Unified user management with Radius

Or how to not suck at access management

Presenter information

- Tomas Kirnak

  System Architect

  MikroTik Certified Trainer

  MikroTik Certified Consultant

unimus

Network backup and management solution

Come visit us at our stand!

www.unimus.net

A show of hands 1

www.unimus.net

Why are we talking about any of this?

- Do you have a single password for your networking devices you share with other admins in your organization?
- Do you have a few common password that you use for you networking devices you share with other admins in your organization?
- Do you have a per-device unique password and then share that using a spreadsheet or password manager?
- The answer to all of these should be **NO**.

Problem 1

- “Do you have a single password for your networking devices you share with other admins in your organization?”

- This is the worst case scenario.
- YOU SHOULD NEVER DO THIS.

- This exposes you to massive risk, and puts your whole network under a huge attack vector.

Problem 1

- Phishing attacks, keyloggers, viruses…
- Telling the password over the phone, or transmitting it over an un-secure medium (email, IM, etc.)

- Selling any of your old office PCs or laptops on eBay
- Putting any of your PCs/laptops to a repair shop

- Any of these can expose your password, and that opens access to the ENTIRE management of your network

Problem 2

- “Do you have a few common password that you use for you networking devices you share with other admins in your organization?”

- Or otherwise known as “Have you ever had to try 4 passwords to successfully login to your device”?
- Almost as bad as 1, but with the addition of never knowing which password is correct for which device, and you now need to remember and share with your colleges multiple passwords.

Problem 3

- “Do you have a per-device unique password and then share that using a spreadsheet or password manager?”

- Better, but still not optimal.
- You still need to share passwords.
- Password distribution, tracking of password change, and such things now become an issue.

The biggest problem

- When you have a single account that multiple people use to access your devices (no matter if its per-device unique), you lose the ability to know who made a change to a device.
- Configuration change auditing is not possible, since you don’t know how made the configuration change.
- In big networks, when you don’t have this, you are not in a good place.

A show of hands 2

www.unimus.net

Why are we talking about any of this 2?

- When you need to change a password on ALL of your devices, will it take only a few easy steps?
- Do you have unique accounts for each of your admins?
- When you need to change a password because it has been compromised (or password expire policy dictates it), will it only take a few easy steps?
- When a new admin is hired, can you create a new unique user account for him that works consistently across the whole network in a few easy steps?

What we want to achieve

- The answer to all the previous questions should have been **YES**.

- If you can do all the things on the previous page, it allows you to:
  - Quickly react to credential breaches/leaks
  - Have per-admin unique credentials for device access accounting
  - Quickly change a password for a single account across your whole network
  - Quickly create new network-wide unique accounts for new employees
  - Quickly remove no-longer necessary access to the network

Per-admin unique credentials

- Per-admin unique account are very important
- Access accounting is very important
- Being able to see which admin made a configuration change is very important
- Auditing, change reviews, etc.

What should you be aiming for?

- Per-admin accounts
- A single authentication point (redundant) that all the devices in your network use to authenticate logins
- A single interface where to create/change/delete accounts
- All access to the devices should be accountable (have access accounting)

What should you be aiming for – next level

- Password policies (complexity + expiry)
- Unified but flexible access policy (authentication != authorization)
- Long and complex passwords stored in a password manager

  ‘rgn908|Dgn0834nDng0348nOAEIfgn038nodnf(OE*TN#(TN’ is good

AAA to the rescue

www.unimus.net

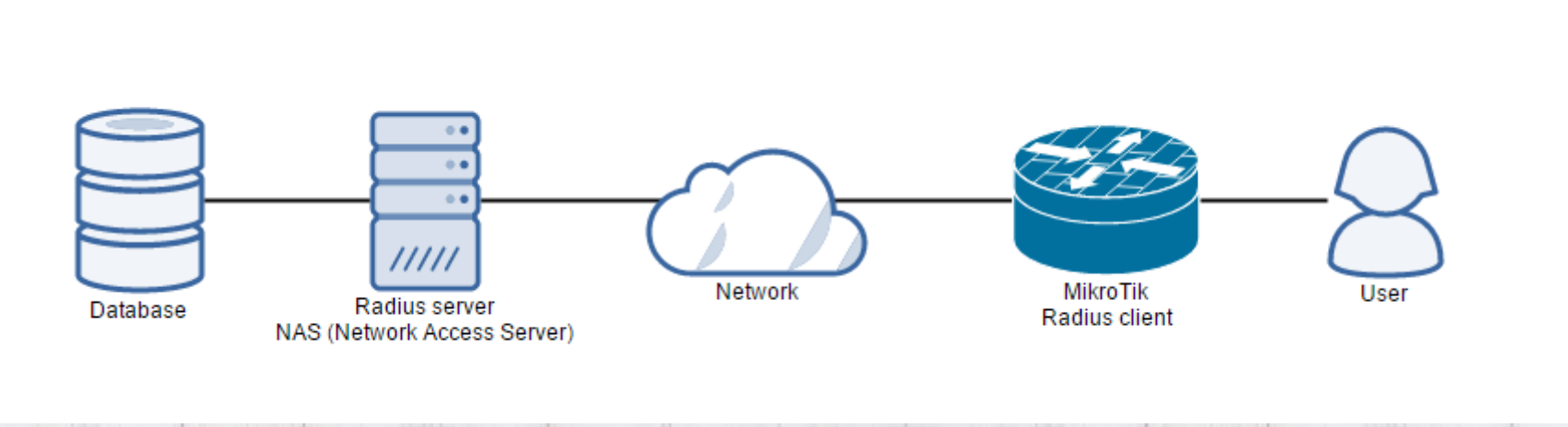
What is AAA

- Proper AAA implementation will do all of this for you

- Authentication
- Authorization
- Accounting

- The most used AAA standard today is RADIUS
  - There is also TACACS+, but lets be honest, nobody uses, or wants to use that…

How does Radius work?

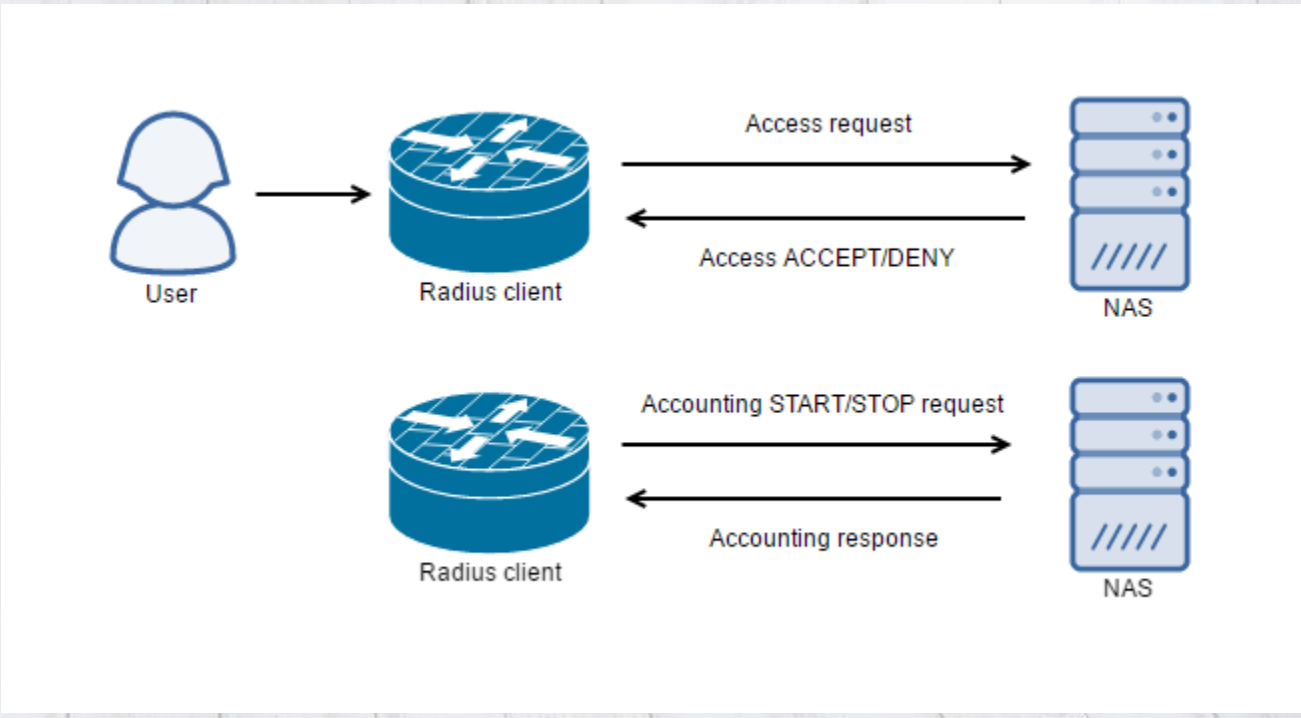


- Radius is not THAT hard (but it chooses its friends)

- You just tell all your MikroTiks to AAA user logins from the Radius server, not from its local user database

What happens at user login/logout?

- MikroTik auth's all logins against the Radius NAS.
  Response can be ACCEPT or DENY.
- Logins and logouts are accounted against the Radius NAS.
  There can also be periodic accounting updates.



This is a simplified diagram

A little complication

- As a part of ACCESS ACCEPT packets, “attributes” are send to the Radius client

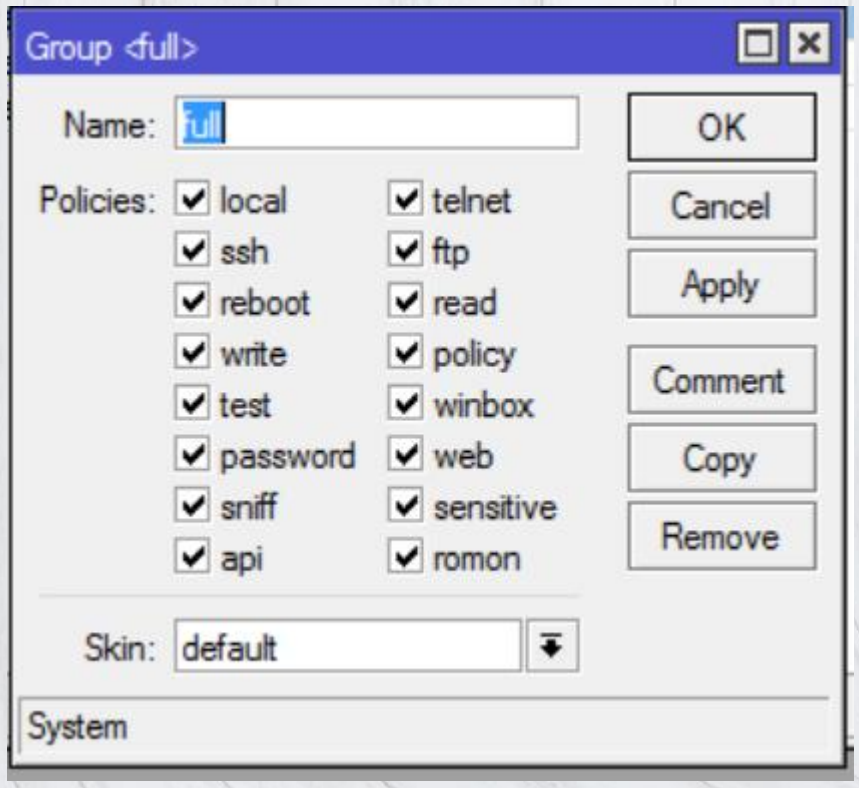
- These attributes can be many different things
- Some are even vendor-specific

Radius attributes

- Example for PPP:
  - IP address to assign to client
  - Queue to assign to client
- Example for us – for login
  - What MikroTik user group to assign to client

How do access policies work in RouterOS?

- Access policies in RouterOS are based on user group membership.
- A group grants a user various priviledges.



Setting user's authorization

- We can specify a group for a user in Radius's access accept reply.
- This allows us to centrally manage user's authorization.

What should we do?

- By pointing our MikroTiks to AAA against a central set of Radius servers, we achieve all the good things we described earlier.
- We will create a unique account for each of our admins in our Radius DB.
- We will have a per-router unique “last resort” local management account, that should never be used, unless communication to Radius (Radii?) servers is down. (we will keep this in a password manager)

How to configure our MikroTiks

/user group
add name=restricted

/user aaa
set default-group=restricted use-radius=yes

/radius
add address=$rad1 service=login timeout=2s src-address=$ipAddress secret=$radSecret
add address=$rad2 service=login timeout=2s src-address=$ipAddress secret=$radSecret

Whats happening there?

- First we create a restricted group.
- Then we enable AAA for router user login, and specify the restricted group as the default group.
- This is a security measure – if a group is not properly received from Radius, user doesn't have access (default authorization policy - NONE).

Whats happening there 2…

- Then we just tell our router to use our Radius (Radii) servers for AAA.
  (we use 2 for redundancy)

How to configure a Radius server

www.unimus.net

Radius servers

- Free, OpenSource, for Linux
  FreeRadius

- For Windows (AD integration)
  Microsoft NPS Radius

FreeRadius

- There are 2 major version of FreeRadius
  - FreeRadius 2
  - FreeRadius 3
- When deploying Radius, be careful which version you deploy
  - They are configured differently

FreeRadius guide

- There used to be a guide here on how to setup FreeRadius here
- It was 20 slides, and about 15 minutes to explain
- It was cut out of here for time-constraint reasons

Microsoft NPS guide

- There used to be a guide here on how to setup NPS here
- It was 15 slides, included AD DC-related config, and took another 10 minutes to explain
- It was cut out of here for time-constraint reasons

So how should I configure the server?

- Luckily, there is quite a lot of materials around the web on both
- Just be careful if you look at guides for
  - FreeRadius 2
  - FreeRadius 3
- Windows Server version for NPS

Additional resources

Things to watch/listen to

www.unimus.net

My other presentations and talks

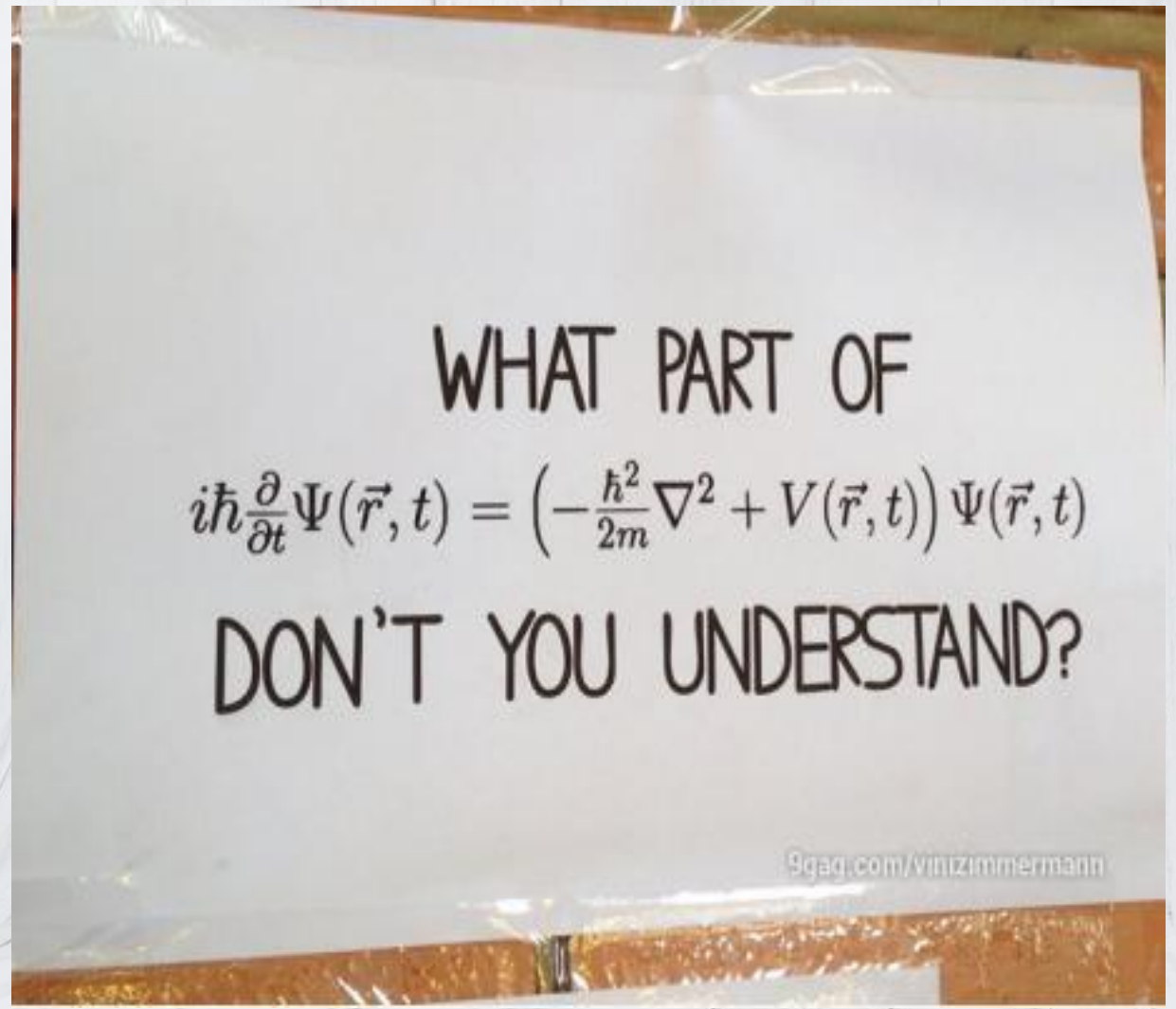
- Find all my other MUM presentations and more on YouTube:
  https://www.youtube.com/c/TomasKirnak/videos

  Load Balancing / Mangle deep dive
  L2TP / IPSec deep dive
  MLPS / VPLS / MTU deep dive
  Monitoring / SNMP deep dive

TheBrothersWISP

- I am a part of The Brothers WISP
- We do a bi-weekly networking podcast
  http://thebrotherswisp.com/
- Give us a listen if you feel like it!

Thank you very much for your attention!



Tomas Kirnak

tomas@unimus.net