Rede Mundial para Acesso Wi-Fi Rápido e Seguro

Ettore Enrico Delfino Ligorio – USP/STI/Internuvem – eduroam AT usp / br

Março - 2016

Agenda

- Definição de Papéis
- Solução de autenticação federada
- Padrões do **eduroam**
- Procedimento para ofertar **eduroam** na Unidade
- Segurança e tratamento de incidentes
- Roteiro de Identificação de problemas

Internuvem

- Provemos serviço de autenticação para redes sem fio.
  - Desafios:
    - Gestão de usuários e privilégios
    - Segurança: Autenticidade, sigilo e integridade.
    - Dificuldade de autenticação a partir de bases isoladas

Gestão de usuários e privilégios

- Uso Senha Única
- Acesso Federado
  - Roaming de usuários de outros entes da federação

Brasil

Mundo inteiro

Segurança

- WPA2 Enterprise
  - 802.1X
  - 802.11i
    - Fase 1: TTLS/Peap (Canal criptográfico)
    - Fase 2: MSchapV2

Dificuldade de autenticação a partir de bases isoladas

cafe comunidade acadêmica federada

- 84 instituições no Brasil
  - Universidades
    - (maioria das federais e estaduais)
  - Institutos Federais
  - Órgãos Governamentais
  - Hospitais

- FaaS – Federation as a Service
  - Interconexão de 61 federações (países)
    - Inclusive a CAFe
  - Oferta de serviços para federados
    - Inclusive **eduroam**

Login no eduroam

- Identificação única na edugain.

“Número USP” @ “usp.br”

Identificação única dentro da instituição

Domínio DNS da instituição. (Identificação única da instituição nas federações)

Quem tem a senha única?

- Todos que tem número USP e já acessaram o portal https://uspdigital.usp.br para criá-la.
  - Podem acessar o eduroam
- Necessário email cadastrado para o número USP

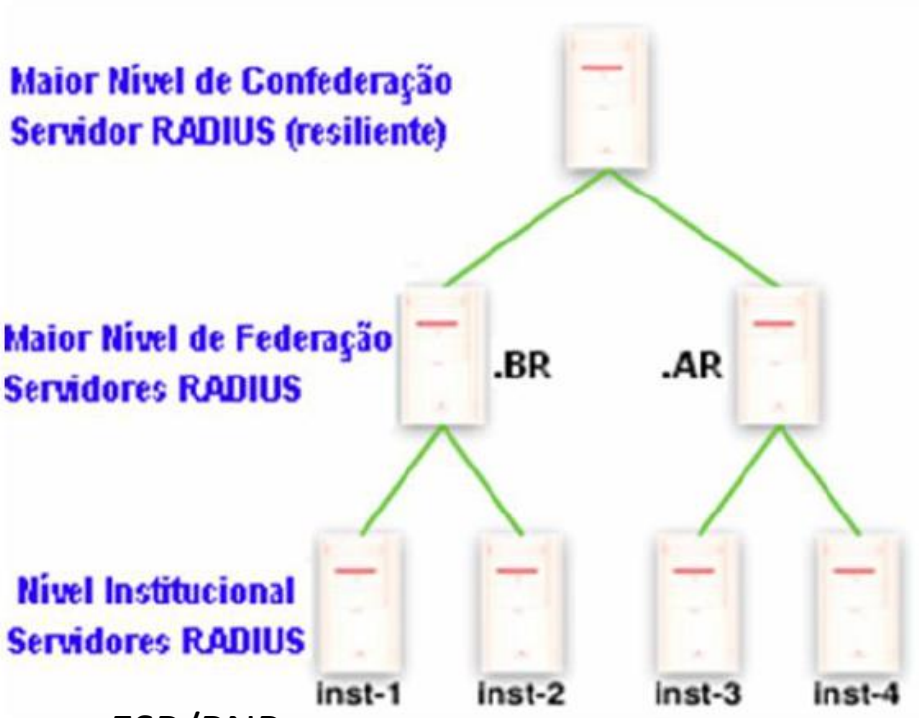
Nomenclatura

- IDP: Provedor de Identidade
  - Responsável pela base de usuários e RADIUS
- SP: Provedor do Serviço
  - Responsável pelos APs que ofertam eduroam

Estrutura Administrativa

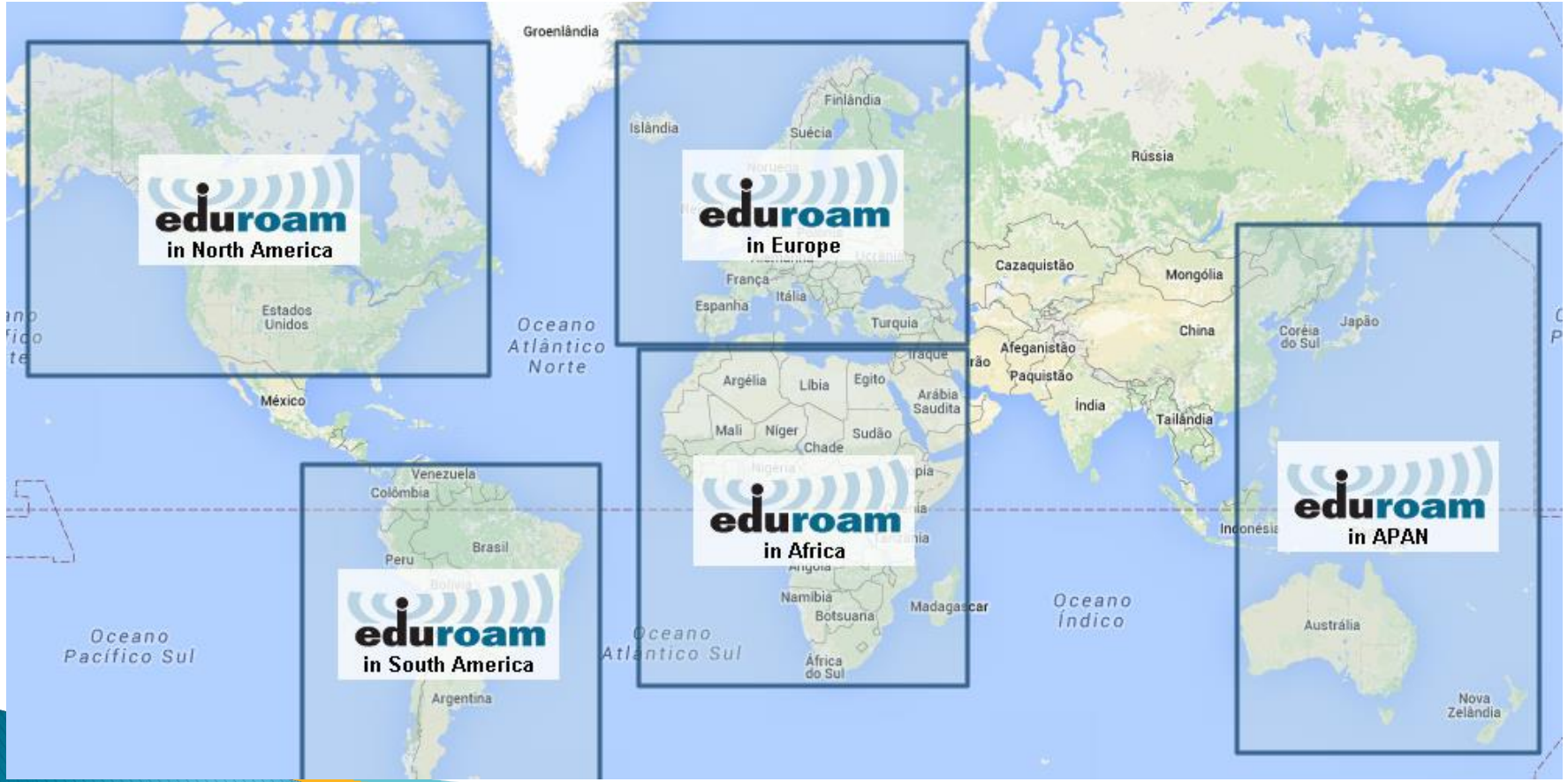
- Operador de Roaming (RO)
- RO Nacional (NRO)
- Confederação de Roaming (RC)
- Instituição Local (SP)

- **Eduroam utiliza uma estrutura hierárquica de servidores RADIUS em 3 níveis**
  - confederação
  - federação (país)
  - instituição
- **Identificação baseada em domínio**



Fonte: Curso eduroam – ESR/RNP

Regiões


eduroam
in North America
eduroam
in Europe
eduroam
in Africa
eduroam
in APAN
eduroam
in South America
Groenlândia
Islândia
Finlândia
Suécia
Rússia
Estados Unidos
França
Espanha
Itália
Turquia
Cazaquistão
Mongólia
China
Coréia do Sul
Japão
Afeganistão
Paquistão
Índia
Tailândia
Indonésia
México
Argélia
Líbia
Egito
Arábia Saudita
Mali
Níger
Chade
Sudão
Venezuela
Colômbia
Brasil
Peru
Bolívia
Argentina
Namíbia
Botsuana
África do Sul
Madagascar
Austrália
Nova Zelândia
Oceano Atlântico Norte
Oceano Pacífico Sul
Oceano Atlântico Sul
Oceano Índico

Países

Metas – eduroam (RFC 7593)

- Identificação única dos usuários em todas as pontas da rede
- Acesso confiável de convidados
- Escalável
- Facilidade de usar e instalar
- Segurança
- Proteção de Pricacidade
- Baseada em padrões

Fundamentos

- IEEE 802.1X: framework de autenticação para liberação de portas L2
- EAP [RFC3748]: Confidencialidade e integridade no transporte de credenciais
- Hierarquia de proxies RADIUS [RFC2865] com TCP/TLS
  - Parecida com DNS

Radius

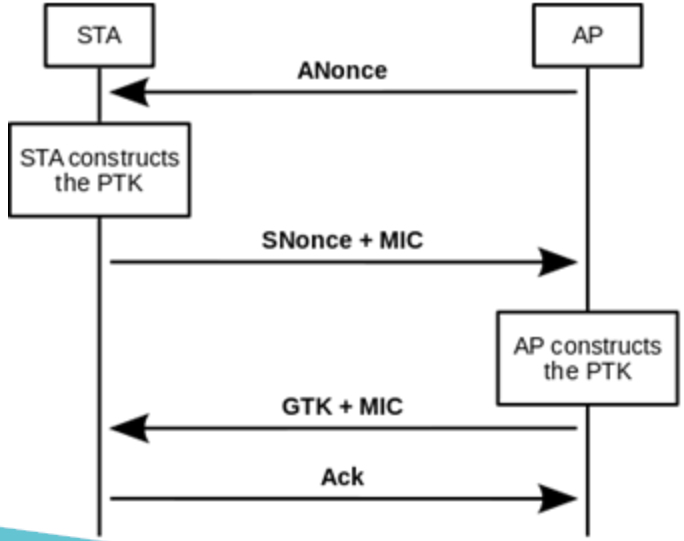
- RADIUS (Remote Authentication Dial In UserService)
  - RFC 2865
  - Autenticação, Autorização e Auditoria (AAA)

eduroam - Arquitetura Clássica

- Relações de Confiança

Autenticação

- **IEEE 802.11i-2004 (**WPA2-Enterprise): substitui o WEP e define o uso de 802.1X e EAP em redes sem fio.



EAP

- Escolha do método
  - Livre entre usuário e instituição de origem
- Integridade
- Confidencialidade

802.1X

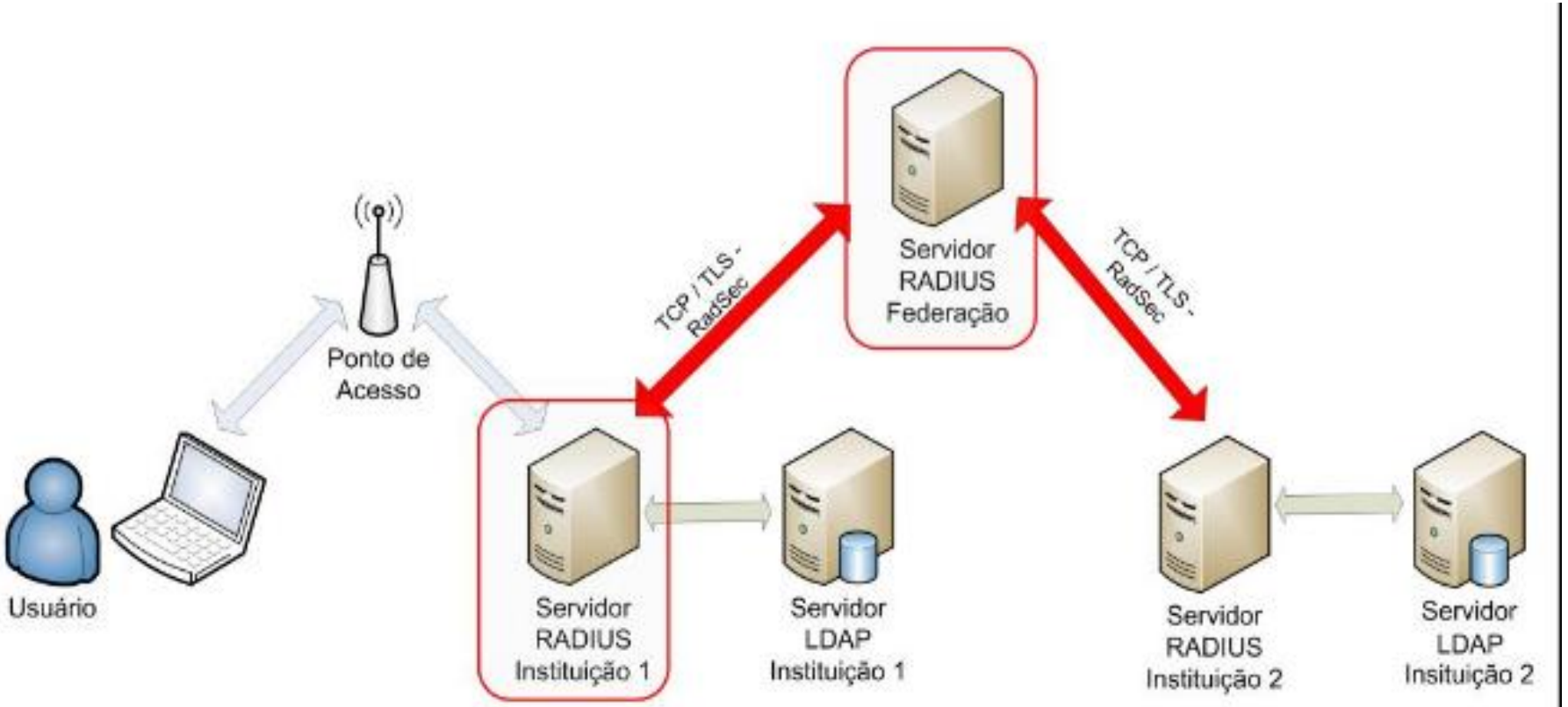
- Visibilidade
- Autenticação Segura
- WPA2/AES
  - Obrigatório
  - WPA/TKIP: hardware legado
    - TKIP basea-se em RC4 que, atualmente, é uma criptografia fraca.

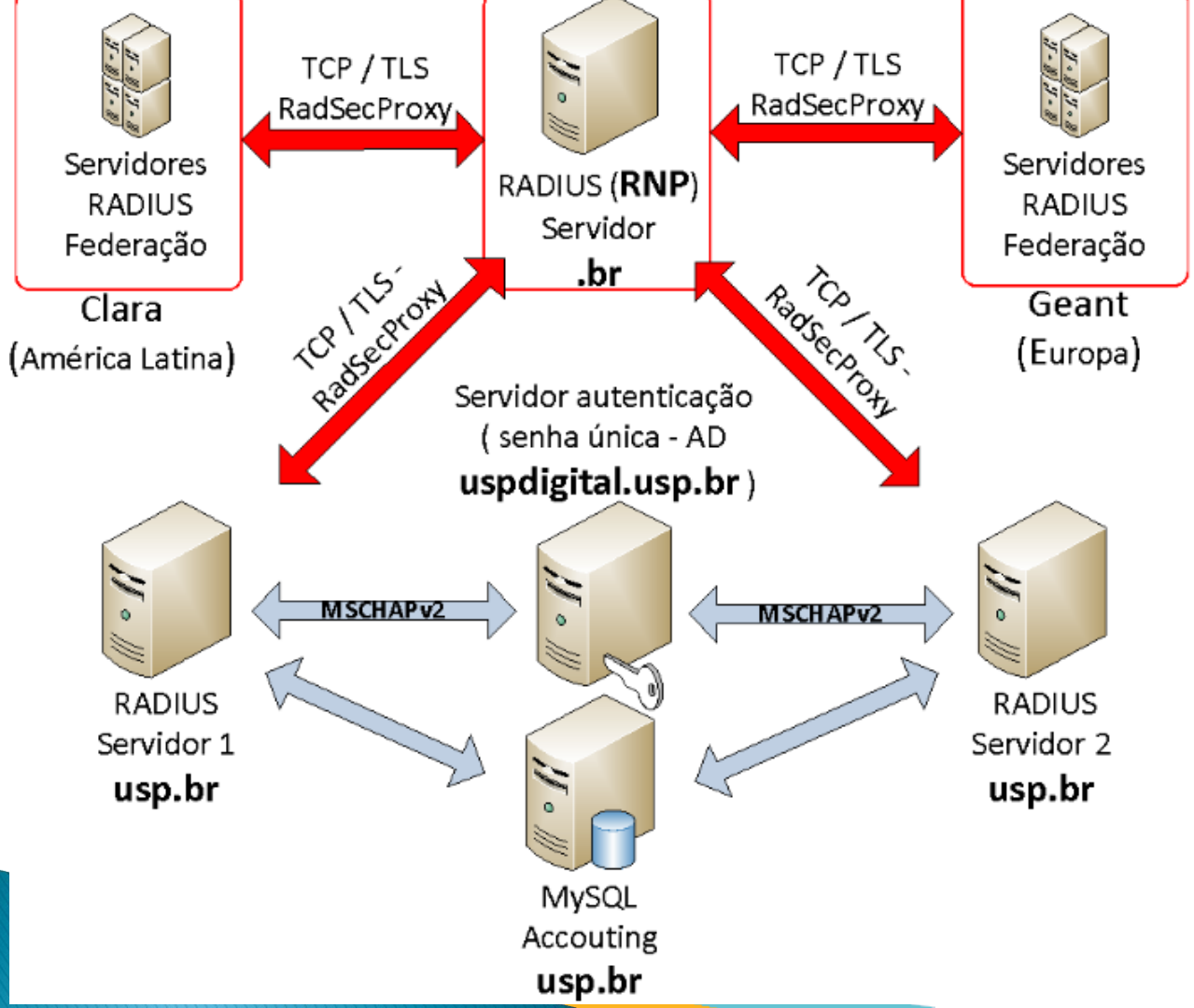
SSID - eduroam

- Obrigatório SSID **eduroam**
  - Todas letras minúsculas

- Conexão automática dentro da federação
  - Fundamental preencher @dominio_instituicao apos o ID no campo de login. Exemplo: 9987654@usp.br

Diagrama – Trust Fabric



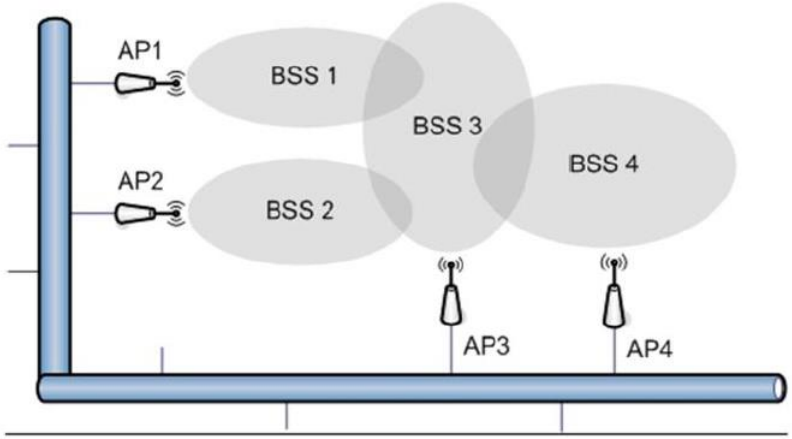


eduroam na USP

geinfo USP

- BSS: conjunto de uma AP e as estacoes que ele conecta
- Em um SP, a oferta do eduroam em múltiplos Aps fornecendo acesso a mesma vlan de clientes caracteriza uma ESS.

Conexão de várias BSS formando um Conjunto de Serviço Estendido (ESS)



Fonte: Curso eduroam – ESR/RNP

Como ativar na unidade

- Rede Clientes eduroam
  - NAT
  - DHCP
  - Vlan isolada
- APs
  - WPA2 AES
  - VLAN e subrede isoladas para gerenciamento
  - Gateway Válido

ALém dos roteiros abaixo, o Wiki da Geant possui boas referências, com roteiros para Aruba, Cisco e Juniper. 3COM 7760 (JD015A)

3COM 8760

CISCO Air LAP-1042n-a-k9 (Aironet)

CISCO Aironet 1240AG Series

CISCO Controller 5500

Controladora Aruba

D-Link DAP-2360

D-Link DAP-2590

D-Link DWL 3200

Foundry

H3C Controller WX5002

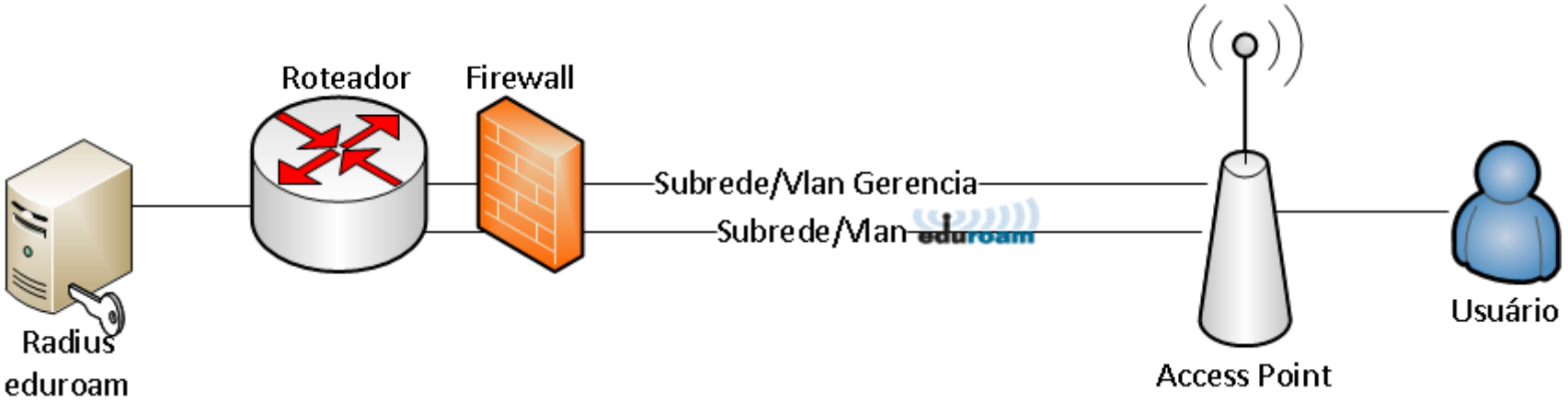
Roteiros Configuração APs

- http://eduroam.usp.br/configuracoes-de-infraestrutura/

Instalação Recomendada

- Uso de ativos de rede apropriados
  - Firewall coorporativo (vlan clientes)
  - Rotedores (roteamento clientes e gerencia)
  - Access Points coorporativos
    - Mesmo assim, respeitar o limites de usuários por AP

Diagrama


Roteador
Firewall
Subrede/Vlan Gerencia
Subrede/Vlan eduroam
Radius
eduroam
Access Point
Usuário

Exemplo: HP7500

- Módulo de firewall pode fazer o NAT
  - Separar ips válidos diferentes para NAT de gerência e NAT dos clientes do eduroam.
- Usar vlans diferentes para gerencia e eduroam
- DHCP da vlan/subrede de clientes do eduroam
- Funciona melhor para aplicativos VoIP e de videoconferência.

Instalação curinga

- pfSense
  - Firewall
  - NAT
  - DHCP
  - DHCPv6
- Lembrar
  - Separar por vlans
  - Bloquear tráfego entre rede gerencia e rede clientes.

Diagrama com pfSense

Como usar pfSense (NICs)

- Dependendo das interfaces físicas disponíveis, usar as porta do switch em modo acesso ou trunk (tag permit)
- Se usar tag, criar a vlan no pfSense e usar a interface com vlan no OPT#.
- OPT da lan eduroam com ipv4 e ipv6

Como usar pfSense (DHCP)

- Somente na interface/vlan de clientes do eduroam
- Especificar os DNS recursivos da USP

- DHCP**6**_Server
  - Statefull
- DHCPServer
- Escolher range grande de ips
  - Reservar os dez primeiros ips da subrede e os 5 últimos para fins administrativos

DNS

- No DHCPServer preencha 143.107.253.3 e 143.107.51.2
- No DHCP**6**_Server preencha 2001:12d0::3 e 2001:12d0:c000::190

Estes servidores suportam DNSSEC

Como usar pfSense (Firewall)

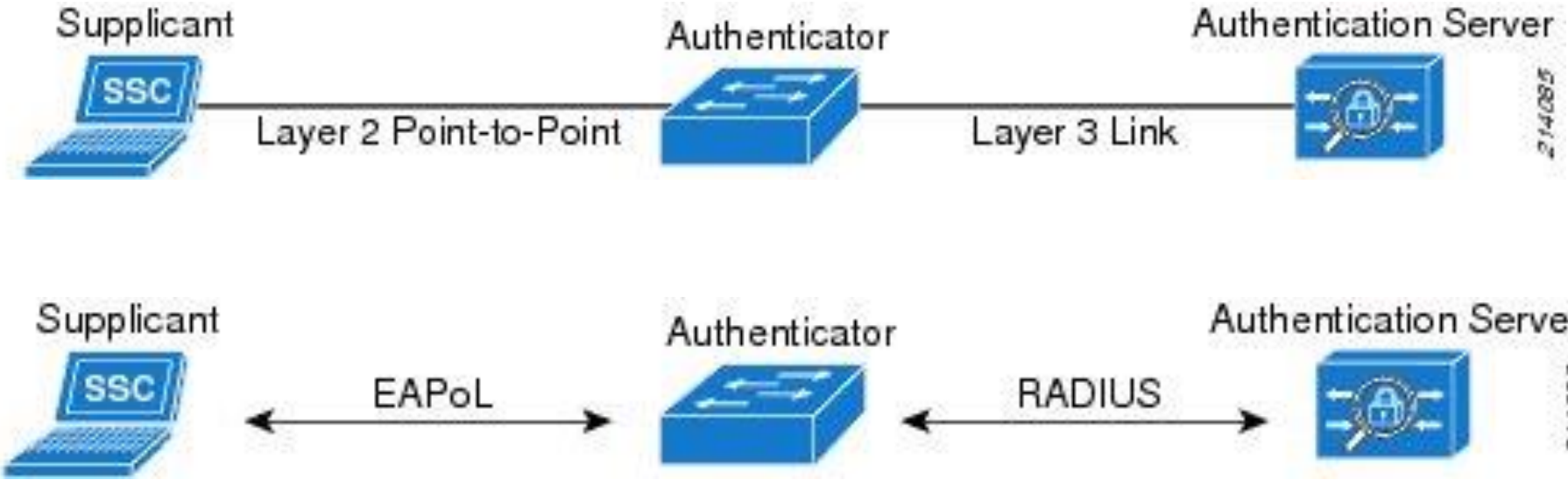
- Liberar comunicação bidirecional com as portas UDP 1812 e 1813 dos servidores RADIUS

- Liberar
  - VoIP/SIP/H323 (videoconferência)
  - VPNs
  - Toda a saída e entrada established ?

Atores de Autenticação

- Suplicante
  - Dispositivo Cliente (smartphone, notebook, desktop, etc)
- NAS (Network Access Server)
  - AcessPoint
- Radius
  - Servidor AAA (Autenticação, Autorização e Accounting)

802.1X


Supplicant
Authenticator
Authentication Server
SSC
Layer 2 Point-to-Point
Layer 3 Link
214085
Supplicant
Authenticator
Authentication Server
SSC
EAPoL
RADIUS
214086

EAPoL

- Code indica tipo de pacote EAP e como deve ser interpretado o campo —data. Tipos comuns:

1: Request

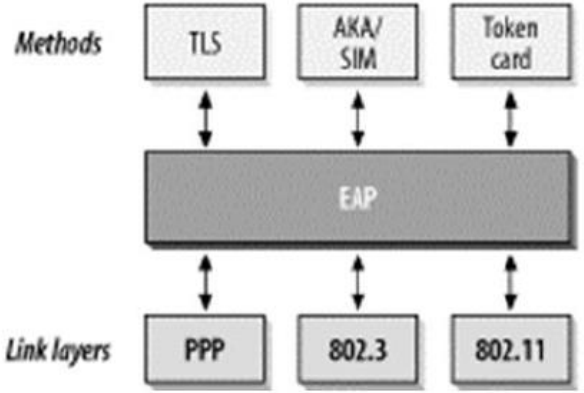
2: Response

3: Success

4: Failure

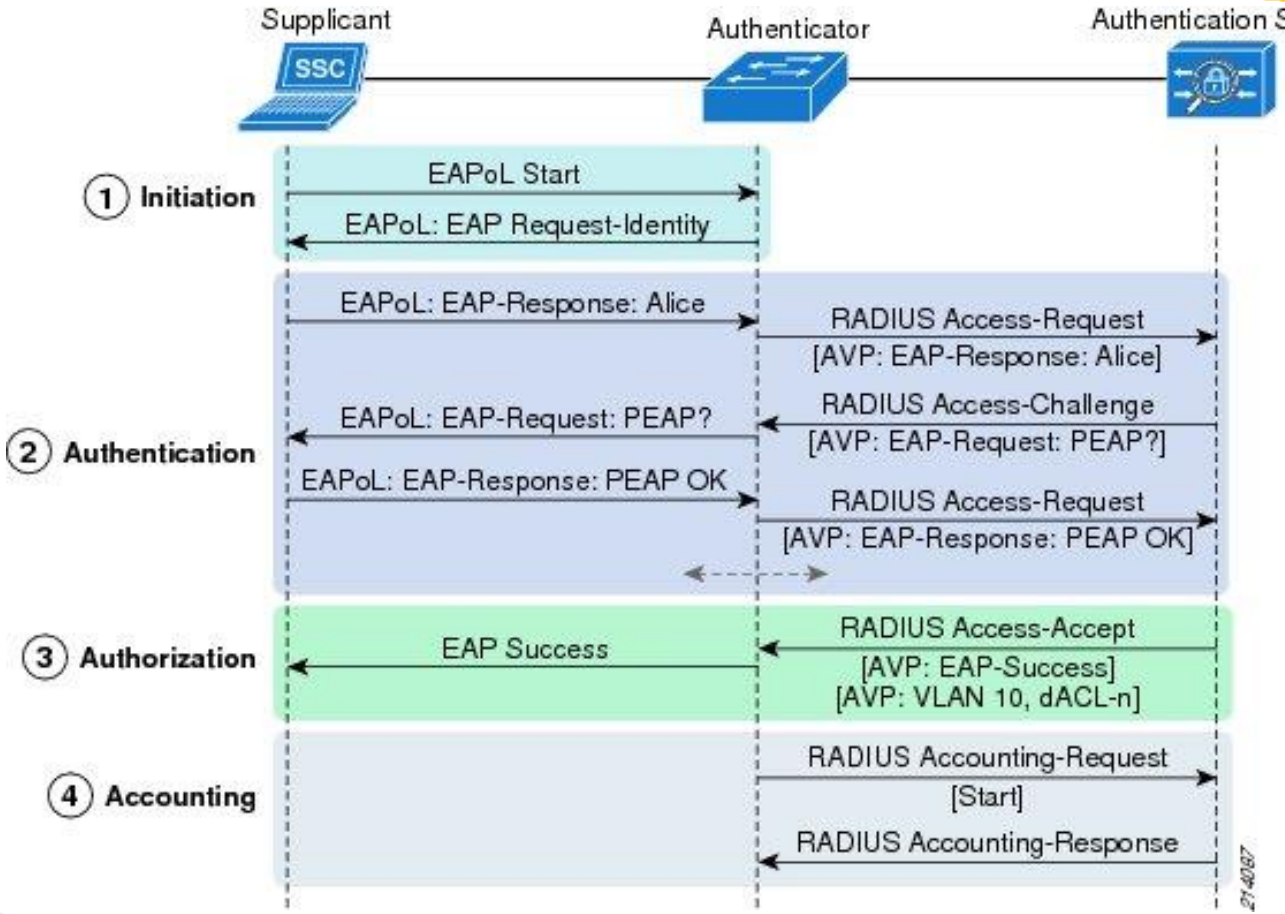
Formato do quadro

Transporta diversos protocolos de autenticação sobre diversos protocolos de camada de enlace.



Fonte: Curso eduroam – ESR/RNP

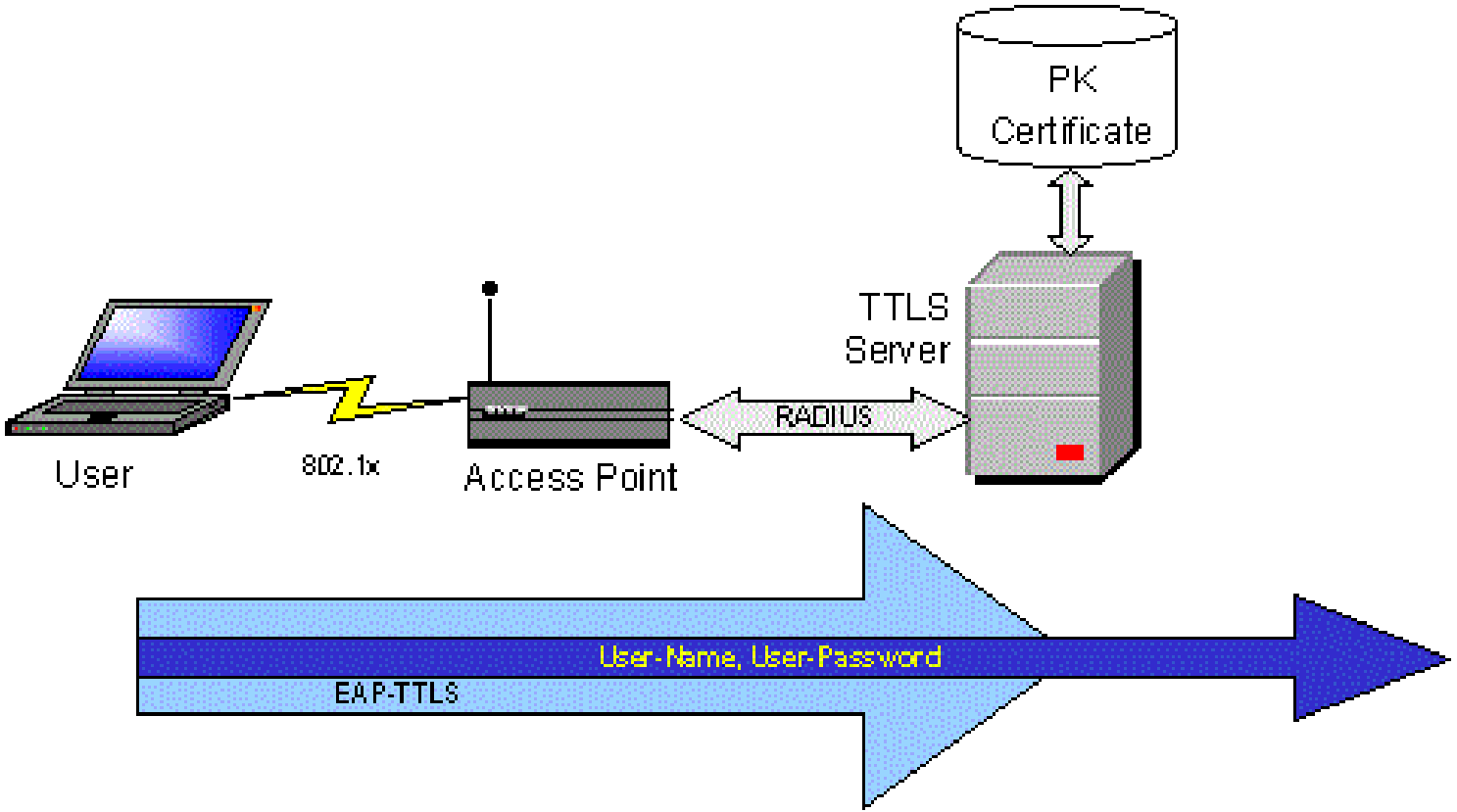
Sequência 802.1X



Processo de Autenticação

- Canal Criptográfico entre NAS e Radius
- Após estabelecer o canal, o NAS envia a senha para o servidor RADIUS

- Durante o processo, o cliente **não** tem acesso L2.


PK
Certificate
TTLS
Server
RADIUS
User
802.1x
Access Point
User-Name, User-Password
EAP-TTLS

MSCHAPv2

- Autenticação Mútua
  - Envio de desafios nos dois sentidos
  - Envia a senha junto com um conjunto de desafios
- Melhor que PAP (senha aberta)
    - Mesmo assim, possui vulnerabilidades.

CAT.eduroam.org

- Android
  - TTLS+MsCHAPv2 (Config. Manual)
  - Bug para usar dois certificados Radius
- Outros sistemas operacionais
  - Use instalador do CAT

Incidentes de segurança

- http://gestao.eduroam.usp.br
- Armazenamos accounting por 3 anos
- Auditabilidade
- Ipv6 facilita tratamento

- https://tools.ietf.org/html/rfc7593#section-5.1

Banda de rede consumida nos aps que foram configurados para enviar accouting para o servidor central.

Início: 23/03/2015 Fim 26/03/2015

AP de origem ou NAS ID: Login: Filtrar

APs ou NAS ID Listados: Selecione um item.
Usuáarios Listados: Selecione um item.

Cliente suplicante:

TX: 3.566.536,0 MB RX: 4.288.465,0 MB

NAS_ID	Cliente suplicante	Sent (bytes)	Recieved (bytes)	Horário	AP de origem	user
10.10.182.102	34-C0-59-6C-B0-93	1484	6839	25/03/2015 09:53:56	24-A4-3C-04-89-DD:eduroam	cb13444@qmul.ac.uk
10.10.182.101	34-C0-59-6C-B0-93	1704	6839	25/03/2015 10:10:25	24-A4-3C-04-8A-57:eduroam	cb13444@qmul.ac.uk
10.10.182.103	34-C0-59-6C-B0-93	0	0	25/03/2015 14:21:11	2A-A4-3C-03-89-6F:eduroam	cb13444@qmul.ac.uk
10.10.182.103	34-C0-59-6C-B0-93	1484	6839	25/03/2015 14:23:18	2A-A4-3C-03-89-6F:eduroam	cb13444@qmul.ac.uk
143.107.151.34	CC-FA-00-B3-EE-1F	4294967296	4294967296	23/03/2015 10:50:38	DE-9F-DB-1B-1F-E0:eduroam	@bristol.ac.uk
143.107.151.34	CC-FA-00-B3-EE-1F	0	0	23/03/2015 10:54:58	DE-9F-DB-1C-1F-E0:eduroam	@bristol.ac.uk
143.107.151.34	CC-FA-00-B3-EE-1F	0	0	23/03/2015 10:57:15	DE-9F-DB-1B-1F-E0:eduroam	@bristol.ac.uk
143.107.151.34	CC-FA-00-B3-EE-1F	4294967296	4294967296	23/03/2015 10:59:52	DE-9F-DB-1C-1F-E0:eduroam	@bristol.ac.uk
143.107.151.34	CC-FA-00-B3-EE-1F	4294967296	4294967296	23/03/2015 12:01:45	DE-9F-DB-1C-A3-EF:eduroam	@bristol.ac.uk
143.107.151.34	CC-FA-00-B3-EE-1F	0	0	23/03/2015 15:15:18	DE-9F-DB-1C-A3-EF:eduroam	@bristol.ac.uk

- Filtros
  - Data
  - Usuario

Dados do accounting

radacctid	bigint(21)	**connectinfo_start**	varchar(50)
acctsessionid	varchar(64)	**connectinfo_stop**	varchar(50)
acctuniqueid	varchar(32)	**acctinputoctets**	bigint(20)
username	varchar(64)	**acctoutputoctets**	bigint(20)
groupname	varchar(64)	**calledstationid**	varchar(50)
realm	varchar(64)	**callingstationid**	varchar(50)
nasipaddress	varchar(15)	**acctterminatecause**	varchar(32)
nasportid	varchar(15)	**servicetype**	varchar(32)
nasporttype	varchar(32)	**framedprotocol**	varchar(32)
acctstarttime	datetime	**framedipaddress**	varchar(15)
acctstoptime	datetime	**acctstartdelay**	int(12)
acctsessiontime	int(12)	**acctstopdelay**	int(12)
acctauthentic	varchar(32)	**xascendsessionsvrkey**	varchar(10)

Problemas de Segurança Comuns em Redes Sem Fio

- Associação não autorizada
- Negação de Serviço (DoS)
- Interceptação de tráfego

Segurança – infraestrutura eduroam

- Entre APs e RADIUS
  - Shared secret
  - Responsabilidade do SP
- Clientes
  - Verificar o certificado do RADIUS

Segurança - Detalhamento

- Isolamento L2
  - Vlan distinta cliente e gerencia
- Isolamento L3
  - Bloqueio de trafego entre rede de clientes e entre clientes e rede de gerencia
- Senhas fortes
  - Gerencia AP
  - Secret Radius
- Firmware Atualizados
- Certificados nos servidores RADIUS (TTLS e PEAP)

Firewall

- Liberar todo icmpv6, VPN, VoIP, SIP, H323, etc

- SP tem liberdade para liberar tudo. Se for bloquear, pelo menos a lista ao lado deve ser liberada.

Service	Protocol / Port	Direction
Standard IPSec VPN	IP protocol 50 (ESP) IP protocol 51 (AH) UDP port 500 (IKE)	incoming and outgoing incoming and outgoing outgoing
OpenVPN 2.0	UDP port 1194	incoming and outgoing
IPv6 Tunnel broker service	IP protocol 41	incoming and outgoing
IPSec NAT-Traversal	UDP/4500	incoming and outgoing
Cisco IPSec VPN over TCP	TCP/10000	outgoing
PPTP VPN	IP protocol 47 (GRE) TCP port 1723	incoming and outgoing outgoing
SSH	TCP port 22	outgoing
HTTP	TCP port 80 TCP port 443 TCP port 3128 TCP port 8080	outgoing outgoing outgoing outgoing
Mail sending	TCP port 465 TCP port 587	outgoing outgoing
Mail reception	TCP port 143 TCP port 993 TCP port 110 TCP port 995	outgoing outgoing outgoing outgoing
FTP (passive)	TCP port 21	outgoing

geinfo USP

Fluxo diagnóstico de problemas

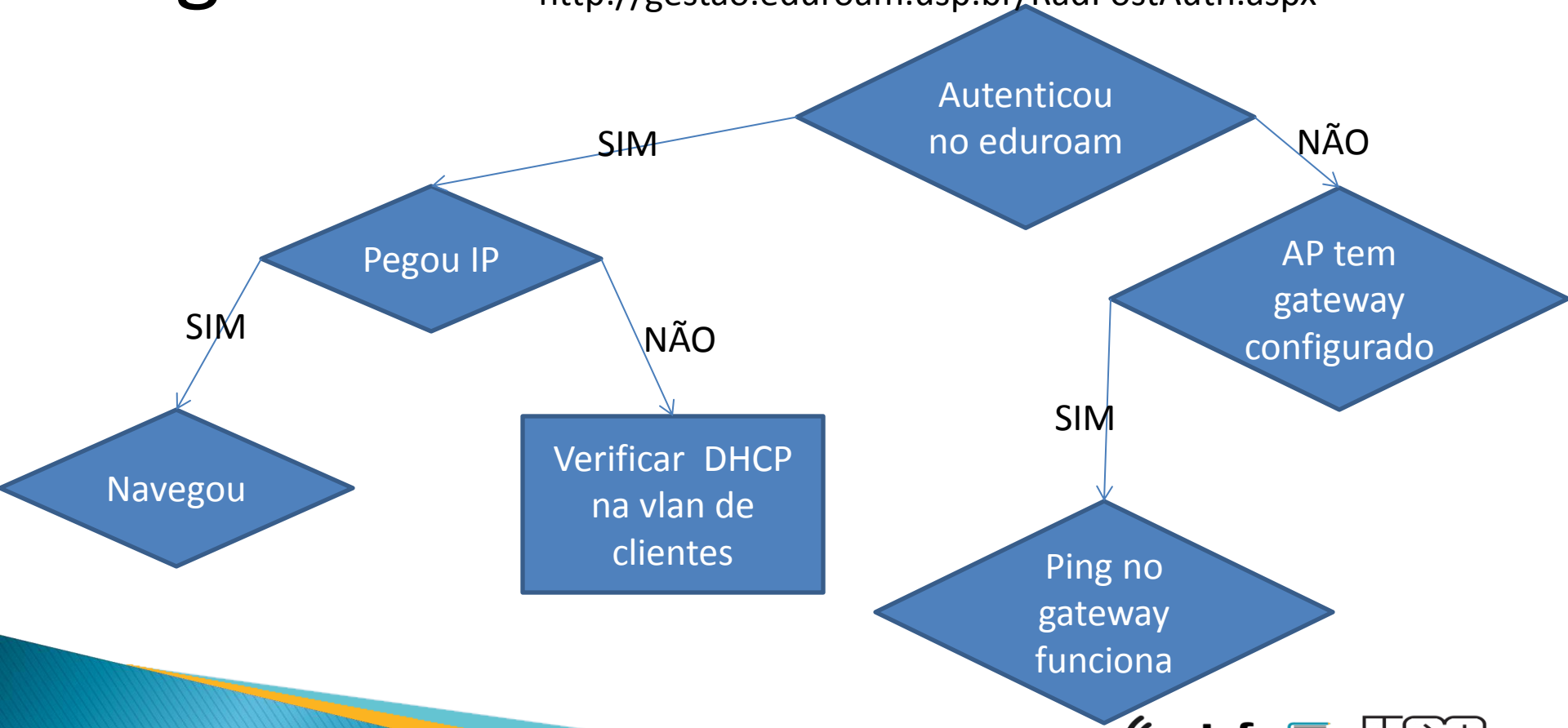
- Fluxograma
- http://Gestao.eduroam.usp.br
- Logs armazenados
- Correlação logs DHCP e accounting
  - NAT atrapalha
  - IPv6 ajuda

Primeiramente, verifique:

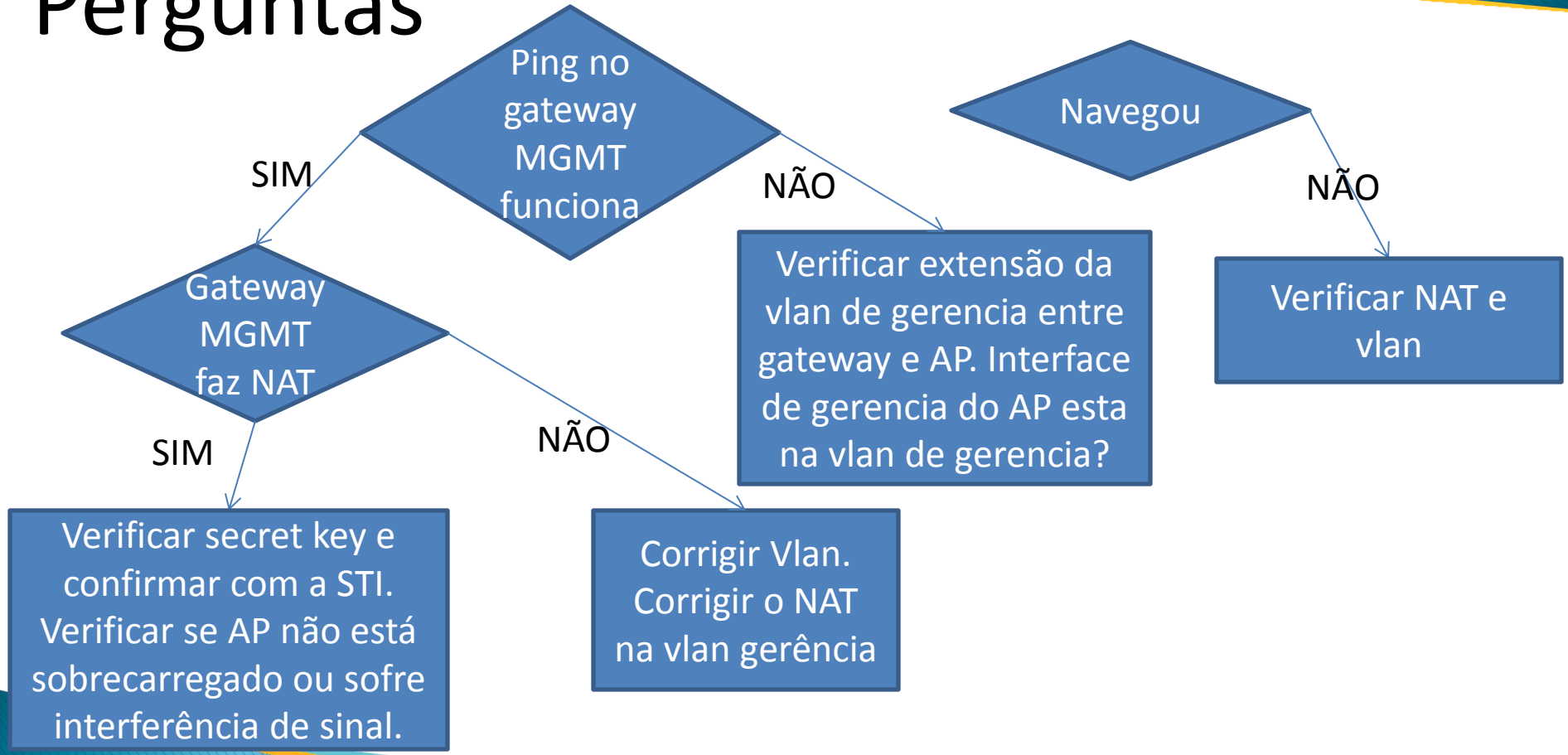
- Porta do switch
  - Modo Trunk
  - Vlans do eduroam e de gerência de Aps permitidas
- Ip de gerência do AP
  - Na vlan de gerência
- Ssid eduroam
  - Na vlan do eduroam
- Caminho entre Aps e servidores de NAT e DHCP
  - Vlan devem estar estendidas
  - porta de interconexão modo trunk all vlans

Perguntas

Veja logins bem sucedidos em
http://gestao.eduroam.usp.br/RadPostAuth.aspx



Perguntas


Ping no gateway MGMT funciona
SIM
NÃO
Gateway MGMT faz NAT
SIM
NÃO
Verificar secret key e confirmar com a STI. Verificar se AP não está sobrecarregado ou sofre interferência de sinal.
Corrigir Vlan. Corrigir o NAT na vlan gerência
Verificar extensão da vlan de gerencia entre gateway e AP. Interface de gerencia do AP esta na vlan de gerencia?
Navegou
NÃO
Verificar NAT e vlan

Benefícios

- Mobilidade
- Segurança
- IPv6
- Senha Única
- Acesso Federado
  - Acesso transparente a usuários de outras instituições

- TEMPO PARA PERGUNTAS
- Eduroam AT usp PONTO br
- https://atendimentosti.usp.br

http://eduroam.usp.br

https://wiki.geant.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus

https://www.eduroam.org/downloads/docs/GN3-12-192_eduroam-policy-service-definition_ver28_26072012.pdf

https://www.youtube.com/watch?v=x1YhuFPxMz8

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html