# Adv. Console Access (T12)

*Advanced Remote Console Access*

***version 1.6***

David K. Z. Harris
zonker@bigbandnet.com

This presentation will be temporarily available at:
http://www.conserver.com/consoles/LISA2002-T12.pdf





This presentation is a supplement to my console services web pages located at **http://www.conserver.com/consoles/**.

These pages have a substantial amount of information noted below each slide. I do this to help minimize the amount of note-taking that you need to do in class, and this should give you more time to listen to the tutorial. However, if you feel that you learn better by taking notes, please feel free to do so.

## About BigBand Networks

- BigBand Networks makes Digital Video grooming hardware for Cable and Satellite companies, to help them make better use of the bandwidth they now have.

Essentially, the hardware and software produced by BigBand Networks can aggregate information on a broadband network, turning a bunch of allocated frequencies into one “Big Band”, allowing the users to spread their data across many channels.

The serial consoles on the BMR chassis run at 115 Kbps, and are VERY verbose. The output is ideal for realtime system monitoring, and statistics gathering, but would be a horror to log for any significant amount of time.

While the chassis normally uses SNMP for management, the serial console also regularly streams information and updates. Administrators can use a Command Line Interface to manage the devices, and automated configuration can be done using ASCII text uploads, or send/expect scripts, etc.

If you are interested, you can find more information and white papers at http://www.bigbandnet.com/

## Pertinent Job History

- ***Network Equipment Technologies***
  - (Comdesign, Bridge Communications)
- ***Telebit Corp.***
- ***Cisco Systems, Inc.***
- ***Apple Computer, Inc.***
- ***Synopsys, Inc.***
- ***Global Networking & Computing***
  - (they became **Certainty Solutions.**)





Before moving into networking, I was a hardware hacker, working in repair and R&D roles. I have been tinkering with serial devices for more than a decade.

My experience, plus reading plenty of manuals, has taught me that there are a few safe bets that you can make when working with unknown serial devices. I've also learned a few tricks that make the job of connecting serial devices to terminal servers easier. I'll share these tricks throughout this presentation. You can also find some good, basic clues on my "Minor Scroll of Console Knowledge" (http://www.conserver.com/consoles/msock.html)

I've also been testing terminal server and console server hardware for a number of years, and I've posted some information about serial console remote access to the web that others have found useful. These pages are posted at my console info web site (http://www.conserver.com/consoles/)

## Useful URL's for after class

- **Conserver Software**
  - www.conserver.com/
- **Console Connection Guides**
  - www.conserver.com/consoles/
- **Serial BREAK testing**
  - www.conserver.com/consoles/breakoff.html
- **Serial adapters and cables**
  - www.americable.com
- **More at the end of the tutorial**




Celeste Stokely has a wonderful archive at http://www.stokely.com/, with lots of useful information for system administrators. Of particular interest is the page related to serial consoles;

http://www.stokely.com/unix.serial.port.resources/index.html

The **console and serial port switches** link on the page above has info about keyboard/video/mouse switches, RS-232 serial switches, and terminal server devices and console servers. (And if you aren't sure what some if these are, then you're in the right class.)

Americable has built a number of specialty cables and adapters for Console Server use, as well as bundling assorted kits for various Console Server hardware vendors RJ-45 wiring formats (Annex/Bay/Nortel, Cisco/Lantronix, IOLAN, and iTouch/Xyplex). If you need cables in custom lengths, they have the recipes, just call and ask for the parts.

## Why we're here today

- ***I'm here to inform you…***
  - So, I need to keep you awake!
- ***I've looked at a lot of options***
  - I like some better than others.
- ***If you don't pick Conserver, please pick something!***
- ***What's in it for you?***
  - This will save you time!

I'm presuming that you are already using some type of remote access to your serial consoles, or that you have already done some investigation on your own, and you're coming to this tutorial to learn more, or to try to solve a particular problem. I'm here to tell you about the information I have discovered over time, tell you what I've learned about various vendors and their hardware, and pass along some tips that may make it easier for you in the future to expand or upgrade your site(s).

If you don't use a logging server with your terminal server or console server hardware, then you should seriously consider adding one. I'll explain why, and help you evaluate your choices.

You can also use a serial console to report security events. There are some messages that are only available from serial consoles. On a Cisco router, when someone makes a configuration change via a telnet session, a notification message is sent to the console port.

Logging to a serial console, you can send output to a printer or another host without telling a cracker where the output is going! And if you send the output to a logging server, you can use other tools to sort through the data (looking for trends, triggering alarms, or performing forensics).

When properly configured, you can remove the video monitor (saving space). Even if you choose to keep the monitor around, you can save power and reduce heat in the room by turning the monitor off, and using the serial console for most operations.

## What We'll Cover

- Ø *Why console ports are good.*
- Ø *Console Server hardware options*
- Ø *Why worry about Serial BREAK*
- Ø *Add-on hardware*
  - ² Telemetry, remote power control
- Ø *Benefits of logging servers*
- Ø *Questions and Answer session.*




There are lots of good reasons why administrators connect to the console ports on their network. You probably know many of them now. We'll discuss many them briefly in class, as we review your options, both adding multi-port serial cards to your hosts, as well as using Console Server Hardware to connect to consoles around your network. We'll look at the security issues, and discuss ways to mitigate them.

We'll consider whether you need to worry about Serial BREAK, and look at optional serial-port-based equipment that you may want to add to your network.

Finally, we'll talk about how you can increase the value and benefits from your new console access by adding a client-server application between you and the terminal servers. In some cases, free software can add value to your terminal server investment.

I'm planning on having time at the end for to open the floor for questions and answers, to try to fill in any blanks you may still have. There will be a Conserver BoF as well, Wednesday night, in case folks want to have a follow-up, and to meet folks who couldn't attend this tutorial.

We will not go deeply into physical-layer connectivity and debugging in this class, due to time constraints, but I'll be glad to address questions individually after class, or at the BoF. There are also lots of links at the end of this presentation that you should find useful for independent follow-up when you get back home.

## How do you work today?

- How many of you, in class today, are still on-call?
- How many of you are PRIMARY on-call for some task today?
- How many have deployed consoles remote access?
- How many can access important consoles at your office, from the conference today, SECURELY?



Pg. 7

If you support many machines, you may be called often to check on one of many devices,perhaps in many different locations.

If you only support a few critical machines, being able to diagnose a problem quickly is important to you.

Maybe you need to support your companies e-presence servers, In this case, time is money, and downtime is money lost!

Remote access to your serial consoles can let you quickly diagnose a problem, and can help you recover from many problems. It can even give you the clues you need to decide if you have to go visit the machine personally, but you will also probably know what parts you need to bring with you, which will save you a second trip.

Sure, your job could become a bit more sedentary, but you'll be able to go and get some exercise, knowing that you can quickly get on the console of any device that you care about if the need arises.

## Why Console Ports are Good

- ***Sometime debug (trace, etc.) is best used on a console port.***
- ***Some security modes, including logging functions, can use serial consoles (some need to…)***
- ***Helps reduce heat generation and power consumption.***
- ***Even PC servers can run 'headless' (lights-out colos).***
- ***Downtime Costs Money!***





When you are trying to capture data from a network interface, you usually don't want to send the captured data results back over the same interface you are monitoring. If you only have a single network interface, the console port lets you manage the network interface without contributing to the traffic.

Sending messages to SYSLOG is good. Sending them out the console port as well is better. A cracker can figure out where your syslog data is going, but they can't tell where data goes once it leaves your serial port. (Even if they manage to modify the log files, they would be hard pressed to find your console data!) We'll discuss logging your console data later in the tutorial.

CRT-type displays take up a lot of room,consume a lot of power, and generate a lot of heat. In large data centers, with dozens of machines, you cannot afford to have one display per machine, and it's difficult to justify a 1:4 or even 1:8 display-to-machine ratio.

There are even options to run your PC-class hardware without a display, using vendor-supplied BIOS, or an add-in EISA or PCI console card. (See the PC Weasel information at the end of the slides.)

## What might you connect to?

- **Hosts**
  - workstations, servers, NMS hosts
- **RAID arrays, Network App Filers**
- **Network equipment**
  - including devices without IP stacks
  - CSU/DSU, TA
- **Telecom gear.**
- **Security devices.**

© 2002
David K. Z. Harris Pg. 9

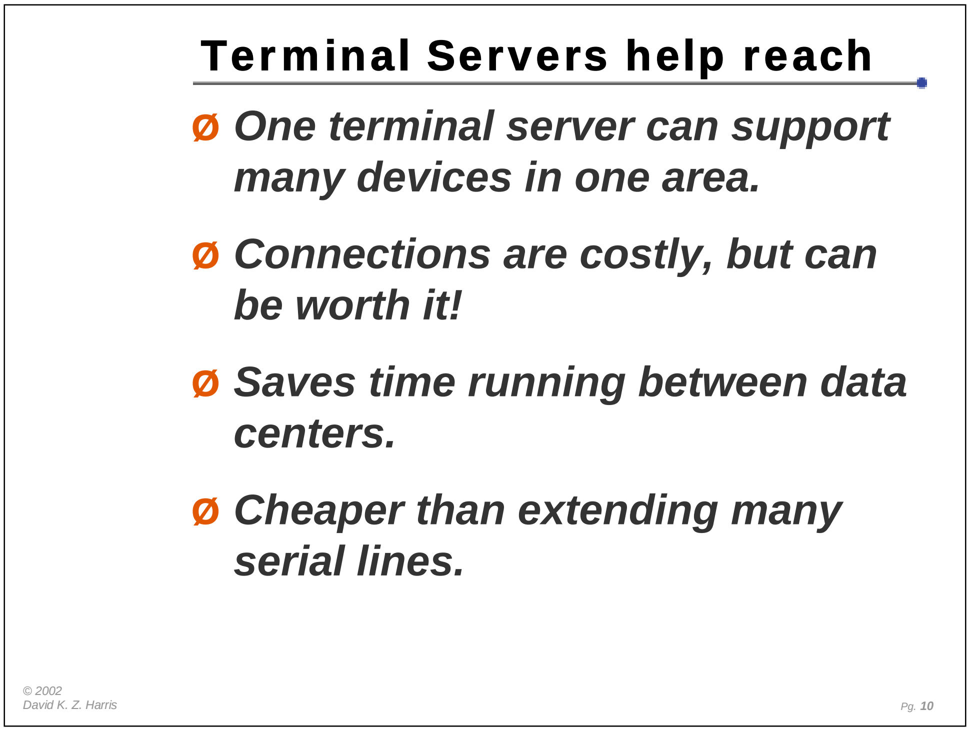
Console ports are not cheap, so we want to use them sparingly.

On the other hand, using a terminal server, you can easily get 16-32 ports in a single device, which may be more than you need initially, which then allows you to connect devices that you may not have considered valuable enough to connect in your initial plans.

Consider that any port that you connect to a terminal server can be logged using an additional logging server. What information do you think is important to capture? These ports should be connected.

If a device constantly repaint, or updates its screen, you may not want to capture the data to a log, but you may still want to connect it, so that you can get to that port from some other place.

Because the terminal server will likely be a capital investment, you may want to share the cost with other departments, and allow them to connect some of their devices to some of the ports.




If you have a bunch of devices at a remote location, you likely have a network already in place for the devices. Usually these are hosts in a remote data center, but they could include network gear in wiring closets, or even a remote site with telemetry and control equipment. In these cases, the terminal server becomes one more addressed device on the network, and it can connect to dozens of devices at one time.

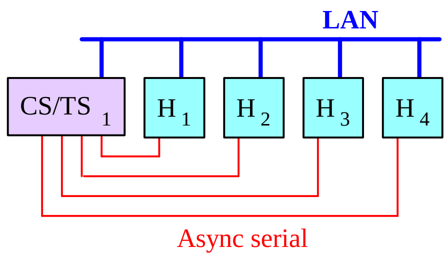
The cost for a 10/1000 switch port is currently cheaper than a serial port some of the expensive terminal servers. However, the costs for the serial ports are beginning to drop. (And they are still cheaper than gigabit ethernet ports!)

The value of deploying terminal servers is from the reduced downtime because technical staff can fix problems more quickly when they can get to the consoles of ailing devices more quickly.

You can use serial extenders, if you have plenty of fiber between the main and remote console locations, but that fiber has value to you as well, which affects your cost equation.

## Basic Serial Hookups

- Console Server connected to the same LAN with the hosts
- Serial connections from the consoles of each host to the Console Server








In the most basic configuration, you connect all of the consoles that you care about to a serial port on a Terminal Server or a Console Server.

Each serial port can be configured for different serial speeds (that is, for any of the common serial speeds), as well as setting the number of bit, parity, and stop bits.

In a simple, isolated deployment, the console server would be connected to the same ethernet network as the hosts. (We'll discuss other connection options later in the tutorial.)

The console server could be a host with a multi-port async module, or a dedicated Console Server device. If the console server is a host, with it's own keyboard and mouse and screen, it may not need to be connected to the network at all.

## Terminal Server Magic

- ***Reverse TCP (Reverse Telnet)***
  - Basic functionality these days
- ***Workstation telnet to TS address:port***
- ***Vendor-specific port formulae***
  - Port ranges are well known…
- ***Vendor-specific features***
  - Not consistent from vendor to vendor
- ***Hackers will look for these!***




Originally, modems or 'dumb terminals' were connected to terminal servers, and users would telnet from the terminal server to other points around the network. Today, most terminal servers allow you to open a socket-based connection to the IP address of the terminal server, but at a high TCP port number, to connect to a particular serial port. (This was known as Reverse-Telnet, because it was the reverse direction to the normal direction of attached terminals using telnet to reach hosts and servers around the network.)

Some vendors allow only 7-bit sessions, while others provide the option for full 8-bit sessions, and even "non-escapable" sessions (where the attached device needs to drop the DCD or hardware handshake lead to disconnect your session).

The list below tells you the formulae to determine the TCP port number for two of the more popular terminal servers (where 'n' is the line (serial port) number you wish to connect).

Cisco: 2000 + n (7-bit), 4000 + n (8-bit)

iTouch/MRV/Xyplex: 2000 + (100 * n)

IOLAN: 10000 + n

Hackers know to port-scan for these, so hide them well!

## Terminal & Console Servers

- ***Terminal Servers were designed to allow ‘dumb terminals’ to access hosts on IP networks.***
- ***Reverse Telnet allowed users on the network to connect to serial ports on terminal servers***
- ***Console Servers are a newer, enhanced Terminal Server, meant for supporting console access.***

Terminal servers are still readily available, and you can pick them up fairly cheaply on eBay, or other dot.com auctions.

However, Terminal Servers didn’t need to care about Serial BREAK in the old days, and sometimes it was designed to send BREAK when sessions cleared up (to reset a modem, for example). So an older unit may send Serial BREAK to attached devices under some conditions. If you have SUN computer consoles attached to your terminal server, a BREAK can halt your SUN.

Serial BREAK is actually a Good Thing, in moderation, and useful for administration of your hosts. You can get more information from my Serial BREAK-off testing pages, http://www.conserver.com/consoles/breakoff.html

Newer Console Servers are generally better about not sending Serial BREAK at the wrong time, but if you have SUN gear, you should make sure that the equipment you are buying is marked “Sun-safe”, or otherwise states that it won’t send Serial BREAK unless you want it to.

Console Servers also typically have better documentation for their implementation of the reverse-TCP connection, and more features for remote access than ‘terminal servers’.

## An Important Distinction

- **_Console Server Application_**
  - A host running software for controlling access to serial consoles around your network, for logging and administration tasks
- **_Console Server Hardware_**
  - A device running  software, which allows connections from across a network to reach serial ports connected to the device.




With the advent of “Console Server” hardware, some distinctions needed to be made. Without these distinctions, discussing Console Servers becomes a bit vague, and can become confusing for the participants.

Consider a host, running a Console Server Application, but also having a multi-port serial board, attached to some serial consoles on other hosts. It serves both of the purposes defined above, controlling access, and logging data, while it also moderates the connection from the Console Server Application to the hardware serial ports. I consider this a Console Server Hybrid.

## Terminal server advantages

- Admin can operate many consoles at once
- One serial port per socket-based session
- Easy to cut-and-paste between sessions
- Different administrators can talk to many different attached devices at one time.

 Pg. 15

It’s common to open many windows to different ports, so you can copy and paste between them.

Many administrators can work with different hosts simultaneously, from different workstations, rather then waiting in line to use a shared terminal or laptop.

Only one person can be connected to each port at any given time. This is normally a good thing, as it can prevent two administrators from making configuration changes at the same time, providing that you make it a policy to make changes from the serial console. If another person tries to connect to a busy port, the connection is refused, with a message to the user.

There is a downside to this, however, in the case that one administrator connects to a port, and then goes to lunch, or home. With the idle session still connected, nobody else can connect to that same port. (Someone with administrator privileges on the terminal server needs to log onto the terminal server, and reset that serial port to break the connection.)

## Terminal Server Disadvantages

- It's not cheap to deploy.
- Only one person can connect to a given port at one time.
- Hard to tell who is connected, if a given port is already busy.
- Difficult to kick someone off if you need to access a port.
- If nobody is connected to a port, incoming data is lost, not logged




Reverse TCP connections are good, and useful. But when you are done with a connection, you must release the connection, or others will not be able to connect to it.

If a port is already in use, your connection is refused, but you don't know who is connected. You will need login privileges on the terminal server to try to find out, and to reset the port to clear that session. Such access to the terminal server would normally be restricted to a few users, which may make it difficult to clear a port quickly.

If nobody is connected, data coming in from attached devices is usually lost forever. (Lightwave Communications 3200 series servers have a 64KB-per-port cyclic buffer, so you do retain some port data if nobody is connected.)

With a logging Console Server application, the application makes the original reverse-TCP connections to all the ports you care about…any incoming data is logged, and (multiple) clients can connect to the (same) sessions through the application server.

## Think About Security

- ***Do you have a security policy?***
- ***Does it consider remote access to serial consoles?***
- ***How concerned are you about 'internal' threats (snooping)?***
- ***What are you trying to protect?***
- ***What is that worth to protect it?***
  - The classic budgeting questions




We will discuss some security issues in this talk, but security is a touchy subject, and a few aspects of most cases are unique.

Due to this, we will discuss general points during the class, and the materials will give you some questions to think about and discuss.

During the conference, we will be holding a Birds of a Feather session, and we'd welcome any additional questions there, if you are comfortable asking them in that forum.

The biggest worry is whether you are concerned with the console traffic being monitored within your network. (Most companies use a "jelly bean" security model…hard on the outside, soft on the inside…meaning that they are not too worried about folks on the inside sniffing the wires.)

In a switched ethernet environment, it's harder for folks to see the packets to and from the terminal servers.

If you have a console server host, you should consider if it is worth making that host single-purpose, and limiting the login accounts

## Terminal Servers and Security

- ***Some vendors are adding SSH to their devices***
  - How will you manage accounts across many boxes?
  - Can they authenticate against an existing server?
  - What happens if they can't reach the server?
- ***Security is still new here...***




SSH has become a vital checkbox for many vendors to add to their terminal servers and other network devices, but the interoperability of the actual implementations, architectures, and failure modes are still far from good. You can get some single-vendor solutions running if you need them today, but you may not be able to integrate it later with other gear that you'll want or need.

Ask your vendor how to manage multiple accounts across multiple terminal servers. What happens when a user changes their password on one device…how does the change propagate to the other devices?

If you authenticate against a central authentication server (ala Cisco TACACS+, or RADIUS), what happens to user authentication if contact with the authentication server is unavailable? (This is an issue for terminal servers in remote offices if the WAN should fail...do you want to install and maintain multiple authentication servers in various offices? Can that management be automated?)

You will have more flexibility if you can implement a management network, to provide the level of security for physical access to the logging and client session data streams.

If you feel you need to add SSH today, you may be limiting your options. Of course, this will change over time, as customers push vendors to address the interoperability issues.

## Who are the vendors?

- *Many players are still in the game*
  - Cisco, Cyclades, Digi, Lantronix
- *Some players have changed.*
  - Computone became Symbiat
  - Xyplex became MRV…
    - (nBase -> iTouch -> MRV)
  - IOLAN became Perle
- *The market is still growing!*



Pg. 19

Cisco has been taking remote access to consoles fairly seriously (Worldcom was very fond of the 3600 family). Cyclades has been in this market for more than a decade, and is a strong player. Digi and Lantronix are still doing well these days.

Computone had been on the ropes in the Point of Sale market, but then they decided to make terminal servers for that arena. This saved the company, but they needed to evolve their product. The economy didn't wait, and Symbiat bought them. You can't find terminal server hardware on the new web pages. They are now out of the hardware business. The shame is that the new products Computone was developing were coming out quickly, but not quickly enough. They also had the BEST Users's documentation I have seen to date.

Xyplex all but died, and was acquired by nBase, who didn't evolve the product, although MCI was very attached to this product family. iTouch Communications took over the line, and continues to sell the older line, but they have evolved new products to be Sun-safe, and expanded the line! They will still support the older gear as well. MRV, the mother company of nBase and iTouch is changing the logo and color, but features will remain the same.

The (Chase Research) IOLAN line was acquired by Perle, who also picked up the Specialix line as well. You can still get the old IOLAN products, but the newer Perle CS line is a very nice family.

## Vendor Links

- ***Cisco Systems***
  - The 2600 and 3600 series.
    - 3660 line numbers are 33-224!
    - IOS 12.05(t), look up UDPTN
    - Async input, multicast output!
  - Use the NM-32A 32-port modules.
  - Americable sells patch panels.
- ***Xyplex, iTouch Communications***
  - The InReach line is now “Sun-safe”
  - The iTouch Xyplex family is not!
- ***Both RJ-45 ports are symetrical!***




Terminal Server Vendors

Cisco Systems http://www.cisco.com

http://www.cisco.com/univercd/cc/td/doc/pcat/2600.htm

http://www.cisco.com/warp/public/cc/pd/rt/2600/prodlit/2600_ds.htm

http://www.cisco.com/warp/public/cc/pd/rt/3600/prodlit/seral_ds.htm

http://www.cisco.com/warp/public/cc/pd/rt/3600/prodlit/3600_ov.htm

Xyplex (was nBase, now iTouch Communications, becoming MRV)

http://www.itouchcom.com/products/index.cfm?cat=scs

http://www.itouchcom.com/news/display.cfm?nwid=2002_07_01

Use the Americable Xyplex adapters for the InReach family as well!

Adapter Vendors

Americable 800-328-7954 http://www.americable.com

http://www.conserver.com/consoles/ciscokit.html

(also annexkit, iolankit, and xyplexkit)

## Vendor Links, cont'd.

- **Cyclades**
  - Built-in Linux core
  - TS2000 is a great device!
  - PC multi-port cards available
  - Most products are Sun-safe
- **Digi Communications**
  - Many devices available
  - PortServer CM is a good tool
  - Many products are now Sun-safe




Cyclades and Digi are both long-time makers in this arena.

Cyclades was the first (and only) console server hardware we found in our Serial BREAK testing that had a software-controlled BREAK problem. Once the recipe was sent on how to demonstrate the problem, we received a patch within a few days which resolved the issue. The TS2000 hardware was also enhanced during the design phase to ensure that the BREAK problem did not exist in the final product.

http://www.cyclades.com/products/ts_series.php

http://www.cyclades.com.pe/Productos/Anexos/ReleaseSerieTS.txt

Digi has also entered the Console Server hardware arena, with the PortServer CM product line. The CM32 is also a good fit with Conserver. The existing PortServer Terminal Server line is also still available.

http://www.digi.com/solutions/devtermsrv/cm/index.shtml

http://www.digi.com/solutions/devtermsrv/termsrv/index.html

support.digi.com/support/techsupport/hardware/portserver/sun_console.html

## Vendor Links, cont'd.

- **_Perle (Perle Systems Ltd.)_**
  - CS9000 is Sun-safe
  - Cables, status LEDs on same side
    - Good or bad? You decide…
  - Good integration with MS Windows
    - May be useful in a mixed environment
- **_Lantronix_**
  - Still a workhorse in the industry




Perle System took on the Chase Research IOLAN line, as well as Specialix products. You can still get support, and buy hardware from Perle if you want these lines. (The IOLAN model 102 and 104 servers are Sun-safe.)

The Perle CS9000 is comparable to the Cyclades TS2000, and the Digi CM32, in that they are all 32 ports, Sun-safe, I rack-unit tall, lightweight. One difference that stands out, to me, is that the transmit and receive data LEDs on the CS9000 are integral to the RJ-45 jack, putting them on the same side of the unit as the cables. (On the Cyclades and Digi units, the LEDs are on the opposite side from the jacks.) Whether this is a benefit or a deficit in your mind will likely depend on how you decide to mount the units.

http://www.perle.com/products/prod_family/console_server/cs9000.html

http://www.perle.com/products/resources/pdfs/CS9000%20Dis%20paper.pdf

http://www.perle.com/products/prod_family/serial_servers/iolan_pl.html

Lantronix has been making serial-to-network interfacing devices for over a decade, and should also be on your list of candidates to investigate.

http://www.lantronix.com/products/cs/index.html

http://www.lantronix.com/learning/tutorials/ds.html

http://www.lantronix.com/learning/wp/conserv_wp.html

## New or old? New or used?

- Do you need support?
- Do you need software?
- Are you trying to expand an existing deployment?
- Can you afford to learn and deploy something new?
- Do you need new features
  - SSL? SSH V2? Sun-safe?




Synopsys had a working installation, based on Xylogics Annex hardware. Even though it sent Serial BREAK on power-off, they kept it. Even after the product line was bought by Bay Networks, they kept it, because they could still buy compatible hardware. Only when Nortel Networks bought Bay Networks, and killed off the product did Synopsys move to the costlier Cisco hardware, and then they retrofitted the Cisco gear across the entire enterprise, replacing all of the older units.

Many folks have been buying older units cheaply, on eBay. But the units didn’t come with their software media (floppy disks, or PCMCIA flash cards), so they wouldn’t boot. If you don’t get the software, and manuals, the unit probably costs too much!

iTouch Communications will still support older Xyplex terminal servers, for the cost of a support contract. Ask yourself how much your hardware is worth if it doesn’t work…and how much is it worth to keep it working.

For larger organizations, buying new is probably worth the cost. You’ll want on-site spares, or a service contract. You’ll want a consistent user interface and features across your enterprise network. And you’ll want to be able to buy more of them next year…

## Security Concerns and Costs

- ***Which network will you connect your devices to?***
- ***In compliance with Security?***
  - SSH? SSL? Radius or TACACS+?
- ***Extending your management network may add cost to your terminal server deployment.***
  - Network links between data centers
  - Extra switch/hub ports
  - Cost-per-port is a bad metric because

If your site is small, you may not have the security overhead, but as you move into larger enterprises, there may be security policies that you need to be aware of before you deploy, so you should investigate the security issues **before** you buy hardware.

Determine which network(s) will host the terminal servers. Do you have available network capacity? Sufficient physical space, power, and cooling?

Is your deployment in compliance with any existing security policies? (You may not be able to connect to certain networks, or you may not be allowed to extend those networks into certain non-secure areas, or you may need permission first.)

You may plan to put the terminal servers on the management network for security reasons. But find out if that network is currently in the area(s) where you want to put the terminal servers. (You may need to use media converters to let you use spare fiber between data centers, or add memory to routers to allow you to use encrypted tunnels, etc.)

Do you have enough open network connections in those places, on those networks, reserved for your terminal servers (or do you need to order more hubs or switches)?

## Choosing your hardware

- *Port densities needed?*
- *Number of devices needed?*
- *Cable lengths an issue…*
- *Would BREAK be a problem?*
- *Do you prefer certain vendors?*
- *Budget concerns…*
  - Patch Panels, or jacks in chassis?
  - Cables and pre-wired adapters





Choose your port densities with cable lengths in mind, since you want to keep your serial cable lengths shorter than 50 feet (16 meters). While most devices can drive a signal farther, some cannot, and those shorter lengths will prove to be limiting during your deployment phase. The cable length and the number of devices will help you decide how many terminal servers you should have in a given data center, and where they should be placed.

If you are serving large numbers of ports, you should consider purchasing multiple terminal servers, and distributing them around the data center, rather than having a single, large server. This becomes your classic “single point of failure” discussion.

Some devices are sensitive to the serial BREAK signal. (Test equipment, modems, and Sun hosts are the most sensitive.) If the serial BREAK would be a problem for some of your devices, your choice of vendors will be smaller. Consider whether you need to plan for ‘partner’ networks, or future mergers…

Console servers are expensive, but the payback comes from minimized downtime. You can add more value to the capital investment by adding free logging software. In addition, you may be able to deploy a modular console server, starting with fewer ports now, but with the ability to add modules later, thereby spreading the cost over a few fiscal quarters (maybe even bridging fiscal years).

## Supplemental Costs

- **High Availability costs more**
  - Service Contract?
  - On-site Spare Equipment?
- **Ancillary Cables and Adapters**
  - CAT-5 cables for patching
  - Patch Panels? Adapters?
  - Distribution Wiring (Rack-to-rack)
  - Test equipment (Signal Tracers)




When you come to depend on some infrastructure equipment, you want to ensure that a hardware failure does not cripple that infrastructure.

If you are ordering a large number of smaller servers, you can probably afford to buy an additional unit to keep as a “hot spare”. If a module or component fails, you can swap a working part from your spare, and then pursue the RMA for the filed component.

When you are using larger servers, that spares cost is higher, and the high cost may be too much to bear. Your options can include paying for a higher level of hardware support from the vendor, that can include short turn-around time for RMA parts, and/or advance swap components. The cost of this higher service contract will be a recurring cost, year after year, but it isn’t the single, big cost for the spare unit.

Remember that the spare unit does not need to be fully stocked! If you have a terminal server with multiple slots, you only need one or two modules for spares use, rather than filling all of the slots.

When you are purchasing your terminal servers, remember to order sufficient stock of RJ-45 adapters, and and needed patch cables (and patch panels?) that you will need to deploy the terminal servers. You should also have an adapter kit, with one of each standard adapter for that terminal server, as well as passive signal tracers for troubleshooting.

## Evaluating the Hardware

- **_Cost per port is just one metric_**
- **_Security features may be needed_**
  - Do you need SSL or SSH access?
    - What version(s)? Interoperability…
  - How often, how many, how long?
- **_Size and port density_**
  - Rack space may be valuable
  - How many ports do you need?
  - Wiring, adapters, patch panels




While many Console Servers now have SSH access capability, SSH V.2 capability has been slow in coming.

Most vendors blanch when you tell them you want to make 32 simultaneous SSH connections to their Console Server, and they'll ask "For how long?", indicating that their SSH may have memory leaks, or SSH sessions may severely tax the performance of the device. (I haven't done a large-scale test, with 32 busy async devices connected to a console server, using SSH to connect to all of the ports, but I also haven't found a vendor who wants me to put their gear up to that test, either.)

SSL access is also starting to be offered by vendors, but then you need to manage certificates.

None of my vendors wanted to discuss where their SSH and SSL core code have come from. But, few Console Server devices have been listed on the SANS vulnerability alerts…

Interoperability between your Console Server hardware and your standard Operating Systems should be investigated, and tested. What will you do if an SSH upgrade or patch breaks the interoperability with your Console Server hardware? How soon can your vendor(s) restore communication?

You may want to consider buying more console servers, and deploying them in your racks, instead of using patch panels and infrastructure wiring to keep the console servers centrally located. Investigate your infrastructure costs, both parts and labor!

## Is Serial BREAK a problem?

- ***The answer varies, site to site***
- ***The answer today may change in a year, or a month.***
  - Corporate acquisitions and mergers
  - Strategic Partnership networks
  - “Visiting Hardware” for developers
- ***More information is available on www.conserver.com***

Older SUN hardware is vulnerable. So are older SGI IRIX machines. Newer SUN machines can be patched and modified. Modems may react badly to BREAK, depending on their configuration. Some telecom test gear is rebooted, and setting reverted by serial BREAK.

Newer console servers don’t cause this problem. I’ve been testing a variety of terminal server and console server hardware, to see which devices send Serial BREAK without the operators instructions. You can find the testing results on http://www.conserver.com/consoles/breakoff.html.

If you only have one or two devices that are susceptible to BREAK, you may be able to connect them with Nu-Data Cisco Serial interfaces (cost is ~$100 per port). If you have more than a dozen ports to protect, you should consider purchasing a Console Server that won’t send BREAK unless you tell it to.

Sun has fixes available (patches and work-arounds) for more recent versions of Solaris. You may need access to SunSolve

## Terminal Servers and Security

- ***Some vendors have added SSL and SSH to their devices***
  - How will you manage accounts across many boxes?
  - Can they authenticate against an existing server?
  - What happens if they can't reach the authentication server?
  - Do you have assorted hardware?
- ***Security is still new here...***





SSH has become a vital checkbox for many vendors to add to their terminal servers and other network devices, but interoperability is still far from good. You can get some single-vendor solutions running if you need them today, but you may not be able to integrate it later with other gear that you'll want or need. It's also not clear whether Console Server hardware SSH V2 implementations are vulnerable to issues on the security bulletins, since most will not disclose where they get their SSH V2 source code.

Ask your vendor how to manage multiple accounts across multiple terminal servers. What happens when a user changes their password on one device…how does the change propagate to the other devices?

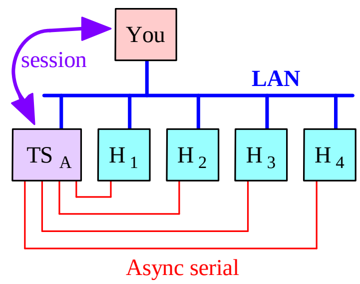
If you authenticate against a central authentication server (ala Cisco TACACS+, or RADIUS), what happens to user authentication if contact with the authentication server is unavailable? (This is an issue for terminal servers in remote offices if the WAN should fail...do you want to install and maintain multiple authentication servers in various offices? Can that management be automated?)

You will have more flexibility if you can implement a management network, to provide the level of security for physical access to the logging and client session data streams. This may still be the most practical way to secure access to your sensitive consoles and data.

If you feel you need to add SSH today, you may be limiting your options. Of course, this will change over time, as customers push vendors to address the interoperability issues.

## Basic Architectures (#1)

- *Adding Terminal Servers*
- *Everything on the same network (the 'no security worries' model)*
  - TS = terminal server Hn = hosts







This presumes that you are not worried about someone on your internal network sniffing the console sessions. In a small network, this provides the convenience factors (fewer display devices, no switchboxes, and different serial port speeds don't bother us).

The terminal server is connected to the serial consoles that we care about, with speeds set on the various terminal server ports to accommodate the speeds of the attached devices.

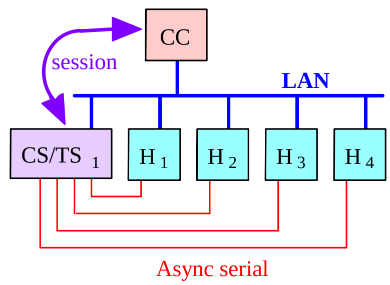
The administrator(s) can sit at their workstations, and connect to the serial ports that they want to control (using Reverse Telnet).

Remember that only one administrator can connect to any given serial port at once in this configuration. (Although administrators can connect to many different serial ports at one time.)

If nobody is connected to a serial port, and data coming in from the attached device is lost. If someone *is* connected and watching, you still only have as much logging as your scrollback buffer will provide for each session.

## Basic Architectures (#2)

- *Adding a logging server*
- *Similar to Terminal Server Deployment*
  - CS=console server app
  - TS= Terminal Server   CC=client







In this configuration, we still don’t worry about internal security.

In this case, the Console Server (CS) has multiple serial ports installed, connected to the various consoles that you care about.

Any data coming in from each attached device is appended to a log file for that specific device. (As an administrator, you may need to watch the size of the log files, and rotate them occasionally.)

In our example, you would use a client (CC) to connect to the console server (CS), and attach to the console logging session that you want to talk to. Anything you type on the client goes to the serial console you are talking to, while anything coming back from that console is logged, and then sent to the client(s) attached to that session.The client software, and/or the server software, watch the data stream from the user, looking for meta-characters coming from the client, to allow for session control.

Some console servers allow more than one client to attach to a single  session at once. All clients see the data coming from the attached device, but only one client can type to the session. (Conserver behaves in this manner.)

## Adding a Console Server App

- **_Combination Server (CS/TS)_**
  - Logging server equipped with multi-port serial card(s)
- **_Separate Server Devices_**
  - Console Server App on the network
  - Terminal servers attach to devices
- **_How to decide which is best?_**




Some console server applications allow you to add some multi-port serial interface cards, and attach serial consoles directly to the console server. In the preceding illustration, we showed this as "CS/TS", because the Console Server is also performing the serial attachment duties of the Terminal Server.

Conserver can support this mode, although we don't normally recommend it, except in small, non-production environments, because you are usually going to be limited by how many serial ports can be hosted on the CPU. (This is a function of the number of spare slots, and the number of poets per card. You wouldn't usually see more than 96 ports on a single server in this mode.)

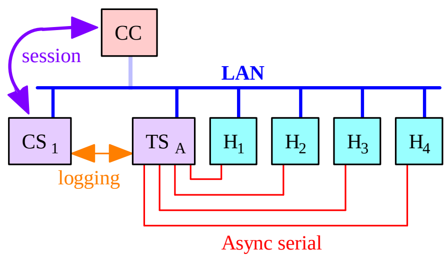
A secondary concern, in our mind, is that the serial ports will normally send a serial BREAK signal when you power-cycle the CPU. In a Sun environment, that signal on the console will halt the server, and you'll have to wait until the CPU boots before you can get back on each console individually and type "go".

The main advantage of this mode is that the logging traffic is kept within the computer, rather than on the network between the terminal server and the console server. (The network load is only partially reduced, since the client sessions still traverse the network to get to the console server.)

As a result, the security issues of sniffing the logging traffic is also reduced, but the client sessions are still exposed, unless the client can use SSL or SSH for the connection to the console server.

## Basic Architectures (#3)

- **_Combining a Console Server App with Terminal Servers_**
  - You can add multiple terminal servers
  - You can mix terminal server types/vendors








This is the most versatile configuration, in our opinion. Again, security on the internal network is not a concern in this model.

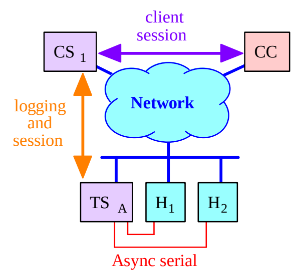
You can get more ports on a terminal server (TS) than you can practically add to a console server (CS) host. And, you can add multiple terminal servers around the network. All of the logging traffic travels from the terminal server to the console server over the same LAN as the host communications and everything else.

If you are using a switched ethernet network, you are already gaining some practical protection from folks sniffing the console sessions.

The logging traffic from the terminal servers are fairly light, even from a large number of busy hosts. Your mileage may vary, of course, as you increase the amount of data that you are logging, and the number of terminal servers that are added around the network. (This traffic is normally contained with the Console Server when you are using built-in serial ports only, instead of terminal servers.)

## Basic Architectures (#4)

- ***Client can access from anywhere on your network***
  - Terminal Server is located physically near consoles
  - Console Server App host doesn't have to be close to monitored consoles.








The console client (CC) can be anywhere on your network.

+ dialed in from home (through your dialup authentication)

+ across the network; on another floor; in another building

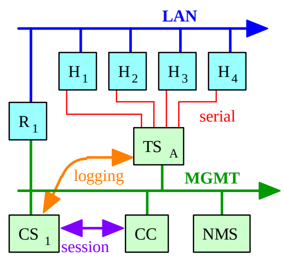
+ across the WAN, from another location

If you need to access across the Internet, we suggest that you use SSH to get to your home network, and then use a client on a machine on your network, rather than using a client on your laptop from the terminal room, for (we hope) perfectly obvious reasons.

Asynchronous serial connections do have length limitations, so you need to have your terminal servers (TS) close to the devices that you want to control remotely. (If you are using serial cards in your Console Server (CS), then that also needs to live near the equipment that will be attached to it.)

## Advanced Architectures (#5)

- **Addressing Security Concerns**
  - Add a management Network
  - Put Network Management Station on this network
  - Put Console Server and clients there








If you are concerned about someone sniffing the client-to-server connections, or the logging streams, then you probably already have a control/management network in place, where your monitoring and control activities take place.

If you are concerned about someone sniffing your console port sessions, and you don't have a dedicated management network, you may be able to implement one easily with a small, robust router, and another Ethernet switch. You need to decide which host(s) can pass traffic through that router…

In this model, the console server (CS), and the client(s) all live on the management network along with the terminal server(s), so that the client sessions, and the logging activity, all happen on the management network.

A good practice is to ensure that your management network is connected using switches, rather than hubs…

Few console servers use SSL or SSH for the client-to-server connections, so these sessions travel in clear text. For this reason, if you are located outside of the management (or security) perimeter, you should consider making an SSH connection to a client host that is on the management net, and then making the client connection from there.

## Security Issues

- It’s easier to maintain secure communication to a Console Server Host, than it is to make secure connections to Console Server hardware.
- Take steps to restrict access to your console servers and logs.
- Centralize your access rights.





Remote access to your serial consoles will become an invaluable tool (if it isn’t already). It can easily become a major part of your administration foundation. Because of this, you will want to ensure that your deployment is sturdy, and reliable.

With Console Server Hardware, you can often use a centralized authentication server (using RADIUS, for example). However, if your workstation clients need to patch/upgrade their SSH version, you could break your access to the console server hardware.

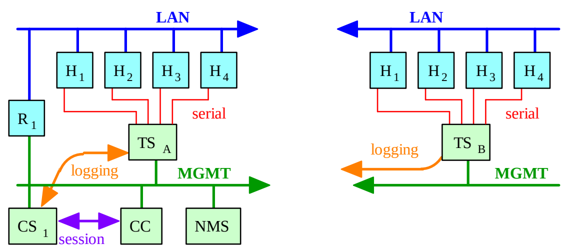
It may be easier to have a logging console server application host, managing the access to the serial consoles. The presumption is that your workstation clients will be using the same OS and SSH code as your console server application host, which would minimize the chances that a patch/upgrade would break host-to-host communications.

You should minimize the number of accounts that have administrative access to your Console Server application host, as well as to your Console Server hardware. Clients do not necessarily need to have shell access to the host/hardware.

Managing who has what access is best done from a central database, rather than needing to make duplicate changes across multiple machines.

## Advanced Architectures (#6)

- **Security for large networks**
  - Physically extend Management Net
  - Requires additional resources
    - fiber runs, hub/switch ports, etc
  - $R_1$ is a router connecting the networks








If you have a need to support multiple data centers, you may want to extend your management network to those other data centers. (Remember that serial lines have fairly limited distances, and it is easier to extend an ethernet network than to extend serial lines.)

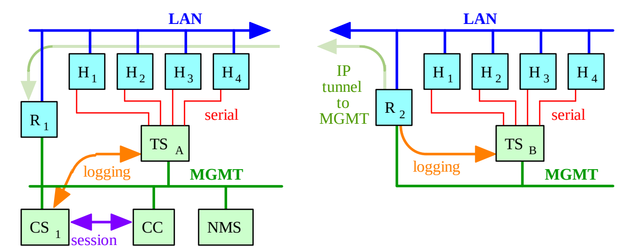
If you have additional fiber pairs between the data centers, you can do this with media converters.

Adding capacity for parallel networks between data centers is an expensive project. The commitments for your fiber may extend to your security needs, telecom systems, and more.

Even if you have enough capacity today, your needs may change in the future. Since you are extending a management network, you should try to think into the future, and plan for a connection that will stand the test of time.

# Advanced Architectures (#7)

- **Security for large networks**
  - Distributed Terminal Servers
  - Use encrypted IP tunnel
  - Management Net is more secure








In an environment where network connection paths are limited, you may want to consider adding an encrypted tunnel from one of your management networks to another.

This may cost you some more memory for the routers, and it may drive you to increase the bandwidth if you are communicating over a WAN link.

It may even push you into a larger router with more capacity (or a hardware compression solution).

When considering this plan, try to think into the future. If you are ordering more RAM, more bandwidth, or a more powerful router, will it be capable of the growing needs of your network.

Changes and upgrades often mean downtime, and you may as well try to do one change instead of many.

## Free software adds value

- Logging
- Forensics data
- Mentoring
- Data for other Apps
  - Netcool
  - Swatch




Terminal servers give you easy access to the serial ports around your networks. A logging console server will open a reverse telnet session to each of the serial ports that you care about, and log any data sent by the attached devices, even if nobody is connected.

Logs provide good forensic data after a crash, break-in, or other problems, especially if nobody was looking when it occurred.

A good console server allows many users to watch a session at the same time,while allowing only one session to write, allowing junior and senior level staff to work together, creating a great mentoring environment.

Each device being logged has a separate log file, which can be easily searched (if you have proper access privileges). Scripts can do this automatically. Some applications (SystemEDGE, from http://www.empire.com) can watch logs for specific messages, and then send alerts or alarms to administrators, or even to other applications, such as network management workstations.

## Console Server App. Costs

- *Software can be free*
  - Commercial solutions ARE available
- *Can be run on an existing CPU*
  - You may want to use a dedicated box
- *Security policy may require a dedicated CPU*
- *Serial cards in the server versus using Terminal Servers*




There are many free solutions available, depending on the features that you want. There are at least two commercial applications available to you. (Aurora Technologies, Computer Associates) Our favorite free application is Conserver, available at http://www.conserver.com/

You can often use free software on an existing server, as the needs of the software themselves do not require much memory or CPU.

However, shared machines often mean security vulnerabilities in the other applications, which could allow unauthorized folks to see the logs (or tamper with them). A shared system often means more users that have legitimate access to the machine, which can be another vulnerability.

If security and integrity of the logs is a concern, you should consider purchasing a dedicated machine, installing a hardened OS, and limiting the number of folks who have login access to the CPU.

Adding multi-port serial cards to a machine increases power consumption, heat output, and (depending on the card) can also increase CPU load.

## Adding a logging server

- **Captures forensics information**
  - Why did it crash?
  - Who made changes?
- **Can be linked to other tools**
- **Allows juniors and seniors to work together**
  - One session controls, others watch
  - A backup administrator can watch the screen during critical changes, or during extended service windows.




You can integrate a commercial logging server with your terminal servers.

You can install many logging servers *instead* of terminal servers.

You can find freeware servers, and save some money.

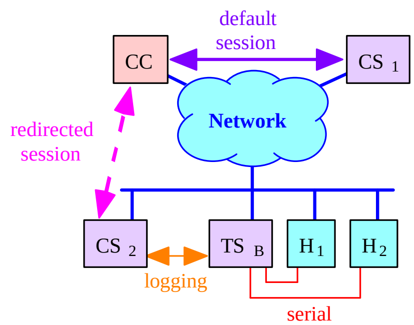
You might be able to program your own in-house…

But ADD SOMETHING! The benefits of these tools are that they will save you time, help keep your systems on-line, and give you better visibility into how your devices are operating. They provide mentoring and training capability in an area where most shops have trouble making the effort to train staff. They give you the ability to distribute the workload across many staffers, regardless of their physical locations.

These tools should be in every shop, to help you do more, much more efficiently, and much more quickly.

## Advanced Architectures (#8)

- **Distributed Console Servers**
  - One master configuration file
  - Client is redirected from ‘local’ server
  - Logging continues if WAN fails!







In the case of Conserver, you can indicate in the configuration file which of a number of distributed conserver hosts is maintaining the logs for any particular device, as well as indicating which remote terminal server is directly connected to the device.

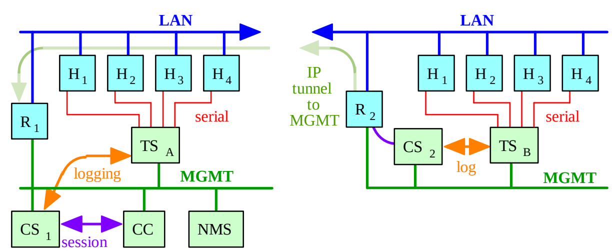
You can then push this master configuration file to all of the distributed conserver hosts.

Each client should try to connect with the conserver host that is closest to the client for all connections. (You can do this via hostnames, or even with a local host file entry.)

If a client (CC) connects to his local conserver host (CS1), but is trying to reach a device that is connected to another conserver host (CS2), the client is redirected to the other conserver host. The client session is then connected with the session of the desired device.

## Advanced Architectures (#9)

- **Distributed CS and Security**
  - Distributed Console Server App and Terminal Servers
  - Logging is on local mgmt net
  - Client sessions traverse the tunnel








We can extend the idea of distributed console server hosts in our earlier security models. In this case, all of the logging traffic is kept on the remote management network, as peer-to-peer traffic, and only the client sessions from other sites is carried over the tunnel. This is, in essence, the architecture used by Synopsys in their field offices

It is possible to have console clients in the remote office, even though it was not shown on the diagram above. With a single configuration file, a client on the remote MGMT network would connect to the console server on the same local network, and it could be redirected to other console server hosts if the client wanted to connect to console devices hosted on other networks.

## Synopsys

- **_Multiple distributed data centers_**
- **_35+ field offices_**
- **_Field sites host a Conserver_**
- **_Router supports_**
  - Dial-in/out ISDN access
  - Local authentication
  - Console ports

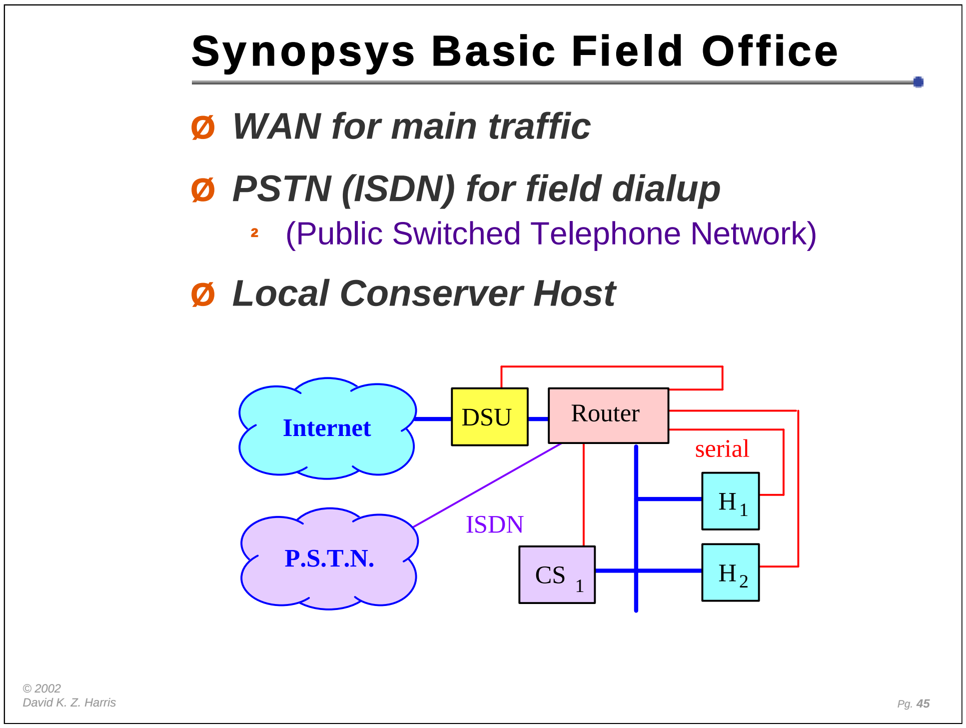



Synopsys has been using Conserver for more than a decade. They had expanded their implementation across the major data centers for the company, and during 2000, they replaced older ANNEX terminal servers for all Cisco 3600-series hardware, to eliminate Serial BREAK problems.

After attending the LISA 2000 tutorial on Conserver, Jeff Komori architected a transition to distributed mode multiple Conserver hosts, and they deployed it across all of their medium and large field offices.

The model for a field office was a Cisco 3640 chassis, with Ethernet, WAN WICs (Serial and ISDN links), MICA modems, and NM-32A serial modules. The High-speed serial WAN link and Ethernet continued to play their traditional WAN/LAN router role. The ISDN and MICA modems provided high-speed modem dial-up access into the field office, reducing the corporate dialup costs. And the async serial card provided console access.

The big win was during a WAN link outage, where a Network Admin could see both sides of the failure, and where console logs turned up configuration needs on field office hosts when the WAN link was down.



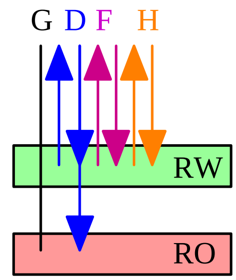

In the field office, the field office router also became the Console Server, and the ‘local dialup connection’ for staff near the field offices.

By adding a local Conserver host in each field office, the system administrators now had a tool to understand what happened to the servers in the field offices when the WAN link failed. This helped uncover system dependencies (such as libraries mounted over the WAN, or DNS dependencies) that would hamper ‘local’ work if the WAN was down. Knowing about a problem is the first step in fixing it.

The dialup access saved significant ISP costs each month. By using an ISDN line into each office, the dialup connections could support speeds greater than 28.8 and 33.6 Kbps. However, this also provided the network administrators a method to ‘be on both sides of a broken WAN’. With the primary link down, they could now perform diagnostics from the field office, as well as from their NOC. This required a local authentication host at the field office, which could be managed from the main office while the WAN was working normally.

## Advanced Architectures (#10)

- **One server for control**
- **Secondary logging server**
  - Dedicated machine
  - No NFS dependencies
  - Only 1-2 admins
  - Physically secured
  - Strictly READ ONLY




- **Ports from devices connected to two jacks!**




Legend: G = signal ground, D = tx and rx data, F = hardware flow control leads, and H = hardware handshaking leads.

Basically, only the signal ground and the data coming from the attached console is delivered to the second port. There is no way to control the attached device from this second port, but you do get a second logging server, to provide a method for you to validate logs on the primary server.

This can be applied in an environment where your logs may be audited, and you need a way to reduce the chances of someone being able to tamper with logs.

One console server is deployed, and is used by console clients. This server can be managed across the network, and probably is a dedicated device, with a minimum number of login accounts.

A second console server is added, which is also dedicated to this task, but is also designed to be a stand-alone server, with no file dependencies to other hosts on the network. You would have a local monitor and keyboard, but this is all in a physically secure location, to prevent access by unauthorized folks.

The console wiring from the attached devices is brought back to the secure location, and connected to TWO sets of jacks (for each attached device). All wires are connected to the RW jack, while only signal ground and receive data are connected to the read-only jack. The RO jacks connect to the second server.

## Installing Terminal Servers

- ***What networks will host them?***
  - DNS addresses and names
  - Do you want them on your mgmt net?
- ***Shelf or Rack Mount?***
  - Where will each one live?
  - Will you need infrastructure cabling?
- ***Power and cooling needs?***
- ***Network connections/addresses?***





Before your terminal servers arrive, you should know where they will physically live (so you will know if you can order a rack-mount version, or if you have to buy shelves). You should have decided what network(s) they will be connected to.

With that information, you can pre-assign IP addresses, and DNS names for the terminal servers.

Before the terminal servers arrive, mark their new locations, so that other administrators don't try to 'squat on your land'. This can mean installing and marking the shelves, or marking the rails where rack-mount gear will be placed. (You should try to reserve your power and network connections as well.) You don't want to go to the data center on install day and find another machine already connected and running…which may delay your installation.

Think about cooling for the new equipment. Do you need to advise someone that new equipment will be installed in the data center? Is there adequate power and cooling capacity in the room?

## Modular Adapters Will Help!

- ***Pre-wired + labeled = trusted***
  - Troubleshooting is faster
  - Easy to spot the wrong part
  - Easy to tell what the right part is
- ***Small cost over parts cost to you***
  - Your time is worth more than that
- ***Get a Passive Signal Tracer!***
  - Invaluable tool for physical layer




Many of the higher-density console servers use an RJ-45 connection, to save space over the DB-n predecessors. However, most of the vendors have different wiring schemes, so you need to know *which* RJ-45 format your adapter is wired for.

If you are moving into a new shop, where the adapters have been built when they were needed, you may find that they are not well labeled, and that the internal wiring probably varies from one adapter to another.

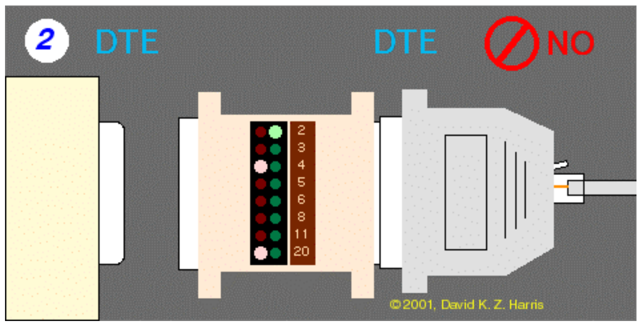
If I don't know the heritage of an adapter, I can't be sure that it's wired for the proper RJ-45 wiring scheme, and that all of the DB-n pins are connected to the correct places. I'll have to spend time to open the adapters to check the wiring (and maybe spend more time to fix them).

For only a little more than the raw parts cost, I can get an adapter that's been wired to my specifications, tested, and labeled. When I see the label, I know what the wiring scheme is, and I can trust that the wiring in the adapter is correct. My time is worth more than the incremental costs.

Get a good passive signal tracer (or more than one). These will also save you time and frustration.

## Signal Tracer Demo

- **_Passive signal tracers don’t need batteries._**
- **_No Break-Out boxes._**







The image above is an ‘animated GIF…so you’ll need to look at the Minor Scroll of Console Knowledge (http://www.conserver.com/consoles/msock.html) to see the image in action. It demonstrates how you test the signals on the host, and then the adapter on the cable. If the signals are identical (both are DTE or both are DCE), then the connection won’t work, so you change the adapter on the cable to be the “other” type, check to confirm that the signals are now opposite, and you are ready to connect the cables, and start checking whether you are ready to send data over the connection.

## Adding Consoles to PCs

- ***Normally, this wouldn't work…***
- ***Some vendors add BIOS support***
  - Compaq, Network Engines
- ***Other vendors add optional cards***
  - Hewlett-Packard
- ***You can add a third-party card***
  - PC-Weasel (EISA and PCI versions)
- ***Rackable Systems' "Phantom"***




Traditionally, the PC architecture has not lent itself to using the COM ports as serial consoles, they way that UNIX machines have.

Even if you are running a UNIX OS on a PC, you have normally needed to wait until the OS is running before the serial console starts passing traffic.

In recent years, some larger vendors have been adding some console capability in the BIOS. Most often, this is basically just redirecting the Power-On Self Test (POST) output to a serial port, and then, only if it thinks your MODEM is on-line!

On some Intel motherboards (SE7500cw2 series boards, some SCB2 as well) have a quirk where "hardware handshake = none" really means "you shouldn't see them", and if you attach a serial cable that asserts hardware signals, the system won't boot. (Disconnect cable, fix setting (or modify cable), and then reconnect cable.)

There have also been attempts to use add-in cards to add another path for managing the basic operations of the servers through a serial console port (instead of a built-in COM port.)

The PC Weasel add-in card is currently available in EISA and PCI, but it appears to the PC as a Hercules monochrome or VGA display card, but it allows you to control the BIOS settings, and redirects all of the monitor output up to the GUI activation, as well as providing some control over remote rebooting. (http://www.realweasel.com/)

## PC BIOS limited access

- **_Usually limited to_**
  - P.O.S.T. output until GUI starts
  - A few BOIS settings (via EISA add-in)
  - Rebooting the server
- **_Some can capture crash dumps_**
  - Compaq lets you replay them!
  - Real-time! ANSI and color!
- **_Some allow multiple accounts_**





Owners of newer Compaq servers have the ability to control basic server functions (power cycling, soft resets, some BIOS support) via a serial console port.

Normally, server owners would connect a modem to each of their server serial ports, with a dedicated modem for each.

Using terminal servers, you reduce the recurring costs of all the phone lines. (Even if you are using analog lines in your phone switch, those lines are not cheap resources.) You can then rely on the strength of your remote access authentication mechanisms to protect access to your server ports, rather than relying on password challenges from the modems.

Modems cannot adequately audit successful (or failed) access attempts, and they don't support remote authentication servers or security token devices.

If you need more security or auditing, your RAS solution can give you more security than modems on console ports.

NOTE: Most PC's communicating via BIOS support require DCD being active before the PC will listen to traffic, even if DSR is active! The developers thought you would only be connecting them to a modem for access...

## Compaq Serial Console

- **_Integrated Remote Console (IRC)_**
  - Must be built into the server hardware
- **_Password in Server NVRAM Access levels allow_**
  - Up to 12 users, definable access rights
  - viewing of statistics and events
  - rebooting the system
- **_http://www.compaq.com_**
  - Search for “integrated remote console”


Pg. 52

Go to the Compaq web site, and get the primer for Integrated Remote Console. (http://www.compaq.com/support/techpubs/user_reference_guides/281862-002.pdf) You can order the document as Compaq part number 281862-002.

The “feature” needs to be built into the server hardware. Check the standard features on your servers, to see if you have it.

This console redirection goes away after the OS goes into graphics mode.

The hardware does not support remote control of Windows NT.

Console (P.O.S.T.) redirection works as long as the display output is ASCII text. Prior to graphics mode, one can boot to DOS or run the EISA configuration utilities.

David Primmer recommends the NT lightsout guide. It's a set of tools and documents that are designed to provide information about setting up, managing, and running Windows NT systems in a headless “lights-out” environment. Go to the Compaq homepage, and search for the keywords “lights out”.

The Proliant and Prosignia lines have an optional Integrated Remote Console, which connects to the ethernet network, and is reachable, even if the server is not functional, using a GUI interface. (http://www.compaq.com/manage/remote-management.html)

## Network Engines

- **_BIOS redirection in ROM > v.96_**
  - Can be installed from Mgmt System
  - Can be upgraded via CD from N.E.
- **_Smart Drive & Ethernet Interfaces_**
  - BIOS hands off to these Smart parts
  - Interfaces report directly to screen
  - (The output from drive controllers and network interfaces do not get redirected to the serial port.)




The Network Engines WebEngine provides for a level of POST redirection, but the BIOS hands off control to the Ethernet controller, and the Hard Drive controllers…and you never see any of the output from these separate controllers, just from the BIOS.

If you have an older unit, contact your Sales Engineer, and ask to get an upgrade CD, or schedule an appointment to have them upgrade the FlashROMs.

This is an early attempt at adding Console redirection at startup. It was added after the product was developed, and as a result, is limited in ability to control some server functions. But the company now understands the needs, and with input from IBM as a partner, should include enhanced capabilities in the newer product models.

## HP Admin Console

- **HP Remote Assistant**
  - Specific to HP Hardware
  - Doesn't catch 'Smart NICs'
- **Allows reset, and power cycle**
  - Graceful reboots require daemons
- **Can page with attached modem**
- **Captures event/status info**
- **Reboot to utility partition**
  - Useful for diagnostics



Pg. 54

Some Netserver CPUs have some remote control capability built in. (HP/UX does have the ability to use a serial port as a console,) You can also add the control capability by installing an HP Remote Assistant management card, with connections to the motherboard for some control functions. You also need the NetServer Navigator CD to configure the system.

The EISA card has an on-board battery, which allows you to power-cycle the CPU as well, if the server is compatible.

The system really wants to be controlled over ethernet, but can be used with a modem, or a direct serial connection.

The emulation is ANSI, Color!

The console can also give you NT Graphics redirection, with appropriate client software on the workstation(s) that you will use to mange the server(s).

## PC Weasel Pointers

- ***PC Weasel***
  - http://www.realweasel.com/
- ***Detail demo ability via Internet.***
  - http://www.realweasel.com/demo.html
- ***Add-in card, with a serial port***
  - Available in EISA & PCI card formats
  - On-board 16550 UART
  - Send/monitor keystrokes
  - Press/release/cycle reset button
  - Cycle power as well




The devices appears to the computer to be a monochrome video adapter. The P.O.S.T. information that is sent to the video adapter interface is then sent to the serial port on the card.

Once the system starts booting the OS, and switches into a graphical mode, the card does two things;

1) Gives you the ability to perform some basic functions, including examining the keyboard buffer, and/or sending keystrokes into the keyboard buffer. You can also push, release, or cycle (push-release) the reset button.

2) If the OS tries to use a serial port as a serial console, the UART on the card will then connect that stream to the serial port on the card. That allows you to use the same connection for your serial console as for basic CPU control.

There have been lots of requests for PCI cards, but clearly not enough (yet).

Canada Connect Corp., Calgary, Alberta

http://www.realweasel.com/

## Rackable Systems

- **Their 1000 Series servers**
  - 2-rack units tall
  - Front-mounted connections
  - Front air-inlet, rear exhaust
- **"Phantom" management system**
  - (PIC Dog!)
  - Available in most 1-, 2-, 3-U servers
  - Display, 8 temperatures, LED signals





You have many options for Intel-based servers. Rackable offers many variations, and features. However, I mention them here because they are Conserver-Friendly!

Cary Roberts (Tellme.com) developed a PIC-controller, with LCD display, for managing the machines in the Tellme data centers. Working with Rackable Systems, the chassis were modified to support the controllers. In return, Rackable is now the exclusive provider of these control boards in their chassis. Rackable refers to the boards as "Phantom".

http://www.rackable.com/advantages.html

http://www.rackable.com/lightsout.html

The board allows soft power on/off/off-pause-on, monitor inlet air temp (up to 8 locations in a chassis), and supports text messaging to the on-board 2-line, 20 character LCD display. You can also control an LED on the chassis (on/off/flashing). The LED and messaging can be used by engineers via the serial console to alert data center technicians when a server needs attention, making it easy to find particular servers, and to pass short messages to the techs. (i.e. "Bad HD, fix me!")

## Remote Power Control

- *Some vendors allow full network access, besides serial access.*
  - Telnet access (some even allow http!)
  - Some UPS vendors allow SNMP control with add-in modules.
- *Restricting access to consoles controls who cycles the power.*
- *Some vendors add serial ports to power controllers.*

© 2002
David K. Z. Harris
Pg. 57

Many UPS vendors allow SNMP management of their larger units. This often includes the ability to shut down output circuits. (However, that's not often practical, since many machines are usually on each circuit.)

American Power Conversion Corp. (http://www.apcc.com/) make a series of remote power control devices that let you cycle power on individual outlets. These units also let you set up a cascaded startup sequence, to avoid power surges when power on the mains return. These devices include a 10-base-t interface, with telnet and http listeners as a standard feature. (http://www.apcc.com/products/masterswitch_plus/index.cfm)

The BayTechDCD folks offer a line of intelligent power controllers in many different configurations. Some of their products even include modems for dial-up access, as well as serial port control. (http://www.baytechdcd.com/)

Server Technologies also has some remote power control devices. Some include a serial switch, so that you can switch your session to one of the attached devices. These also include the feature that you can examine an approximate power consumption for each of the switched outlets via remote control! (http://www.servertech.com/products/Default.htm)

## Wrap-up

- ***Did we cover everything?***
  - Console Server features, sources
  - Evaluation criteria, BREAK info
  - Console Server Application info.
  - Best Practices
- ***Questions and Answers.***
  - BOF session, Wed, 7-9p, Salon K
  - Vendors: Cyclades and Aurora Tech
- ***Please fill in your evaluation forms and drop them off***




Hopefully I've done what I came to do, which is to inform you about Console Server vendors and hardware, to give you some criteria to use for evaluating their features, and give you some practical working knowledge that may help you set up Console Servers at your site. And I hope that I was able to answer some of the questions and concerns that the students had coming into the class.

We will have a BoF session tomorrow night, from 7p-9p, on the 5th floor, in Salon K. Bryan Stansell should be there, as should Dave Stuit. There are a few other interesting BoF sessions, but come to ours if you can!

I haven't convinced Lee Damon that Remote Access to Serial Consoles warrants a "Guru is In" session. If you have a feeling one way or the other, please let me know, or contact Lee, or the conference organizers, and let them know what you think. I'd like to do a session that is partly a workshop, fielding questions from the audience, and trying to solve their console problems. Sort of a cross between the BoF, and a Work In Progress report.

While the LISA staff are interested in getting an evaluation form from all of you, I'm also interested in your responses, since I'll get some feedback from the LISA folks about how well you think I did.

On behalf of the Conserver development team, thanks for attending, and I thank you for turning in your tutorial evaluations.

David K. Z. Harris      BigBand Networks

## Suggested Reading

- *Aurora Technologies*
  - http://www.auroratech.com/
  - /free guide.html
  - A good primer for console services, and an even-handed discussion of "Distributed Servers" versus "Console Servers plus Terminal Servers" topic
  - Email info@auroratech.com, and ask for the Guide to Multiport Connectivity for Solaris and NT.




There are very few comprehensive works, explaining how to set up serial console services, which is why we developed this tutorial. However, Aurora Technologies has provided a good discussion of the topic, called "Guide to Multiport Connectivity for Solaris and NT"

The Aurora folks lean more towards a commercial server application (with support!), and they favor using many servers with multiple-port async cards installed in the servers.

While Conserver can support multi-port cards in the servers, we also feel that Terminal Servers are probably a better solution for large sites, or for sites with needs to connect many distributed ports.

Rather than just taking our word for everything we have described here, we would encourage you to contact Aurora Technologies, and ask for a copy of their guide. Read through it, and get their side of the story as well.

## Web Links

- **Ø *Stokely Consulting***
  - http://www.stokely.com/
  - Good sysadmin and netadmin info
  - Useful K/V/M info as well.
- **Ø *Conserver.Com***
  - http://www.conserver.com/
    Distribution repository and FAQ
  - http://www.conserver.com/consoles/
    Console connection guides
- **Ø *Credits…***





Celeste Stokely has been providing a lot of useful information on her website, and you can find a good deal of information about the problem that Serial BREAK can cause a Sun CPU, as well as a vast array of systems administration topics and tutorial pages. (There are other useful pages as well. Check it out!)

Bryan Stansell has put Conserver.Com on the Internet, to make it easier for folks to find the most recent version of the Conserver code, as well as providing email lists for new version announcements, and for a users support forum.

David K. Z. Harris has been working on the serial console guides for 5+ years, and has recently moved them to the conserver.com. These include Console connection guides, as well as some basic serial tutorial pages.

Dave Stuit has helped with the man pages and FAQ, as well as providing valuable input for these slides.

Bryan, Dave, and David worked for Certainty Solutions (formerly GNAC), and all three continue their support of Conserver while pursuing new efforts.

## Vendor Links

- **_Cisco Systems_**
  - The 2600 and 3600 series.
    - 3660 line numbers are 33-224!
    - IOS 12.05(t), look up UDPTN
    - Async input, multicast output!
  - Use the NM-32A 32-port modules.
  - Americable sells patch panels.
- **_Xyplex, iTouch Communications_**
  - The InReach line is now “Sun-safe”
  - The iTouch Xyplex family is not!
- **_Both RJ-45 ports are symetrical!_**





Terminal Server Vendors

Cisco Systems http://www.cisco.com

http://www.cisco.com/univercd/cc/td/doc/pcat/2600.htm

http://www.cisco.com/warp/public/cc/pd/rt/2600/prodlit/2600_ds.htm

http://www.cisco.com/warp/public/cc/pd/rt/3600/prodlit/seral_ds.htm

http://www.cisco.com/warp/public/cc/pd/rt/3600/prodlit/3600_ov.htm

Xyplex (was nBase, now iTouch Communications, becoming MRV)

http://www.itouchcom.com/products/index.cfm?cat=scs

http://www.itouchcom.com/news/display.cfm?nwid=2002_07_01

Use the Americable Xyplex adapters for the InReach family as well!

Adapter Vendors

Americable 800-328-7954 http://www.americable.com

http://www.conserver.com/consoles/ciscokit.html

(also annexkit, iolankit, and xyplexkit)

## Vendor Links, cont'd.

- ***Cyclades***
  - Built-in Linux core
  - TS2000 is a great device!
  - PC multi-port cards available
  - Most products are Sun-safe
- ***Digi Communications***
  - Many devices available
  - PortServer CM is a good tool
  - Many products are now Sun-safe




Cyclades and Digi are both long-time makers in this arena.

Cyclades was the first (and only) console server hardware we found in our Serial BREAK testing that had a software-controlled BREAK problem. Once the recipe was sent on how to demonstrate the problem, we received a patch within a few days which resolved the issue. The TS2000 hardware was also enhanced during the design phase to ensure that the BREAK problem did not exist in the final product.

http://www.cyclades.com/products/ts_series.php

http://www.cyclades.com.pe/Productos/Anexos/ReleaseSerieTS.txt

Digi has also entered the Console Server hardware arena, with the PortServer CM product line. The CM32 is also a good fit with Conserver. The existing PortServer Terminal Server line is also still available.

http://www.digi.com/solutions/devtermsrv/cm/index.shtml

http://www.digi.com/solutions/devtermsrv/termsrv/index.html

support.digi.com/support/techsupport/hardware/portserver/sun_console.html

## Vendor Links, cont'd.

- **Perle (Perle Systems Ltd.)**
  - CS9000 is Sun-safe
  - Cables, status LEDs on same side
    - Good or bad? You decide…
  - Good integration with MS Windows
    - May be useful in a mixed environment
- **Lantronix**
  - Still a workhorse in the industry

Perle System took on the Chase Research IOLAN line, as well as Specialix products. You can still get support, and buy hardware from Perle if you want these lines. (The IOLAN model 102 and 104 servers are Sun-safe.)

The Perle CS9000 is comparable to the Cyclades TS2000, and the Digi CM32, in that they are all 32 ports, Sun-safe, I rack-unit tall, lightweight. One difference that stands out, to me, is that the transmit and receive data LEDs on the CS9000 are integral to the RJ-45 jack, putting them on the same side of the unit as the cables. (On the Cyclades and Digi units, the LEDs are on the opposite side from the jacks.) Whether this is a benefit or a deficit in your mind will likely depend on how you decide to mount the units.

http://www.perle.com/products/prod_family/console_server/cs9000.html

http://www.perle.com/products/resources/pdfs/CS9000%20Dis%20paper.pdf

http://www.perle.com/products/prod_family/serial_servers/iolan_pl.html

Lantronix has been making serial-to-network interfacing devices for over a decade, and should also be on your list of candidates to investigate.

http://www.lantronix.com/products/cs/index.html

http://www.lantronix.com/learning/tutorials/ds.html

http://www.lantronix.com/learning/wp/conserv_wp.html

## Accessory Vendor Info

- ***Nu-Data non-BREAK adapters***
- ***PC Weasel in-server cards***
- ***ASP Technology***
  - CatWalk interface
  - Power interface for Xyplex, Digi
- ***DataTran passive signal tracers***
  - If you can find them, BUY THEM!
  - Two LEDS are better than one…




Nu-Data is the sole source for a “Non-aborting Serial Console Adapter” (part number 4723), but their website PDF links have been broken for longer than I can remember. The units cost about $100 per port, which is OK if you only have a few devices that you need to protect. If you have 10 or more devices to protect, you should consider getting a Sun-safe console server device instead.

http://www.nudata.com/ v) 800.844.5757 f) 732.905.5708

http://www.nudata.com/workstationproducts1.htm

Real Weasel produces the PC-Weasel cards. This is the sweetest solution I know for MS-OS machines, and their PCI version has been out for about a year now. It gives you soft power control, and gets around the BIOS limitation in systems with Smart NICs and Smart drive controllers. They also have a couple other references on their web site for other hardware solutions, but none is as sweet, in my opinion. Clever Canucks! Try the web demo!

http://www.realweasel.com/ v) 403.705.2025 f) 403.705.2026

http://www.realweasel.com/oph.html

ASP Technology sells a console server application, but they are clever hardware hackers as well. The in-line dongles for the power leads on Xyplex and Digi product make them Sun-safe, but the CatWalk let’s you put a local terminal on sensitive hosts, while leaving them connected for remote access by console server hardware. Very clever indeed.

http://www.asptech.com/ v) 970.686.1211

## Accessory Vendor Info

- ***Weeder Technologies***
  - Serial interfaces for process control
  - Counters, timers, motor control
  - Analog and digital I/O
- ***Black Box Corporation***
- ***Patton Electronics***
  - Maybe they can make signal tracers
  - Can't hurt to call and ask for them.





Weeder Technologies

If you are looking for ways to get information from devices that don't have consoles, check out this site. While there are a few places to find process control interfaces, this is probably the best site. Useful info, compact products, and a good variety should fill many of your unusual needs, and help you put a console on hardware.

http://www.weedtech.com/ v/f) 850.863.5723

Black Box has always been a favorite resource. They OEM and rebrand many products, and provide a wide array of interfacing devices. I've also used their catalogs as teaching materials, because they have useful block diagrams, and informational notation for using many of the products. Consider getting a printed catalog for your bookshelf.

http://www.blackbox.com/ v) **724.746.5500** **f) 724.746.0746**

Patton Electronics is another vendor with a wide array. The problem with that is that it's hard to find a solution on a website if you don't know what the solution is already. Luckily, you can easily request a printed catalog from their web site.

http://www.patton.com/ 301.675.1000

# Remote Power Control

- **American Power Conversion**
  - MasterSwitch line
- **BayTech**
  - RPC product line
- **Server Technologies**
  - Sentry product line




American Power Conversion has been a long-time UPS maker, and a leader in developing SNMP management for UPS gear. Their MasterSwitch product line allows for serial port access to power outlets, as well as telnet and HTTP control.

http://www.apcc.com/

http://www.apcc.com/products/family/index.cfm?id=70

http://www.apcc.com/support/contact/index.cfm

BayTech has been developing power control products for nearly a decade, but they've been working on digital equipment for more than 25 years. Their remote control power strips can be controlled via a serial connection, or some have an integrated modem.

http://www.baytech.net/cgi-private/product/ v) 800.523.2702

http://www.baytech.net/cgi-private/product?catagory=RPC+SERIES

http://www.baytech.net/support/demoinst.shtml

Server Technologies is new to me, but their Sentry line looks very interesting. It's larger than the APC and BayTech units, but it also can switch more power. (Both APC and BayTech have some units witch can switch lots of power. If you need to switch high-current loads, do your homework and check all three!) I like the Power Tower power strip, but other units also switch a console port as well as switching a power connection.

http://www.servertech.com/ v) 775.284.2000

## Americable

- **_Custom cables and adapters_**
  - Serial adapter kits for consoles
    - Annex/Bay/Nortel
    - Cisco/Lantronix
    - IOLAN
    - iTouch/Xyplex
- **_Short power cords_**
- **_Fiber and Ethernet gear/cables_**
- **_Fast turnaround_**




I've used Americable as a vendor for more than 6 years, and I've been very happy with them as a vendor. They've been able to turn some important orders around very quickly. Some of my other vendors haven't passed this test…

Americable has also worked with me to define and stock special serial adapters for Console Server use, as well as making special adapter and cable bundles for the Console Server vendors listed above. These kits have helped many folks get consoles connected to their networks quickly. But what is important to me is that they made the effort to define and build these parts and kits, before there was a demand, based on my requests. As a vendor, they make efforts to provide or acquire whatever we've been looking for. In many cases, buying something through Americable has been cheaper than buying it on my own from the manufacturer.

It's amazing how much short power cords and appropriate-length cables can clean up a rack!

My contact has been Steve Vacik (svacik@americable.com, x-3824), but I like everyone that I've met at Americable.

http://www.americable.com/ v) 800.328.7954 f) 952.944.8021

http://www.conserver.com/consoles/ciscokit.html

I've had good dealings with them, and good response from them, but I have heard of a couple folks having had past problems. Check with your colleagues, and see if you have a reason to be wary, but I've had good luck so far.