ASUS GigaX2024 Switch
Release Note 2.1.0

2004/8/23

Date	Firmware Release Version	BootRom Release Version	Notes
2004/08/23	2.1.0	2.0	Initial release
2004/05/12	2.0.0	2.0	Initial release

GX2024 2.1.0 release

Upgrade Guide:

1. **There are 2 different packages for firmware<2.1.0>**
   a. **gx2024_2.1.0_full**

      Full package contains the latest bootrom<2.0> image in it. Bootrom will also be auto upgraded (if older version is detected on the system) when upgrading this firmware image. Firmware upgrading processes are noted on item 7, 12, and 13.

   b. **gx2024_2.1.0_light**

      Light package is a pure firmware image. Before upgrading this package, user is recommended manually upgrade the latest bootrom by him/herself. Bootrom upgrading process is explained on item 2. Firmware upgrading processes are commented on item 7, 12, and 13.

*Light package is not available on ASUSTEK web site.

2. **Upgrade to bootrom<2.0> by console**
3. [Step 1] Hit any key on console to enter command mode during system startup (POST)
4. [Step 2] Set baud rate to highest speed (115200 bps) for the most efficient speedup. (Optional)
5. [Step 3] Issue command 'x', transfer bootrom image with 1K Xmodem through terminal.
6. [Step 4] Reboot the switch by power cycle.
7. **Upgrade firmware<2.1.0> by console**
8. [Step 1] Hit any key on console to enter command mode during system startup (POST)
9. [Step 2] Set baud rate to highest speed (115200 bps) for the most efficient speedup. (Optional)
10. [Step 3] Issue command 'x', transfer firmware image with 1K Xmodem through terminal.
11. [Step 4] Press 'g' to start the system.
12. **Upgrade firmware<2.1.0> by ftp**
13. **Upgrade firmware<2.1.0> by web** *

*Please refer to the user manual

Bootrom version:

Version 2.0 **: It is a requirement to upgrade the bootrom version to 2.0 to run firmware 2.1.0 release.

Firmware version: 2.1.0

Bug fixes:

1. Change port's VLAN tag/untag setting by GUI, after save the change, the configured port will experience a moment of disconnection.
2. System will crash when create VLAN name with the longest string and save in GUI.
3. Create 255 VLAN entries, and then change or display VLAN setting, system will crash.
4. First, create a trunk group T1 and save. Second, execute VLAN save. All ports in trunk group T1 will receiving broadcast packets.
5. Input the character "/" following a command, the prompt string display abnormal (ex:"l2///","net///interface//////"...etc.).
6. The identical user name could not with different password.
7. System will remove the monitor port automatically from the MARL table (static multicast) when mirror is enabled, but it will not retrieve (add to MARL table) automatically when mirror is disabled or remove monitor port.
8. CLI command “l2 trunk create” and “l2 trunk add”: monitor port can’t be added to trunk group.
9. CLI command “l2 cos show”: the values of 'weight' and 'latency' are abnormal.
10. First, setting a Static Multicast group (the port members are belong to one SOC) and remove it. Second, transmit the static multicast address. Packets only flooding to one SOC.
11. CPU is overloaded by multicast packets.
12. User can input CLI command “sys def *” before login.
13. System will crash when user input CLI command “snmp/get 1”.
14. support half duplex flow control.

Feature Enhancement:

1. **DHCP snooping** added, new feature.

   DHCP snooping is a DHCP security feature that provides security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding table. The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information that corresponds to the local untrusted interfaces of a switch. DHCP snooping gives you a way to differentiate between untrusted interfaces connected to the end-user and trusted interfaces connected to the DHCP server or another switch.

2. **DHCP client** added, new feature.

   DHCP client feature enables the switch to obtain its own IP address from a DHCP server, rather than to be configured manually by network administrators. If DHCP client

feature is enabled and an IP address has been configured, the previously configured IP address will be ignored. To manually set an IP address for a switch, DHCP client must be disabled first.

3. **802.1x with VLAN assignment** add, new feature.

   Administrator can configure a guest VLAN for each 802.1x port on the switch to provide limited services to clients (for example, upgrading their system for 802.1x authentication). Therefore, clients that are not 802.1x-capable are put into the guest VLAN. Any number of hosts are allowed access once the switch port is moved to the guest VLAN.If an 802.1x port is authenticated, then put the port to the RADIUS server assigned VLAN.

4. **SNMPv3** add, new feature.

   SNMPv3 Agent solves the problems of Security and Access control in SNMPv2. The SNMPv3 framework is v3/v2/v1 compatible. It mainly consists of 2 parts:

   1. User-Based Security Model --

      USM provides authentication (MD5 and SHA1 protocol) and privacy (DES protocol)services for SNMP. It includes a set of timeliness mechanisms to guard against message delay and message replay.

   2. View-Based Access Control --

      Access control is a security function performed at the PDU level. An access control document defines mechanisms for determining whether access to a managed object in a local MIB by a remote principal should be allowed.

5. **Syslog** add, new feature.

   Syslog can be sent out to syslog server due to system error, user configuration, status change, status periodic report, program invocation/exit, or conditions being met. Syslog server can quantify the messages into one of several broad categories consist of the facility that generated them, along with an indication of the severity of the message. Administrator can filter the messages and also having the ability to place status or informative messages in a file for later perusal.

6. **System bind with VLAN**, new feature.

   Assign a VLAN ID to system (sw0), only the ports which were assigned the VLAN ID the same as the VLAN ID of system (sw0) can access the switch (ex: telnet, http …).

   Note: If the 802.1x supplicants are authenticated by a RADIUS server, the VLAN ID of the RADIUS server connected port must the same as the VLAN ID of the system (sw0).

7. **Dual file system**, new feature.

   There are two advantages in dual file system:

a. Reduce the size of the configuration files (all files are compressed) to extend the flash's life.

b. Protect the configuration files from harm in abnormal operation (ex: power on/off when access configuration files). The file system is partitioned into two parts: major and mirror file system. If one file system was corrupted, another will restore it. If two file systems were all corrupted, then system will erase both and create default configuration files.

8. **System IP configuration**.

Checking reserved IP address according to RFC 1166:

0.0.0.0 means "this network" ---- Reserved

127.0.0.0 is a loopback address ---- Reserved

All Class D addresses: 224.*.*.* to 239.*.*.* ----Reserved

All Class E addresses: 240.*.*.* to 255.*.*.* ---- Reserved

9. **Backup or restore configuration by console**, new feature.

10. **Debug function enhancement**, new feature.

sysGuard is a debug function enhancement on aos2.1. Since some critical information is hard to collect after a system has crashed. It supports:

1. Switching traffics monitoring
2. CPU usage monitoring
3. Memory usage monitoring
4. System health (temperatures, fans, voltages) monitoring
5. CPU-incoming packets capturing
6. SMTP based reporting (optional)

Firmware version 2.0.0

Bug fixes:

1. SNMPd memory leak when accessing a non-existed OID.
2. HTTPd memory leak when ring-buffer is unavailable.
3. STP BPDUs do not send when broadcast/multicast traffics storming.
4. Reserved group addresses packets, e.g.; pause frames, BPDUs, etc, should not be relayed.
5. CLI command: "**sys users add**" username cannot contain character other than alpha-numeric type.
6. CLI command: "**net interface ip**" setting system IP as either loopback IP address (x.x.x.0), or broadcast IP address (x.x.x.255), are forbidden.

7. STP GUI bug: bridge priority value could not set to 0.

Feature Enhancement:

11. RSTP(**802.1w**) added, new feature.

    ieee802.1w Rapid Spanning-Tree Protocol (RSTP) is an evolution of the 802.1d standard. In most cases, RSTP performs better than the legacy STP since it can achieve much faster convergence in a properly configured network (sometimes in the order of a few hundred milliseconds). RSTP is also capable of reverting back to STP in order to interoperate with legacy bridges on a per-port basis.

12. LACP(**802.1ad**) added, new feature.

    The Link Aggregation Control Protocol (LACP) is required by the IEEE standard 802.3ad for dynamically changing configuration information among cooperating systems in order to automatically configure and maintain link aggregation groups. The protocol is able to automatically detect the presence and capabilities of other aggregation capable devices, i.e. with LACP it is possible to specify which links in a system can be aggregated.

13. **802.1x** Radius added, new feature.

    IEEE 802.1x is a security function in a LAN or MAN environment. The port-based network access control only allows authorized user to access the network. An authentication server (RADIUS) server provides service to the switch authentication request for the host that connects to the switch port. The connected port is initially blocked until the connecting host passed the authentication process. The 802.1x features provided by AOS 2.0 are:

    1. Single mode & Multi mode:

       Single Mode: Only one host is allowed for each port.

       Multi Mode: All the hosts are allowed if one of them passed the authentication.

    2. Use RADIUS server or local authentication database to do the authentication
    3. Store port identification to RADIUS server. This information may be used for accounting considerations.

    IEEE Std 802.1X-2001 pg-14 sec-7.4 note:

    EAPOL frames transmitted by a PAE shall not be VLAN tagged, but may optionally be priority tagged. All PAEs shall be capable of receiving both priority tagged and untagged EAPOL frames.

14. **Watchdog timer** added, new feature.

    Watchdog timer is worked as a safeguard mechanism to prevent the software run in infinite loop. The watchdog timer is set to 50 seconds in Gx2048. In case of watchdog

timer is not cleared by implemented software more than 50 seconds, watchdog timer will issue an internal CPU reset to force system reboot.

15. **Autoconfig** added, new feature.

    Autoconfig is a function to make configure the system easier. Configuration commands are written in a file, and the file can be transmitted to the switch by ftp or http. When the autoconfig file is received by the system, the confuguration commands will be executed in sequence automatically. This saves a lot of time when configuring a lot of switches with the same setting is needed, because the same command lines will not to be typed repeatedly.

16. **Protocol stack**: TCP connections have a limitation up to 16.

17. FTPd & TELNETd both services have each connection limitation up to 3.

18. **Protocol Stack Enhancements:**

    Protocol stack porting based on most current stable Net BSD release. The new protocol stack is verified to be ok from various Denial of Service attacks. Common Denial of Service attacks are listed as follows:

    1. BLOOP:

       Spoofed/mal-formed ICMP packets

    2. BLAND:

       Encapsulate an IP packet with options inside an ICMP packet. This ICMP packet is with type parameter problems.

    3. TWINGE:

       Attacker sends packets cycling through all possible ICMP message types and subtypes.

    4. REVERSED TEARDROP:

       Fragmented packets with fragment offset larger than total packet length in the header.

    5. JOLT2, OVERDROP:

       On reception of large fragmented packets at high speed, CPU usage may go to 100% due to logging/console output activities.

    6. OCTOPUS:

       Sending normal TCP connection requests at high speed. It will consume system network resource and crash the target system eventually.

    7. PING FLOODING:

       Sending ICMP request packets at very high speed. It may consume system memory and eventually crash the system.

    8. SYN FLOODING:

       Attacker sends half open TCP SYN packets to the target system. Those packets will fill up the target system listen queue and stop accept new connections. Target system may crash if network resources get used up.

    9. LAND ATTACK:

       Attacker sends a spoofed packet to the target system where the source address:port combination equals to the destination address:port combination.

    10. TARGA3:

Attacker sends random malformed IP packets can cause TCP/IP stack to crash. Malformed IP packets consist of invalid fragmentation, protocol, packet size, header values, options, offsets, TCP segments and routing flags.

11. SYNDROP:

    Attacker sends TCP SYN packets with overlapped IP fragments.

12. TEARDROP:

    Attacker sends overlapped fragmented packets to the target system.

13. SSPING/PING OF DEATH:

    A series of over sized (64K bytes in size) ICMP packets can consume lots of buffer space and cause system crash. Also, CPU may go to 100% since it needs to reassemble the packet.

14. SMURF:

    Attacker sends a spoofed ICMP packet to various broadcast addresses resulting in multiple replies to the spoofed source address.

15. OPENTEAR:

    Sending randomly spoofed source address UDP fragmented packets to different ports.

19. GUI web pages up-to-date.