two simultaneous connections. RFC2068 mandates the two connection limit. These settings can be changed only through IE registry to any non standard value.	http://support.microsoft.com/kb/282402 http://www.ietf.org/rfc/rfc2068.txt

Layer 2

Headline	Description	Reference
Bridging->Multicast ->Multicast Group	FireFox browser will not show Interface Details if the user Adds a Multicast Group entry and then selects it from the Bridge Multicast Address combo box. Recommended Workaround: If possible use Internet Explorer for this setting.	67870
Bridging-> VLAN Management-> Properties	HTTP connection terminates when trying to delete a very large group of VLANs (e.g., 256) Recommended Workaround: Delete VLANs in groups smaller than 256.	67322
System ->System Management-> IP Addressing	When changing the management VLAN, the DHCP address on the default VLAN is not removed from the previous VLAN management.	67761

PoE Features

Headline	Description	Reference
PoE	When a stack composed of 3 units is connected via the copper ports (uplink port, POE connection port) and the user tries to access the POE settings for unit 2, then the device loses its HTTP connection. Recommended Workaround: Increase the Web time out parameter.	67690

Quality of Service

Headline	Description	Reference
QOS->Bandwidth-> Edit Bandwidth	The default value of the Committed Burst Size (CBS) filed is shown as 128000, but it is not supported with 10/100 ports.	67952

RMON & Statistics

Headline	Description	Reference
Statistics->RMON->Alarm	In Add RMON Alarm, if a value is related to the GVRP counter name, the message 'Illegal Object' is displayed, and the entry is not added to the ‘AlarmTable'.	67602

Stacking

Headline	Description	Reference
Stacking	When administratively setting all ports in a stack of two units to "Up" using the window screen. Bridging -> Port Management-> Port Settings -> Edit, unit 2 reboots.	67902
Stacking - Restore to Default	When the default settings are restored using the web interface or the Menu CLI interface, the configuration file reverts to default settings, but stacking settings are not restored.	
Stacking- Restore to Default	When the default settings are restored using hard restore defaults, all default settings are reset, including stacking configuration.	
Stacking- Restore to Default	When the hardware "reset to default" button is pushed on the master unit, all default settings are restored on the master unit.	
Stacking- Restore to Default	If the configuration file, which has information for all units in the stack, is first reset to default (and synchronized with the backup unit), then, the master unit settings are reset to default (stackable mode, auto-numbering). Note that as a result of the reset, the master unit is reset. During the reset, the backup unit becomes master of the stack, with the default configuration file. The master unit then rejoins the stack, and is assigned a new number, using auto-numbering.	
Stacking- Restore to Default	The stacking configuration is reset for each unit individually. Performing a hard reset on any unit resets it to its default state of a stackable unit in auto-numbering mode. Performing a hard reset on any slave unit (including the backup unit) results in setting the unit to be in stackable mode with auto-numbering mode enabled. If the stack is in ring configuration, it will become a chain until the unit "rejoins" the stack. The unit is re-assigned a number, based on the auto-numbering algorithm.	

Security

Headline	Description	Reference
Security Suite - DoS Prevention - Martian Address	User cannot set an IP address for which Martian Address protection will be defined, in addition to preconfigured IP addresses.	68696
Security Suite - DoS Prevention - Martian Address	The address 127.0.0.0/8, which is used as the internet host loopback address, is not predefined in the Martian Address list.	68697

Supported Firmware Functionality

Feature Overview

This section describes the device features. For details regarding the system functionalities, refer to the User's Guide.

General Features

Power over Ethernet (On SFE2000P and SGE2000P only)

Power over Ethernet (PoE) provides power to devices over existing LAN cabling, without updating or modifying the network infrastructure. Power over Ethernet removes the necessity of placing network devices next to power sources.

Head of Line Blocking

Head of Line (HOL) blocking results in traffic delays and frame loss caused by traffic competing for the same egress port resources. HOL blocking queues packets, and the packets at the head of the queue are forwarded before packets at the end of the queue.

Flow Control Support (IEEE 802.3X)

Flow control enables lower speed devices to communicate with higher speed devices by requesting that the higher speed device refrains from sending packets. Transmissions are temporarily halted to prevent buffer overflows.

Back Pressure Support

On half-duplex links, the receiving port prevents buffer overflows by occupying the link so that it is unavailable for additional traffic.

Virtual Cable Testing (VCT)

VCT detects and reports copper link cabling occurrences, such as open cables and cable shorts.

Optical Transceiver Analysis

The Finisar optical transceiver provides access to a set of parameters that can be monitored and displayed to the system administrator.

MDI/MDIX Support

The device automatically detects whether the cable connected to an RJ-45 port is crossed or straight through, when auto-negotiation is enabled. Standard wiring for end stations is Media-Dependent Interface (MDI) and the standard wiring for hubs and switches is known as Media-Dependent Interface with Crossover (MDIX).

Auto Negotiation

Auto negotiation allows the device to advertise modes of operation. The auto negotiation function provides the means to exchange information between two devices that share a point-to-point link segment, and to automatically configure both devices to take maximum advantage of their transmission capabilities.

Auto-negotiation advertisement is also supported. Port advertisement allows the system administrator to configure the port speeds advertised.

Manual Port Control and Identification

While port settings can be derived automatically, as described above, many settings can be set by the user manually.

MAC Address Supported Features

MAC Address Capacity Support

This device supports up to 8K MAC addresses. It reserves specific MAC addresses for system use.

Static MAC Entries

MAC entries can be manually entered in the Bridging Table, as an alternative to learning them from incoming frames. These user-defined entries are not subject to aging and are preserved across resets and reboots.

Automatic Aging for MAC Addresses

MAC addresses from which no traffic is received for a given period are aged out. This prevents the Bridging Table from overflowing.

VLAN-aware MAC-based Switching

The device always performs VLAN-aware bridging. Classic bridging (IEEE802.1D) is not performed, where frames are forwarded based only on their destination MAC address. However, a similar functionality may be configured for untagged frames. Frames addressed to a destination MAC address that are not associated with any port are flooded to all ports of the relevant VLAN.

MAC/IP Address to Port View

Displays the MAC addresses and IP addresses that are associated with a given port. For each port, it is possible to display the MAC addresses and IP addresses that are associated with that port. The information is based on information available in the ARP table, but is presented differently.

Layer 2 Features

IGMP Snooping

IGMP Snooping examines IGMP frame contents when they are forwarded by the device from work stations to an upstream Multicast router. From the frame, the device identifies work stations configured for Multicast sessions and identifies which Multicast routers are sending Multicast frames.

Port Mirroring

Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from a monitored port to a monitoring port. Users specify which target port receives copies of all traffic passing through a specified source port.

Packet Broadcast Storm Control

Storm Control enables limiting the amount of Multicast and Broadcast frames accepted and forwarded by the device. When Layer 2 frames are forwarded, Broadcast and Multicast frames are flooded to all ports on the relevant VLAN. This occupies bandwidth and loads all nodes connected on all ports.

L2 Multicast Forwarding and Filtering

When a frame arrives on any switch port and its destination address is in an L2 multicast address, it is forwarded to all relevant ports – that is, ports that are members of the relevant multicast group.

Static Multicast Groups

The user may define multicast groups to be supported, per port. Each such group is defined in the context of a specific single VLAN.

In general, this feature allows the user to manually achieve what IGMP snooping can do automatically as a replacement (when it is undesirable to use IGMP snooping) or as a supplement (e.g. to handle hosts that do not generate IGMP reports correctly).

Environmental Monitoring

Power Supply Status

The system is capable of having two power supplies. If more than one power supply is present, the power supplies are hot swappable, and the system is able to monitor their status.

Fan Status

The system monitors the status of the fans, if they are present.

Stacking

Stack Management

The stack is controlled and managed from a single unit called the master unit. Any other unit member of the stack is named stack slave.

The stack master provides:

- Single point of control and management for every member of the stack, including itself
- Single interface for the user to control and mange the stack

Stand-alone and Stack-mode Operation

Each unit may work in one of two modes: Stand-alone, or Stack-mode. The operational mode is determined at Boot time of the software, and can only be changed by a unit reset.

Stack Membership

A stack is comprised of units based on the same types of Packet Processors. A stack can include up to eight FE devices, or up to eight GE devices.

A stack cannot include devices from different families; i.e., it cannot be comprised of FE units and GE units.

A stack can be comprised of different types of units in the same family; i.e., a stack can support different kinds of FE units OR different kinds of GE units.

PoE and non-PoE devices can be members of the same stack, as long as they are from the same family.

Stacking Ports

A standard copper GE cable is used to connect the stacked units.

If the unit is a "standalone" mode, all the GE ports are available to the user.

If the unit is in a "stack" mode, there are two, dedicated GE ports that are used for stack connection (port 12 and port 24 in SGE2000).

The default ports used for stacking are two pre-determined GE copper ports.

However, the user can define the stacking links to be the fiber links, instead of the copper ones. This can be done after the system starts up, and the configuration takes effect after the stack is reset. (A stack is reset by resetting the master unit.) The configuration is for the entire stack.

Stack Members Numbers - Unit ID

A stack member is identified by a unique number.

Stack Master Election Process

Only two Units at most in the entire stack can be "Master Enabled" unit, in other words can be elected as a Master of the stack or Master Backup of the stack. "Master Enabled" units are determined by setting their UNIT ID to one or two.

Master Failure Backup

The Master and its Master Backup maintain a "Warm Standby" approach in case an active Master fails. If this happens, the Backup Master takes its place and continues to operate the Stack normally.

Hot extraction /Unit failure/Stacking cable disconnection or failure

Failure of a unit, hot extraction of a unit, or any stacking link failure causes a topology change, which is monitored and kept by the Master of the stack.

VLAN Supported Features

VLAN Support

VLANs are collections of switching ports that comprise a single broadcast domain. Packets are classified as belonging to a VLAN based on either the VLAN tag or based on a combination of the ingress port and packet contents. Packets sharing common attributes can be grouped in the same VLAN.

Port Based Virtual LANs (VLANs)

Port-based VLANs classify incoming packets to VLANs based on their ingress port.

Full 802.1Q VLAN Tagging Compliance

IEEE 802.1Q defines an architecture for virtual bridged LANs, the services provided in VLANs and the protocols and algorithms involved in the provision of these services.

Protocol Based VLAN

VLAN classification rules are defined on data-link layer (Layer 2) protocol identification. Protocol based VLANs are used for isolating Layer 2 traffic for differing Layer 3 protocols.

GVRP Support

GARP VLAN Registration Protocol (GVRP) provides IEEE 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. When GVRP is enabled, the device registers and propagates VLAN membership on all ports that are part of the active underlying "Spanning Tree Protocol Features" topology.

Private VLAN Edge

A port can be defined as a Private VLAN Edge port of an uplink port, so that it will be isolated from other ports.

Spanning Tree Protocol Features

Spanning Tree Protocol (STP)

802.1d Spanning tree is a standard Layer 2 switch requirement that allows bridges to automatically prevent and resolve L2 forwarding loops. Switches exchange configuration messages using specifically formatted frames and selectively enable and disable forwarding on ports.

Fast Link

STP can take up to 30-60 seconds to converge. During this time, STP detects possible loops, allowing time for status changes to propagate and for relevant devices to respond. 30-60 seconds is considered too long of a response time for many applications. The Fast Link option bypasses this delay and can be used in network topologies where forwarding loops do not occur.

IEEE 802.1w Rapid Spanning Tree

Spanning Tree can take 30-60 seconds for each host to decide whether its ports are actively forwarding traffic. Rapid Spanning Tree (RSTP) detects uses of network topologies to enable faster convergence, without creating forwarding loops.

IEEE 802.1s Multiple Spanning Tree

Multiple Spanning Tree (MSTP) operation maps VLANs into STP instances. MSTP provides differing load balancing scenario. Packets assigned to various VLANs are transmitted along different paths within MSTP Regions (MST Regions). Regions are one or more MSTP bridges by which frames can be transmitted. The standard lets administrators assign VLAN traffic to unique paths.

STP Root Guard

Network administrators may want to prevent devices outside of the core of the network from being assigned the spanning tree role of "root". Spanning Tree Root Guard is used to prevent an unauthorized device from becoming the root of a spanning tree.

If root guard is enabled on a port, it is never selected as the STP root port; the roles it can be assigned are: Designated, Alternate, Backup or Disabled. Root guard functionality enables detection and resolution of miss configurations, while preventing loops or loss of connectivity.

BPDU filtering (when STP is disabled)

On a LAN interconnected by multiple bridges, Spanning Tree selects a controlling Root Bridge and Port for the entire bridged LAN, and a Designated Bridge and Port for each individual LAN segment. When traffic passes from one end station to another across the LAN, it is forwarded through the designated Bridge/Port for the LAN segment, to the Root Bridge, which in turn forwards the traffic to the designated Bridges/Ports on the opposite side. Bridges use Bridge Protocol Data Units (BPDUs) to communicate Spanning Tree information.

Link Aggregation

Link Aggregation

Up to eight Aggregated Links may be defined, each with up to eight member ports, to form a single Link Aggregated Group (LAG). This enables:

Fault tolerance protection from physical link disruption

- Higher bandwidth connections
- Improved bandwidth granularity
- High bandwidth server connectivity LAG is composed of ports with the same speed, set to full-duplex operation

Link Aggregation and LACP

LACP uses peer exchanges across links to determine, on an ongoing basis, the aggregation capability of various links, and continuously provides the maximum level of aggregation capability achievable between a given pair of systems. LACP automatically determines, configures, binds and monitors the port binding within the system.

Access Control Lists (ACLs)

Access Control Lists (ACLs) are a general mechanism to inspect incoming frames and classify them into named logical groups based on various criteria. Each such group may have specific actions that are carried out on each frame classified as a member of that group.

- IP ACL classification
- MAC Access Lists
- ACL actions

Quality of Service Features

Class Of Service 802.1p Support

The IEEE 802.1p signaling technique is an OSI Layer 2 standard for marking and prioritizing network traffic at the data link/MAC sub-layer. 802.1p traffic is classified and sent to the destination. No bandwidth reservations or limits are established or enforced. 802.1p is a derivation of the 802.1Q (VLANs) standard. 802.1p establishes eight levels of priority, similar to the IP Precedence IP Header bit-field.

Quality of Service Support

To overcome unpredictable network traffic and optimize performance, you can apply Quality of Service (QoS) throughout the network to ensure that network traffic is prioritized according to specific criteria. Your switch supports two modes of QoS: basic and advanced.

Quality of Service Basic Mode

In basic QoS mode, it is possible to activate a trust mode (to trust VPT, DSCP, TCP/UDP or none). In addition, a single access control list can be attached to an interface.

Quality of Service Advanced Mode

Advanced Quality of Service mode specifies flow classification and assigns rule actions that relate to bandwidth management. These rules can be grouped into a policy, which can be applied to an interface.

Device Management Features

BootP and DHCP Clients

DHCP enables additional setup parameters to be received from a network server upon system startup. DHCP service is an on-going process. DHCP is an extension to BootP.

SNMP Alarms and Trap Logs

The system logs events with severity codes and timestamps. Events are sent as SNMP traps to a Trap Recipient List.

SNMP Versions 1, 2 and 3

Simple Network Management Protocol (SNMP) over the UDP/IP protocol controls access to the system, a list of community entries is defined, each of which consists of a community string and its access privileges. There are 3 levels of SNMP security read-only, read-write and super. Only a super user can access the community table.

Web Based Management

With web based management, the system can be managed from any web browser. The system contains an Embedded Web Server (EWS), which serves HTML pages, through which the system can be monitored and configured. The system internally converts web-based input into configuration commands, MIB variable settings and other management-related settings.

Configuration File Download and Upload

The device configuration is stored in a configuration file. The Configuration file includes both system wide and port specific device configuration. The system can display configuration files in the form of a collection of CLI commands, which are stored and manipulated as text files.

TFTP Trivial File Transfer Protocol

The device supports boot image, software and configuration upload/download via TFTP.

Remote Monitoring

Remote Monitoring (RMON) is an extension to SNMP, which provides comprehensive network traffic monitoring capabilities (as opposed to SNMP which allows network device management and monitoring). RMON is a standard MIB that defines current and historical MAC-layer statistics and control objects, allowing real-time information to be captured across the entire network.

Menu based Command Line Interface

Menu based Command Line Interface (CLI) syntax and semantics conform. CLI is composed of mandatory and optional elements.

Syslog

Syslog is a protocol that enables event notifications to be sent to a set of remote servers, where they can be stored, examined, and acted upon. The system sends notifications of significant events in real time, and keeps a record of these events for after-the-fact usage.

SNTP

The Simple Network Time Protocol (SNTP) assures accurate network Ethernet Switch clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. Time sources are established by Stratums. Stratums define the distance from the reference clock.

Traceroute

Traceroute discovers IP routes that packets were forwarded along during the forwarding process. The CLI Traceroute utility can be executed from either the user-exec or privileged modes.

Security Features

SSL

Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data through privacy, authentication, and data integrity. It relies upon certificates and public and private keys.

Port Based Authentication (802.1x)

Port based authentication enables authenticating system users on a per-port basis via an external server. Only authenticated and approved system users can transmit and receive data. Ports are authenticated via the Remote Authentication Dial In User Service (RADIUS) server using the Extensible Authentication Protocol (EAP).

Locked Port Support

Locked Port increases network security by limiting access on a specific port only to users with specific MAC addresses. These addresses are either manually defined or learned on that port. When a frame is seen on a locked port, and the frame source MAC address is not tied to that port, the protection mechanism is invoked.

RADIUS Client

RADIUS is a client/server-based protocol. A RADIUS server maintains a user database, which contains per-user authentication information, such as user name, password and accounting information.

SSH

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH version 2 is currently supported. The SSH server feature enables an SSH client to establish a secure, encrypted connection with a device. This connection provides functionality that is similar to an inbound telnet connection. SSH uses RSA and DSA Public Key cryptography for device connections and authentication.

TACACS+

TACACS+ provides centralized security for validation of users accessing the device. TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes.

Password Management

Password management provides increased network security and improved password control. Passwords for SSH, Telnet, HTTP, HTTPS, and SNMP access are assigned security features.

802.1x – Enhanced Features

- Single-host/Multiple-hosts- Single-host mode enables only the host that has been authorized to get access to the port. Filtering is based on the source MAC address. Multiple-hosts mode enables multiple hosts to be attached to a single 802.1X-enabled port. In this mode, only one of the attached hosts must be authorized for all hosts to be granted network access. If the port becomes unauthorized (re-authentication fails or an EAPOL-logoff message is received), all attached clients are denied access to the network.
- Guest VLAN - limited access to the network when the port is unauthorized.
- Unauthenticated VLANs - some VLANs in the switch would always be available, even if the port were unauthorized.

DoS Attack Prevention Engine

The device supports the ability to enable canned DoS protection to port, including:

- Illegal TCP/ICMP packet check
- Martian address check

- Prevention of TCP connections from a specific interface

Added Functionality in This Release of the Firmware

N/A

Issues Resolved in this Release

N/A