GigaX2024 Switch
Release Note 2.0.0

2004/5/12

GX2024 2.0.0 release

Upgrade Guide:

1. **There are 2 different packages for firmware<2.0.0>**
   a. **gx2024_2.0.0_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_2.0.0_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<2.0.0> 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<2.0.0> by ftp** *
13. **Upgrade firmware<2.0.0> 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 2.0.0 release.

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:

1. 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.

2. 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.

3. **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.

4. **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 Gx2024. 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.

5. **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.

6. **Protocol stack**: TCP connections have a limitation up to 16.
7. FTPd & TELNETd both services have each connection limitation up to 3.
8. **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.

9. GUI web pages up-to-date.