WISCONSIN

UNIVERSITY OF WISCONSIN–MADISON

Wired Network Port Security at SSEC

Scott Nolin
UW SSEC
June 28, 2012

Introductions

About the UW Space Science and Engineering Center

WISCONSIN
UNIVERSITY OF WISCONSIN-MADISON

About the UW Space Science and Engineering Center

- Research Center focused on geophysical research and technology to enhance our understanding of the atmosphere of Earth, the other planets in our Solar System, and the cosmos.
- Over 100 ongoing projects at any one time.
- Federal agencies provide most of SSEC's financial support through the competitive proposal process, with modest amounts from other universities and governments,. SSEC also has strong ties with private sector aerospace companies developing remote sensing technologies.

Previous Port Security Work at SSEC

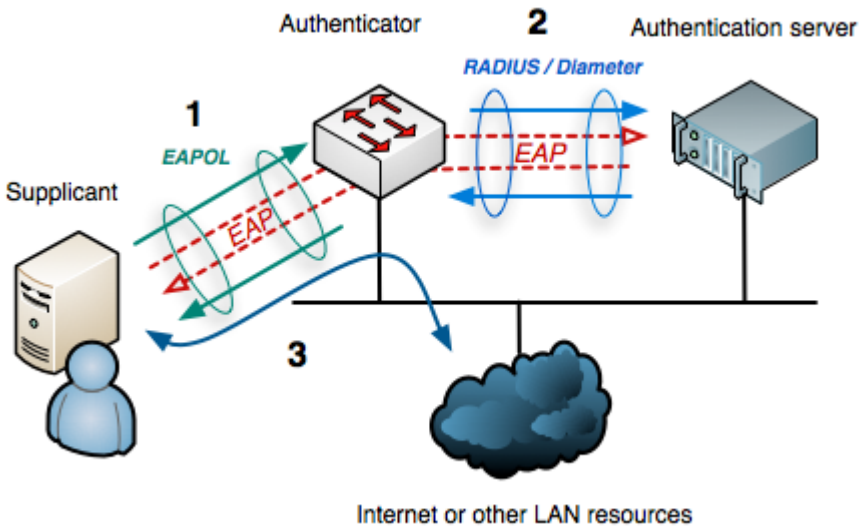
Over the years I'd been searching for a way to do dynamic VLAN assignment to help control "surprise" devices on the network.

- In the past Cisco provided VLAN Management Policy Server (VMPS) for dynamic VLAN assignment. I did that as a proof-of-concept for our systems and considered rolling it out, but did not for these reasons.
  1. It depended on a proprietary solution (Cisco-only).
  2. I had to use a reverse-engineered vmps server, openvmps, which made me a little nervous.
  3. While this worked on thousands of ports just fine according to reports, the cost of failure was high.
  4. I read about an emerging standard to do this task, and more, 802.1x . . .

What is 802.1x?

- IEEE standard for port-based network access control.
- For wired or wireless.
  - Wireless use very common.
  - We will focus on wired ports.
- It keeps the port disconnected until authentication is complete
  - Only EAP packets flow
- Authentication is provided by a server
  - Most Commonly RADIUS
  - Can use AD password, certificates, etc

What is 802.1x?



Picture from WikiMedia Commons

802.1x *with* VLAN Assignment

- Not part of the standard, but most vendors have implemented it. So it's "802.1x with VLAN assignment".
- Access ports only (no trunks)
- Assigns VLAN based on Authentication Database settings

802.1x *with* MAB

- MAC Authentication Bypass (MAB) is also not part of 802.1x
- It's purpose is to provide access for machines without 802.1x clients, for example printers.
- Authenticates based on MAC address from Auth Server.
  - . . . which are trivially spoofed.
  - Makes a simple path for transition to more security
- We configure switches to first try 802.1x, then fall back to MAB. This allows for a transition to 802.1x authentication methods.

Why Bother?

- Clearly a path to better security.
  - Secures the physical port
  - Industry standard
  - Security zones follow the computer or person, not the port you (think or hope) they plug into
  - Enables NAC/NAP possibilities
- Eases administrative burden for supporting network.
  - VLANS dynamically assigned.
  - Allows simple tracking of machines (do you know who's on your network, and **where**?)
- BYOD, guests access, etc.
- Makes IPv6 Stateless Autoconfiguration a reasonable option for any port.

802.1x with VLAN Assigment and MAB at SSEC

1. Switch recognizes link
2. Waits for 802.1x authentication
3. No 802.1x attempt from client
    1. Falls back to MAB
        1. If machine's mac address is in database, grants access to specific VLAN
        2. If not, goes to Visitor VLAN
4. If there is an 802.1x attempt from client
    1. On success – assign to vlan, grant
    2. On failure – assign to visitor VLAN (could be something else..)

NOTE – Our current setup at SSEC only uses MAB. So technically we could make it only attempt MAB, but we assume we will transition to also using other authentication methods. For example AD auth, or certificates.

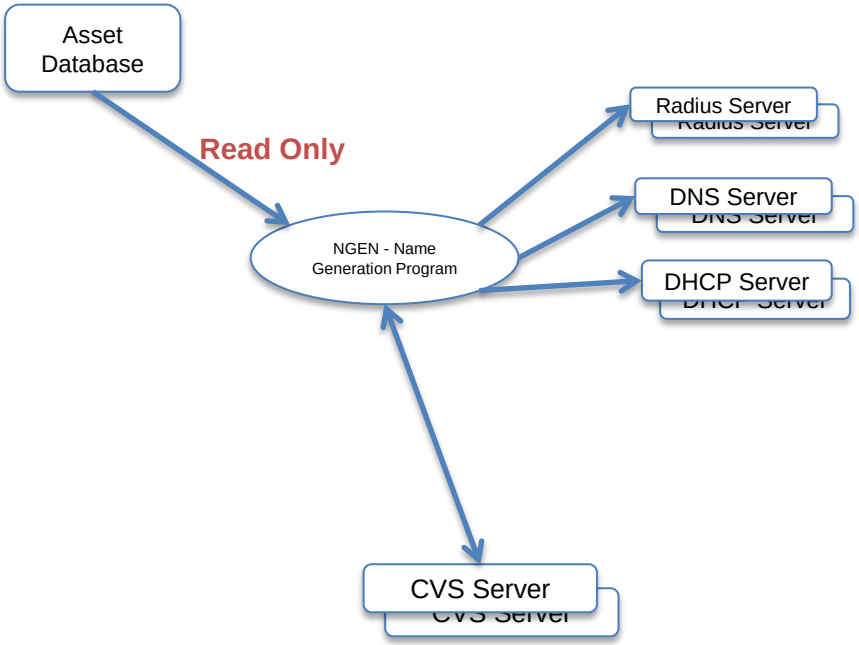
The SSEC User Experience

1. Plug your random laptop unknown to anyone at the center into an open port.
   - Open a browser and you see a splash screen (in our case welcoming to the visitor network and asking for a login).
   - If Needed: Talk to Technical Computing and get appropriate access.
2. Move an existing network machine
   - *I know, your users don't do this without asking, right?*
   - Ok, nothing to see here.
     - It just works and they're on the right VLAN.

The SSEC Sysadmin Experience

- Edit the machine database, assign the machine to a vlan.
  - MAC address is the only other required field strictly for this to work.
  - Obviously, a convenient place to do other stuff, such as DNS addresses, which we do.
- Run program to enable machine on network.

Data Flow



IPv6 Stateless Autoconfiguration

- In the past DHCP has been used as a sort of cheap port access control mechanism for IPv4.
  - You can just guess an IP (it's no secret what our netblocks are!), so it only protects you from the innocent. Still, it's convenient.
- IPv6 provides for stateless autconfiguration
  - Any device in the world automatically gets access
- 802.1x can provide sane access control, so you can turn those Router Advertisements on.

IPv6 Stateless Autoconfiguration

- Using MAB as a transition technology to 802.1x means we must have MAC addresses in a database. So…
- It's relatively simple to build the stateless autoconf supplied IPv6 address if you want "static" addresses.
  - You must turn off client's privacy extensions for this to work completely for managing your machines if that's desired.

Possibilities

- Use 802.1x without MAB, or use both
  - Authenticate with certificates, login to AD, or some combination
  - Newer Cisco authentication features are very flexible, allowing priority, order, etc.
  - Helps enable Network Access Protection schemes.
    - For example, now laptops roam in the wild, and then go right onto our normal network. Automated security audits, antivirus, and so on for each new connection would be ideal. The laptop doesn't go into the secured zone until it passes requirements / is automatically patched etc.

Possible Conflicts

- Radius servers (AAA) defined globally for a switch stack(?).
  - How do departments who share equipment use this? Global radius database only they can edit? Slick radius realm stuff I don't understand?
- Eduroam - uses 802.1x with realms.
  - Can an Eduroam enabled switch provide other arbitrary services like MAB or departmentally controlled certificates?

Found on the Web: Freenac

- Provides a lot of what you see here.
  - “We have taken OpenVMPS, added a MySQL back end, a nice GUI, some advanced PHP control scripts, scalability, redundancy, alerting and some more features.”
- But supports 802.1x too. Unsure if VMPS is an option or used alongside 802.1x as an integral component after reading their docs.
- Last release 2007.
- The MySQL back end might be interesting if you want to build an asset database.

Appendix: Example Interface Config

```
! Note these are tweaked to fail 802.1x quickly and use MAB
! Using the newer 'flexauth' features for order and priority might be better for your needs
! Customize to suit the environment
interface GigabitEthernet1/0/2
 description 802.1x
 switchport access vlan 111
 switchport mode access
 ip access-group block_dhcp in
 authentication event fail retry 0 action authorize vlan 222
 authentication event no-response action authorize vlan 222
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate 120
 authentication violation protect
 ipv6 traffic-filter block_rogue in
 mab
! with older versions this is 'dot1x mac-auth-bypass', commands have changed very recently
 dot1x pae authenticator
 dot1x timeout quiet-period 1
 dot1x timeout tx-period 1
 dot1x timeout supp-timeout 1
 dot1x max-req 1
 spanning-tree portfast
!
```

Discussion