GB Bewapass Entro – Questions and answers

A. Bewapass/Entro V4 in TCP/IP Local Area Network

1. How does the traffic load look like when using Entro in TCP/IP LAN?

Answer:
Because Entro/TCP is evolved from RS485, the traffic is relatively moderate depending on that the database is very hard packed. Trying to describe the traffic the SR32i will have a socket open to every other SR32i. This socket is alive and is tested for failures with a special ping-message every eight second (in version 4). This is not an ICMP-ping, rather a common TCP/IP package with some information (only a few bytes in size).
Beside this, in an idling system, there is a comparing-of-databases message to the node nearby approx. every ninth second. The time depends of the configuration. In a small system this could be every sixth second. Also this message is short - approx. 40 bytes plus the length of header (se item 2).

2. How does the messages look like e g for events and creating cardholders? What is size of packages is sent?

Answer:
The packet size is currently 407 bytes (plus TCP header and IP header together with a MD5 hashing of the message). Totally it is less than 500 bytes. The information sent in case of an event (e g granted access) is approx. 40 bytes. Creating a new cardholder results in a database update with a frame of 80 bytes and a 10-byte frame.

3. How often does the SR32i communicate with each other?

Answer:
At least every 6-8 second.

4. How often does the SR32i requests a timeserver?

Answer:
It does it every 23rd hour continuously.

5. What happens if the SR32i loses the database and uploads from another SR32i – does the LAN become slow?

Answer:
No, because we only use a fraction of the total capacity. Entro uses 10Mbit LAN and just a few percent of that. The reason is that the Entro primary should handle the access issues rapid. The communication has a lower task priority. In addition the communication is encrypted with 128-bit RC4, which together with the MD5 authentication takes CPU power and reduces the speed. However – in modern LANs switches are often used which do not affect the speed negative.

6. Is it possible to change the IP port used by the system – e g if 4001 and 4002 are occupied by another application?

Answer:
Only port 4002 is used in communication to the PC (and may be in conflict with other application is the same PC). In version 4 you cannot change the port. The risk for a conflict is seen as minimal. If this should be a problem we will of course solve it. There are no applications known so far that uses this port.

7. How is the traffic affected? Use of "sniffers"?

Answer:
We have (during the development phase) off course have been using "sniffers" (three commercial and one of our own). We have also bursted 100% bandwidth to the SR32i to see the effects of the information quantity. Both UDP and TCP. This is however not quite so dramatic relative to a 100 Mbit LAN.

8. Why not use VLAN?

Answer:
The recommendation is that you use TCP (instead of UDP) because it is quite harmless on the LAN. The UDP (in version 4) have the advantage that it is easy to install but it "talks" quite loud due to token-passing technique. In addition it uses broadcast and will pass through switches. The UDP solution is mainly intended as an easy way to set-up a dedicated network for SR32i without any PC connected. That is as an alternative to a twisted-pair RS485 solution.

VLAN is a good alternative to create a more secure network. It is however difficult for Bewator to state general recommendations how to build the users own LAN. There is no reason for using VLAN, due to network load, in a Entro TCP/IP environment. In general we recommend IT-managers to use LAN switches rather than an Entro recommendation.

9. Is it possible to run Entro via Citrix VTS Mainframe v 1.8?

Answer:
We do not really support a configuration with Citrix and/or PC Anywhere, VNC etc. However we can not see why it should not work.
Remote programming can also beside modems be done via TCP/IP.

10. Can database files be placed on a LAN-server to make it possible making backups in nighttime?

Answer:
To store the files on a server is not a problem itself, just install the software on the server. You then must of course be sure that the server is running all the time.

The way Entro is designed there is also redundancy integrated in the database, because all data is stored in every SR32i (except events handshaked from the PC).

11. Is the communication secure in Bewapass/Entro?

Answer:
All communication in Bewapass/Entro version 4 is heavily encrypted. At the moment RSA RC4 128-bit is used. This is the same level as most banks are using. The encryption key can easily be changed. In Internet applications the IT-manager can raise the security by increasing the encryption set up in the LAN itself. In addition the *User name* and *Password* is checked at login as well as the correct *System name*.

12. What is RSA RC4?

Answer:
RC4 is a symmetric encryption method, developed by RSA Security, which has been used for many years and is seen to be very reliable. Bewapass/Entro uses 128-bit strong encryption.

13. 128-bit encryption does not sound enough! I use 1024 on my e-mail!

Answer:
When comparing encryption algorithms, it is not correct to compare only the amount of bits because different encryption methods have different strength. Bewapass/Entro use a *symmetric* method not to compare with e-mail software (usually using PGP or similar), which is an *asymmetric* method (with public keys). These methods normally require a higher size of key to fulfil the security need.

14. What is MD5?

Answer:
MD5 is a method to confirm messages and logins. This is used in Bewapass/Entro to ensure that all messages are correct when they arrive. In addition also as an extra security when logging on via an web browser on to the Reservation system

B. What level of redundancy is there in the system?

Answer:
The system is seen as very reliable. A breakdown often appears in the installation and set-up phase (or because of poor planning).
If there however is an accident the Bewapass/Entro have a range of technical solutions who eases a fast trouble-shooting and repair. E g removable, straight-through terminal blocks supports even a change of parts when the system is still running (somewhat like plug-and-play).
Under normal, preventive efforts we think that Bewapass/Entro (with its integrated monitoring functions and distributed intelligence) is very good alternative with good redundancy to reasonable price level.

15. Why use battery-backup (UPS)?

Answer:
One of the best insurances against breakdowns etc, is to install the necessary amount of battery-backed power supplies. A correct planning regarding number of doors, type of locks, distances, cable type etc is then of course a prerequisite.

We recommend every SR32i (together with its doors) to have its own power supply, if it is possible. First because of it gives a nicer, “cleaner” installation. Secondly it is possible to connect a power fail signal from the power supply to the SR32i. Every segment of the system can then separately be monitored for main voltage breakdowns. An alarm event can be sent to the PC and/or an external alarm system.

16. What happens if an SR32i gets a short interruption?

Answer:
Every SR32i as well as the PC have a complete copy of the database (mirroring). As long as the hardware is intact but an interruption occur (e g the data memory is corrupt) the data is recovered automatically trough an up- or download. The stop of communication will generate an internal alarm to connected PC and/or an external alarm.

17. What happens if an SR32i fails?

Answer:
Due the SR32i:s isolation capabilities the superior (global) communication will probably still work. If the door environment still have got its power and includes a DC21 (with memory) these will pass to an autonomic mode where decisions of access or not are taken locally. Other doors (without DC21) can be locked or unlocked. When the faulty SR32i is replaced it will automatically recover itself via a download from another SR32i (or PC). The event alarm functions still apply.

18. What happens if a reader fails?

Answer:
In most cases other doors controlled by the same SR32i will still work. An alarm event will be sent from the actual SR32i because the actual door ”disappears”.

19. What happens during a cable failure?

Answer:
- A stop in the *global* communication (between SR32i Segment Controllers) will be discovered and an alarm event is sent from every SR32i respectively. The doors can work as usual.
- A stop in the *local* communication (between an SR32i and door) will be discovered by the actual SR32i and an alarm event is sent from actual SR32i. The doors can work as usual.
- A stop in the communication with the PC has the same effect as if the PC is turned off. I e all data is still stored in the system (together with an amount of events). When the communication is established again and the PC goes online – all events is transferred automatically.

(SE) Bewapass Entro - Frågor och svar

A. Bewapass/Entro V4 i TCP/IP nätverk

1. Hur mycket och hur ser trafiken ut på TCP/IP nätet när man kör Entro systemet via detta ?

Svar:
Eftersom Entro/TCP har sitt ursprung i RS485, så är trafiken relativt begränsad, detta beror i sin tur på att databasen är hårt bitpackad. För att försöka beskriva hur trafiken ser ut, kan vi säga att alla SR32i håller en socket öppen mot alla andra SR32i. Denna socket hålls vid liv och testas för förlorad kommunikation genom ett eget "ping-meddelande" som går var åttonde sekund i version 4 (detta är alltså inte ett ICMP-ping, utan ett vanligt TCP/IP paket med lite information.
Det är dessutom endast några få bytes stort. Förutom detta, skickas i ett "vilande" system, endast ett databasjämförande meddelande till noden "bredvid" var 9 sekund ungefär (beror lite på systemets konfiguration; kan vara var 6 sekund i ett mindre system). Även detta meddelande är kort; ca 40 bytes data, samt header längden (se punkt 2).

2. Hur ser paketen ut vid t ex olika händelser, när man lägger in nya användare? Hur stora paket skickas?

Svar:
Paketstorleken är idag max 407 bytes data (på detta tillkommer TCP header och IP header samt en MD5 hashning av meddelandet). Dvs mindre än 500 byte totalt. Det som skickas vid en logghändelse (t ex giltig passage) är ett paket på ungefär 40 bytes. När man lägger in en person är det databasuppdatering som sker, och det är i en persons fall, en post med storlek 80 bytes, och en post på 10 bytes.

3. Hur ofta pratar SR32i med varandra ?

Svar:
Minst var 6/8:e sekund.

4. Hur ofta tar SR32i kontakt med tidsserver ?

Svar:
Var 23:e timme löpande.

5. Vad händer om en SR32i tappar sin databas och börjar tanka över hela databasen från en annan SR32i, blir nätet segt då?

Svar:
Nej, därför att vi utnyttjar endast en bråkdel av kapaciteten: Entro använder 10 MBit teknik, och av denna används några få procent! Orsaken till detta är att Entro primärt skall hantera passersystemdelen snabbt, kommunikationen sker med lägre taskprioritet! Dessutom krypteras all kommunikation med 128-bit RC4, som, tillsammans med MD5 autentisering konsumerar ganska mycket CPU, och därigenom utgör en begränsning av kommunikationshastigheten. Dessutom; i de flesta moderna kontorsnätverk används switchar, vilket gör att nätet inte alls påverkas i negativ bemärkelse.

6. Kan man ändra IP porten som systemet använder. Tex om port 4011 och 4002 redan används av en annan applikation ?

Svar:
Endast ena porten (4002) används vid kommunikation mot PC (och följaktligen skulle kunna krocka med annan applikation på samma PC). I version 4.0 kan man inte ändra denna. Risken för en "krock" anses som minimal. Skulle detta dock vara ett problem, skulle vi naturligtvis lösa detta. Det finns inga kända applikationer som använder denna port.

7. Hur påverkas trafikbelastningen ? Sniffer användning ?

Svar:
Vi har under hela utvecklingsarbetet naturligtvis haft sniffers (3 olika kommersiella och dessutom egenutvecklade) påkopplade. Vi har också burstat 100% bandbredd mot SR32i för att testa att dom tål informationsmängden. Både UDP och TCP. Det är dock ganska odramatisk information som man ser, speciellt på ett 100Mbit nätverk.

8. Varför inte krav att använda VLAN ?

Svar:
Rekommendationen är att man kör TCP varianten (i motsats till UDP) om man kan, eftersom den är "tyst" på nätet. UDP versionen som finns i version 4 har speciellt den fördelen att den enkel att installera, men den pratar ganska ”högt” idag, eftersom det är ett token-passing nät, och som kör broad cast (och därigenom passerar vanliga switchar). UDP lösningen är framför allt tänkt som den enklaste lösningen att få igång nät på eget "LAN" mellan SR32i där man kanske inte har PC normalt, dvs mer som kabel alternativ till RS485 twisted pair.

VLAN är ett bra alternativ, på alla sätt och vis, speciellt om man är vill bygga på med extra säkerhet! Dock är det svårt för Bewator att gå ut med allmänna rekommendationer om hur slutkunden skall bygga sitt nätverk.
Ur belastningssynpunkt, och förutsatt att man har valt i Entro att köra TCP/IP ser vi ingen orsak till att köra VLAN, med avseende på trafikmängden. Vanligt switchat nätverk rekommenderar vi naturligtvis,
men snarare som allmän rekommendation till nätverksansvariga, än som "Entro rekommendation".

9. Jag undrar också om man kan köra Entro applikationen via Citrix VTS MainFrame v.1.8 ? (Fjärradministrera)

Svar:
Vi stödjer inte aktivt denna konfiguration med Citrix och/eller PC-Anywhere, VNC osv. osv.
Men vi ser inte någon anledning till att det inte skall fungera.

Fjärradministrera kan ju dessutom, förutom modem direkt, göras via TCP/IP.

10. Kan databas filerna ligga på en server på nätverket för att på så sätt hänga med i backup som körs på natten t ex ?

Svar:
Att lagra databasfilerna på en central server är i sig inget problem, annat än att man blir beroende av att servern är tillgänglig. Enklast gör man detta genom att installera mjukvaran på servern.

Som Entro är uppbyggt finns ju redundans i databasen inbyggt i systemet, eftersom all data sparas i SR32i, förutom händelser som har ”handskakats” av PC:n.

11. Är kommunikationen säker i Bewapass/Entro?

Svar:
All kommunikation i Bewapass/Entro V4 är starkt krypterat, för närvarande används RSA RC4 128bit. Detta är i dagsläget samma nivå som många banker ligger på. Krypteringsnycklarna kan enkelt ändras vid behov. Vid Internet styrning så kan IT ansvarig själv öka detta ytterligare via sina egna krypteringsinställningar för nätverket.
Utöver det så kontrolleras både *användarenamn* och *password* vid inloggning samt även att *systemnamn* överensstämmer.

12. Vad är RSA RC4?

Svar:
RC4 är en symmetrisk krypteringsmetod, utvecklad av RSA Security, som har används under många år, och som anses vara mycket tillförlitlig. Bewapass/Entro använder detta med 128 bitars stark kryptering.

13. 128 bitars kryptering låter inte så mycket! Mina e-mail krypterar jag med 1024 bitar!

Svar:
När man jämför krypteringsalgoritmer, kan man inte bara jämföra bittalet, eftersom olika krypteringsmetoder har olika styrkor. Bewapass/Entro använder en *symmetrisk* krypteringsmetod, till skillnad från t.ex. e-post program som vanligtvis använder PGP eller liknande, som är en *asymmetrisk* metod (med publika nycklar). Dessa metoder kräver normalt en större nyckelstorlek för att åstadkomma samma nivå av säkerhet.

14. Vad är MD5?

Svar:
MD5 är metod för att bekräfta meddelanden, och inloggningar. Detta används i Entro för att säkerställa att alla meddelanden är intakta när dom kommer fram, samt som en extra säkerhet vid inloggning via webbläsare till bokningssystemet.

B. Vilken redundans finns i systemet ?

Svar:
Vi kan notera att systemet allmänt bedöms som mycket driftsäkert. Driftstörningar härrör oftast till initiala problem i samband med installation (eller bristfällig dimensionering).
Om olyckan ändå är framme – så har Bewapass Entro en mängd tekniska lösningar som underlättar snabb felsökning och reparation. T.ex. jackbara, genomgående plintar som medför att anläggningsdelar kan bytas under drift.

Vid normala, preventiva insatser, så bedömer vi att Bewapass/Entro med sina övervakningsfunktioner och sin distribuerade intelligens är ett mycket gott alternativ i fråga om redundans till ett rimligt pris.

15. Varför batteribackup (UPS) 24Volt ?

Svar:
En av de bästa försäkringarna mot störningar, driftstopp etc. är att använda batteribackup i nödvändigt antal. En korrekt dimensionering vad gäller antal dörrar, låstyp, avstånd, kabeltyp etc är då givetvis en förutsättning.
Om anläggningen har möjlighet, så rekommenderar vi att varje SR32i central (med sina dörrar) får en egen batteribackup. Dels på grund av en ”renare” installation kabelmässigt, men också på grund av möjligheten att ansluta en fysisk signal från en batteribackup till SR32i. Varje anläggningsdel kan då övervakas separat och känna av om t.ex. nätspänningen försvinner. Larmsystemet i Entro skickar sedan ett internt larm till ansluten PC och/eller externt larm.

16. Vad händer om en undercentral SR32i får en tillfällig störning ?

Svar:
Såväl PC som andra SR32i har en komplett kopia på databasen (spegling). Så länge hårdvaran är intakt, men en störning sker så att t.ex. minnet slås ut- så återskapas informationen automatiskt genom att en återladdning sker. Kommunikationstoppet genererar ett internt larm till ansluten PC och/eller externt larm.

17. Vad händer om en undercentral SR32i går sönder.

Svar:
På grund av SR32i:s väl utbyggda isolationsförmåga så kommer troligen den överordnade (globala) kommunikationen att fungera. Om dörrmiljöerna fortfarande har spänning och innefattar en DC21 (med eget minne), så kan dessa gå över i ett autonomt läge där ett beslut, om giltiga kort, kan tas lokalt. Andra dörrar kan då vara låsta (eller olåsta). Då felaktig SR32i har bytts – så återstartas systemets funktion automatiskt via återladdning. Larmsystemet fungerar även här.

18. Vad händer om en läsare går sönder

Svar:
I de allra flesta fall kommer andra dörrar ”under” samma SR32i att fungera. Ett larm sänds även i detta fall från aktuell SR32i eftersom aktuell dörr ”försvinner”.

19. Vad händer vid kabelbrott

Svar:
Globala kommunikationsstopp (mellan SR32i centraler) upptäcks och sänder larm från respektive central. Dörrarna kan fungera som vanligt.
Lokala kommunikationsstopp (mellan SR32i och dörrmiljö) upptäcks av aktuell central och sänder även ett larm. Andra dörrar kan fungera som vanligt.
Kommunikationsstopp till PC ger samma effekt som PC:n avstängd – dvs all persondata finns kvar i anläggningen och en viss mängd händelser lagras även där. När kontakten etableras igen – översänds alla händelser automatiskt.