ONE-WAY CABLE FOR IDS DEPLOYMENT

Adam Pointon

Sentinel Data Security

Revision history

Revision v0.2	25 November 2004
Revision v0.1	29 April 2002

Table of Contents

1. About this document

This document was originally written by Patrick Gray in 2002, which can be found here: http://www.sentinelsecurity.net/whitepapers/OneWayCable-original.pdf

2. Copyleft and License

3. Why the one-way cable?

When deploying network intrusion detection systems (NIDS), it’s vital to keep these systems invisible to users and abusers of the network(s) they monitor.

By using a one-way cable, it is not physically possible (without firmware modification), to send packets in both directions down the wire, usually out from the NIDS.

Yet it still allows the interface to monitor all packets coming in the other direction.

This is a very effective way to achieve a main goal of network intrusion detection; to be undetected, yet able to directly monitor network traffic.

4. Connection speed

Using the method described later in this document, it is possible for a 100Mbit network card to maintain 100Mbps half-duplex network connectivity, with no errors.

5. Connection options

We commonly use 100Mbps hubs with one-way cable setups, as it also allows us to not only sniff at 100Mbps half duplex, but also have a one-way cable back into the sniffing hub.

This allows packet flow in the other direction, which we use for active-response techniques including TCP resets and ICMP responses.

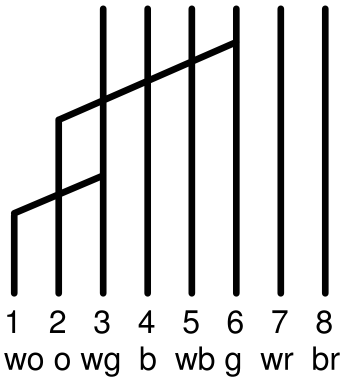
6. Different approaches

There are a few papers online that detail how to make a one way cable by introducing a high pass filter (capacitor) in-line with the transmit pair.

That method is supposed to introduce CRC errors to the transmit pair, however this produced some very weird results for us when we tested it at 100Mbps.

7. Proven method

Seen below, this wiring diagram is what we use to create the one-way ethernet cable.



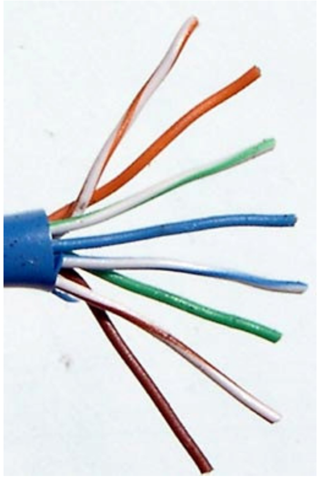
If the above cable modification is made flawlessly, then there should be no transmission problems, or packet loss. However if the wiring modification is imperfect, then there will be problems, mainly poor electromagnetic performance, which results in packet loss.

8. Step by step guide

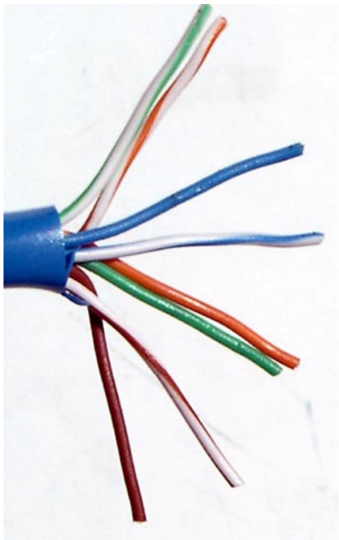
8.1 Measure out the length of cable you wish to use and cut, freeing it from the reel (this is important as you need to remove a twisted pair from the entire length of the cable).

8.2 Strip one end as you would normally, to attach a RJ45 head.

8.3 Untwist and separate the wires into a correct[1] order (shown below).

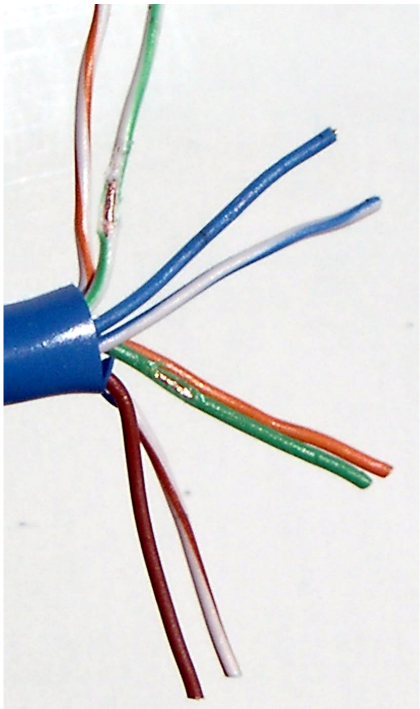


8.4 Group wires 1 and 3, 2 and 6, as per wiring diagram in section 7.

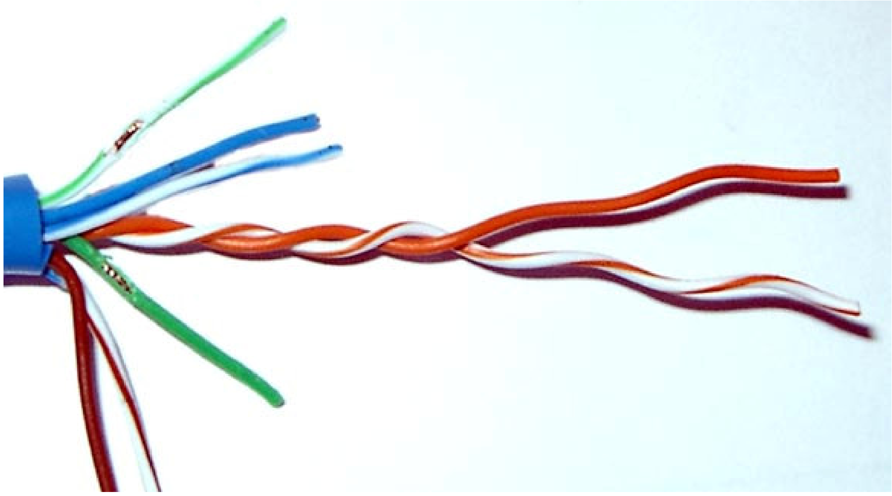


[1] Standard EIA/TIA T568B - http://www.faqs.org/faqs/LANs/cabling-faq/index.html

8.5 Using a sharp knife, cut the plastic covering off the wires you need to join too, being careful not to damage the wires at all.



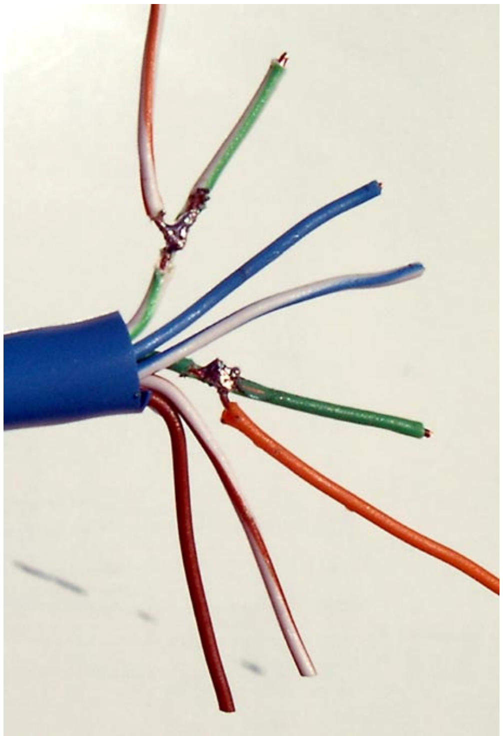
8.6 Now completely remove the orange and white/orange twisted pair from the entire length of the cable. This helps reduce unwanted transmission line effects which could introduce errors.



8.7 Cut a short length (5 cm / 2.5 inches) of the freshly removed orange and white/orange wire pair and untwist.

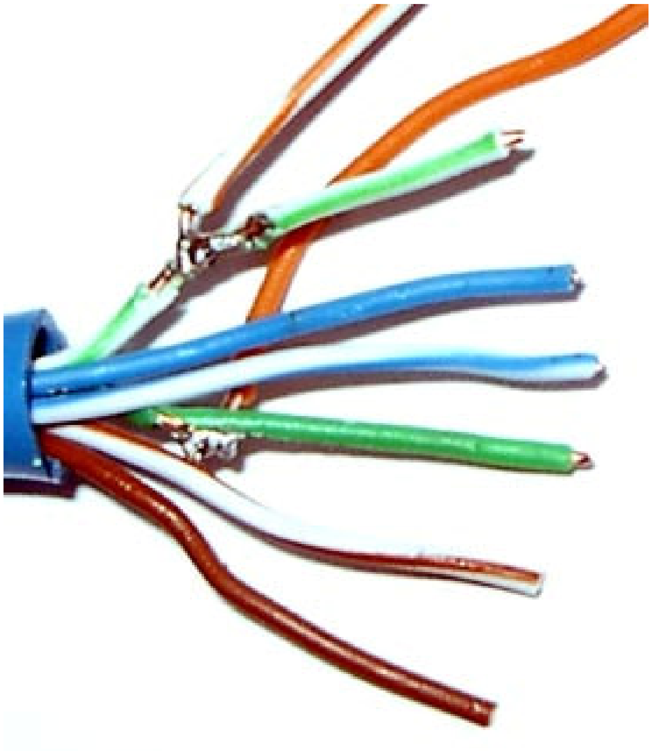
8.8 Solder the removed wires, as per wiring diagram
(As seen in section 7).

Wire 1 to wire 3 and wire 2 to wire 6.

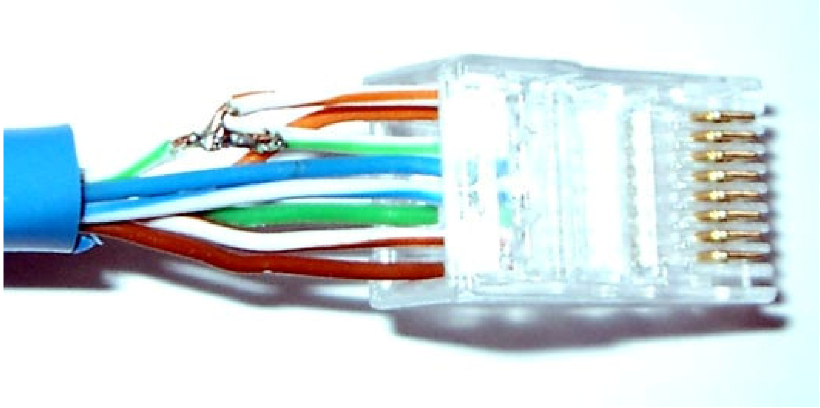


8.9 Prepare the wires to slide into a RJ45 head, being careful to keep the solder/bare wire apart.

At this point, you could/should insulate the bare wire/solder section with electrical tape. (This has been skipped so it is easier to see exactly what's happening).

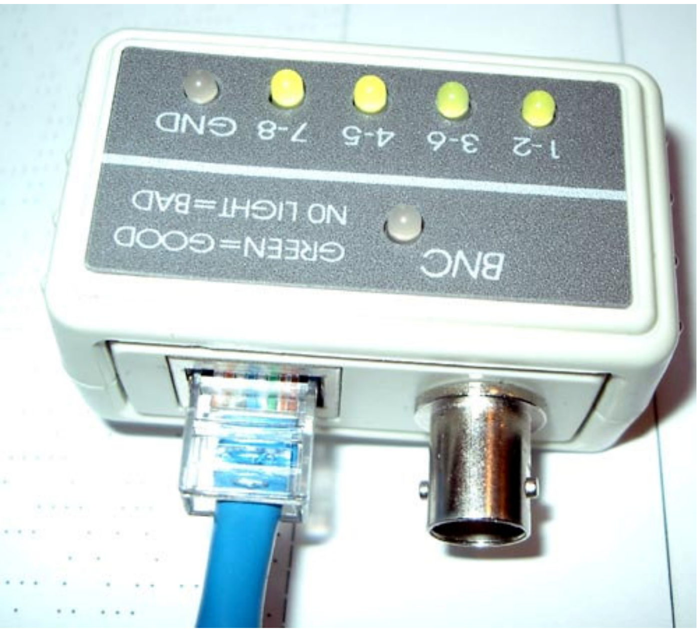


8.10 Ensuring you have the correct wire order (See 8.3), slide the wires carefully into the RJ45 head.

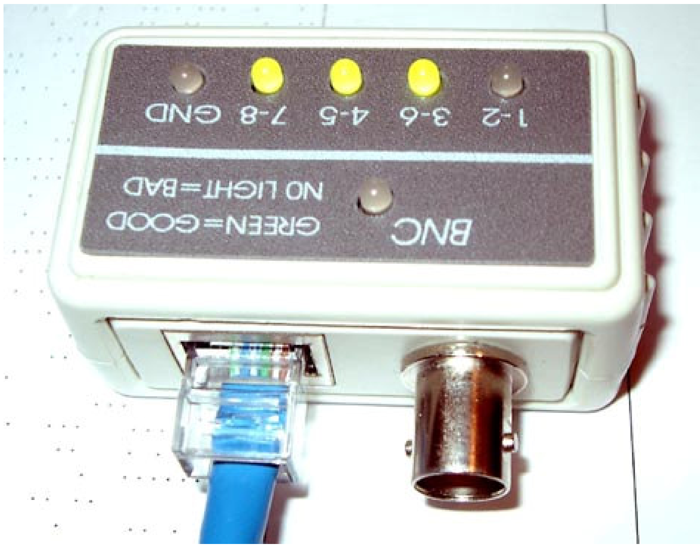


8.10 Crimp and cable-test.

Modified / Soldered end (shows up all 8 wires)



Other end (shows up only the 6 wired wires)



8.11 Label the ends

The modified head, with all 8 wires, should go into the SNIFFING device, be it a 100mbit hub, a mirror/span port or a proper network tap.

The un-modified head, with only 6 wires, should go into the SNIFFER device, the NIDS system.

Incorrect cabling will lead to link failure, nothing more, so use what the LED's are there for.

9. Conclusion

You should now have a 100% effective and very cheap 100mbit half duplex network tap.

appendix a: about Sentinel Data Security

Established in 1998, Sentinel Data Security is an information security consultancy. It has grown into a leading supplier of value for money threat management services by helping organisations develop, implement, and maintain best practice business security strategies for their information assets.

Sentinel Data Security provide affordable & independent specialist consulting services, and ongoing management & monitoring to ensure your network data

with defined deliverables to suit your organisations needs.
Its people consult to a diverse range of entities; from small businesses to blue chips, and government departments & agencies. These engineers and consultants have broad experience gained over years in the security arena, and backed up by official certification from security industry bodies. It is this experience that makes these consulting services relevant, and therefore invaluable to Sentinel clients.
Quality management and standards are implemented through Sentinel Data Security's 'Security Management Framework'. This policy and procedures document has been developed specifically for Sentinel Data Security and has been closely aligned to AS/NZS 7799.2:2000 standards.
Sentinel's dedicated and talented experts, quality infrastructure and management services ensure your security needs will always be in good hands.
Sentinel can help your organisation in the following areas:

consulting services

- **information security governance**
- **strategy development**
- **roles, responsibilities and reports identification**
- **policies, procedures and guidelines development**
- **national privacy policy due diligence auditing**

- **risk management**
- **process development**
- **risk identification and analysis**
- **risk mitigation strategy development**

- **information security programme management**
- **security governance framework implementation**

- **information security management**
- **compliance assessment**
- **metrics development**
- **balanced scorecard development**
- **framework development**
- **wireless system policy, auditing, planning and design**

- **response management**
- **root cause analysis**
- **mitigation strategy development**
- **backup strategy development**
- **business continuity planning**
- **disaster recovery planning**
- **forensics**
  - anton pillar search orders
  - network / system forensics
- **vulnerability assessment**
  - penetration testing
  - social engineering
  - application source code audits
  - network / application design audits

solutions

- **design & implementation of ids, firewalls, vpn's**
- **perimeter security**
  - firewalls
  - VPN's
  - load balancing
  - traffic shaping
  - honey nets
- **intrusion detection**
  - network intrusion detection systems
  - host intrusion detection systems

- **design & implementation of authentication & encryption**
- **authentication solutions**
- **encryption solutions**
  - PGP
  - PKI

- **design & implementation of content security**
- **content access control**
- **post delivery policy control for email & documents**
- **content filtering & logging**
- **virus control**

- **tools**
- **self auditing software**

24 x 7 Managed Services

- **intrusion detection system monitoring**
- **intrusion detection system management**
- **firewall monitoring**
- **firewall management**
- **sms & paging alerts**
- **authentication token management**
- **document and email security management**

For more information about Sentinel, please visit: http://sentinelsecurity.net