
ESTD1845
QUEEN'S
UNIVERSITY
BELFAST

AAA/Firewalls – Part 1

Dr. Sandra Scott-Hayward

CSC3064 Lecture 11

School of Electronics, Electrical Engineering and Computer Science

Session Overview

- Network Access Control
- AAA – RADIUS, Kerberos
- IEEE 802.1X
- Virtual Local Area Networks (VLANs)

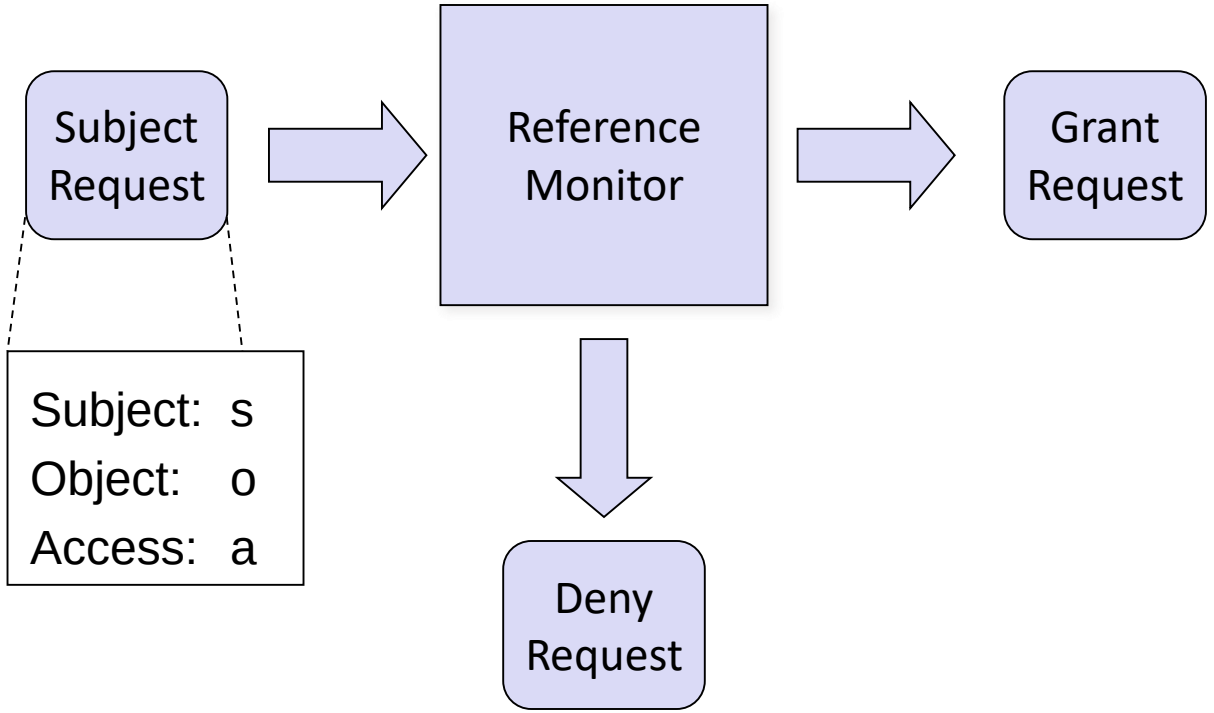
References:
Jacobson, Douglas. *Introduction to network security*. CRC Press, 2008.
Schäfer, Günter, and Michael Rossberg. *Security in Fixed and Wireless Networks*. John Wiley & Sons, 2016.
Stallings, William. *Network security essentials: applications and standards*. Pearson Education India, 2007

QUEEN'S UNIVERSITY BELFAST

What is access control?

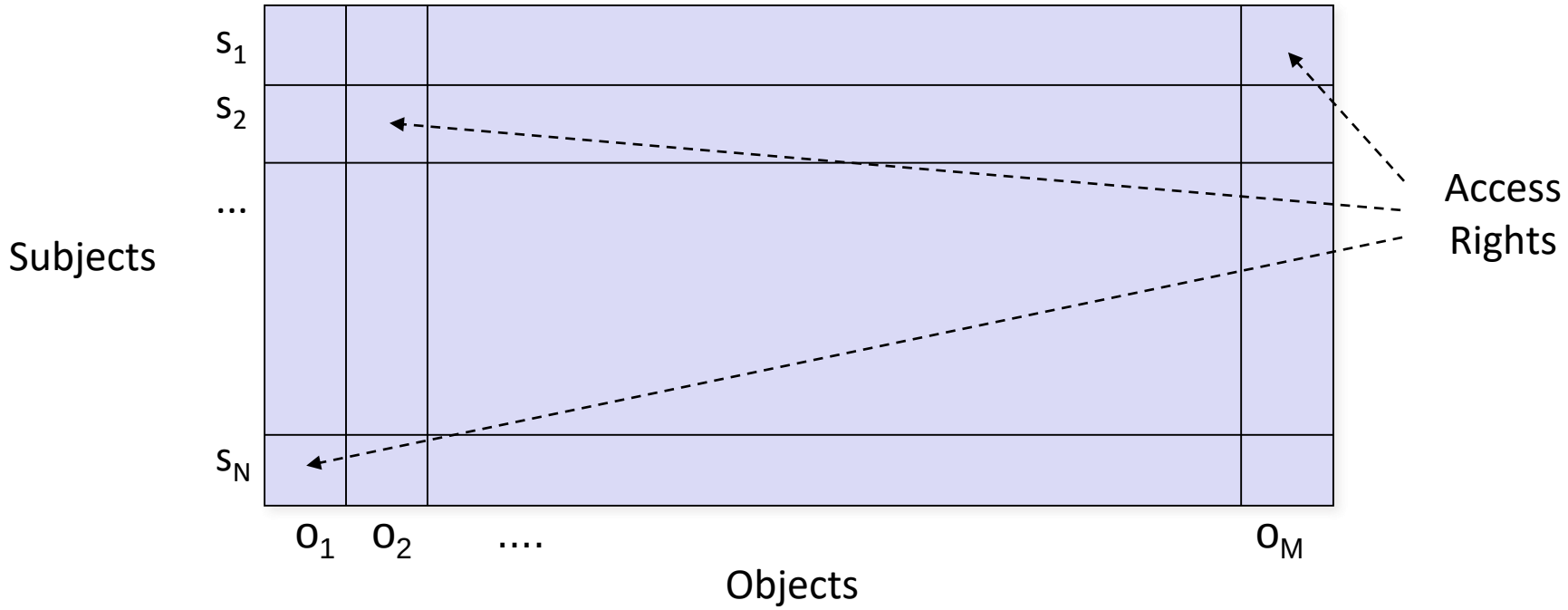
Access control comprises those mechanisms that enforce mediation on subject requests for access to objects as defined in some specified security policy.

An important conceptual model in this context is the *reference monitor*:



QUEEN'S UNIVERSITY BELFAST

Access matrix



	UserMary Directory	UserBob Directory	UserBruce Directory	Printer001
Mary	Full Control	Write	Write	Execute
Bob	Read	Full Control	Write	Execute
Bruce	No Access	Write	Full Control	Execute
Sally	No Access	No Access	No Access	No Access

QUEEN'S UNIVERSITY BELFAST

Network Access Control

- NAC Systems deal with 3 categories of components:

Access Requester (AR)

- Node that is attempting to access the network and may be any device that is managed by the NAC system, including workstations, servers, printers, cameras, and other IP-enabled devices
- Also referred to as *supplicants,* or clients

Policy Server

- Determines what access should be granted
- Often relies on backend systems

Network Access Server (NAS)

- Functions as an access control point for users in remote locations connecting to an enterprise's internal network
- Also called a *media gateway, remote access server (RAS), or policy server*
- May include its own authentication services or rely on a separate authentication service from the policy server

QUEEN'S UNIVERSITY BELFAST

What is AAA?

- Authentication
  - ensuring that the identity of an entity is correct, based on known credentials

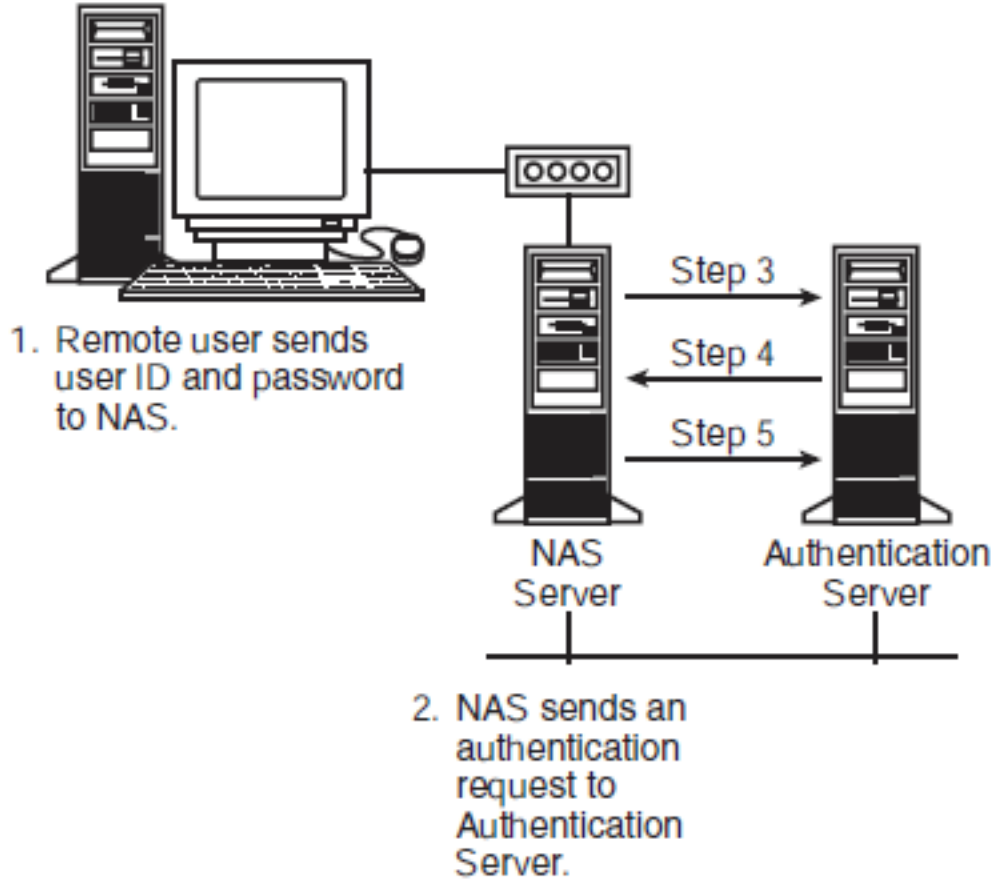
- Authorization
  - ensuring that an entity has permission to access the resource they are requesting

- Accounting
  - keeping an auditable record of which entities have accessed which resources

QUEEN'S UNIVERSITY BELFAST

Basic Steps of a AAA service

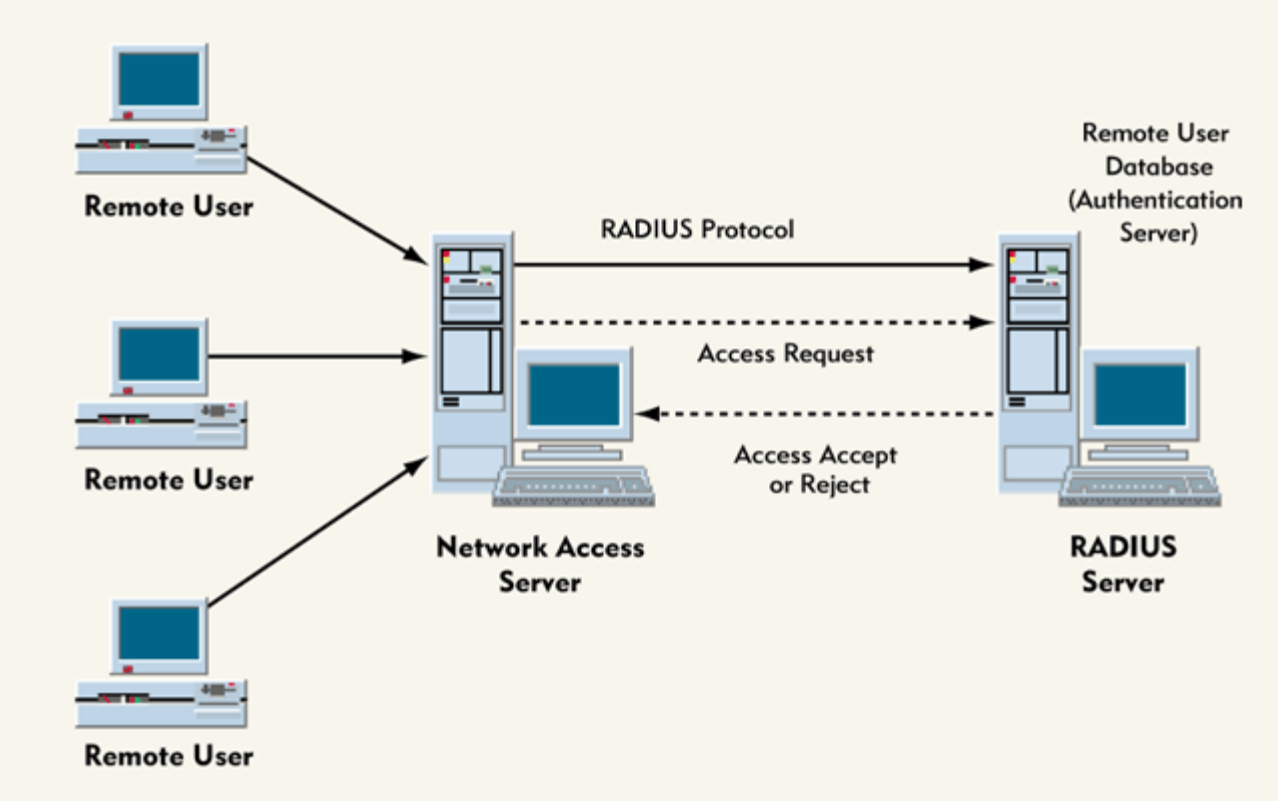
1. Remote user sends a user ID and password to the NAS (network access server).
2. The NAS collects the remote user's user ID and password.
3. The NAS sends an authentication request to the AAA server (policy server).
4. The AAA server checks identity and returns connection parameters and authorization information.
5. The NAS confirms connection and writes the audit record.



QUEEN'S UNIVERSITY BELFAST

RADIUS

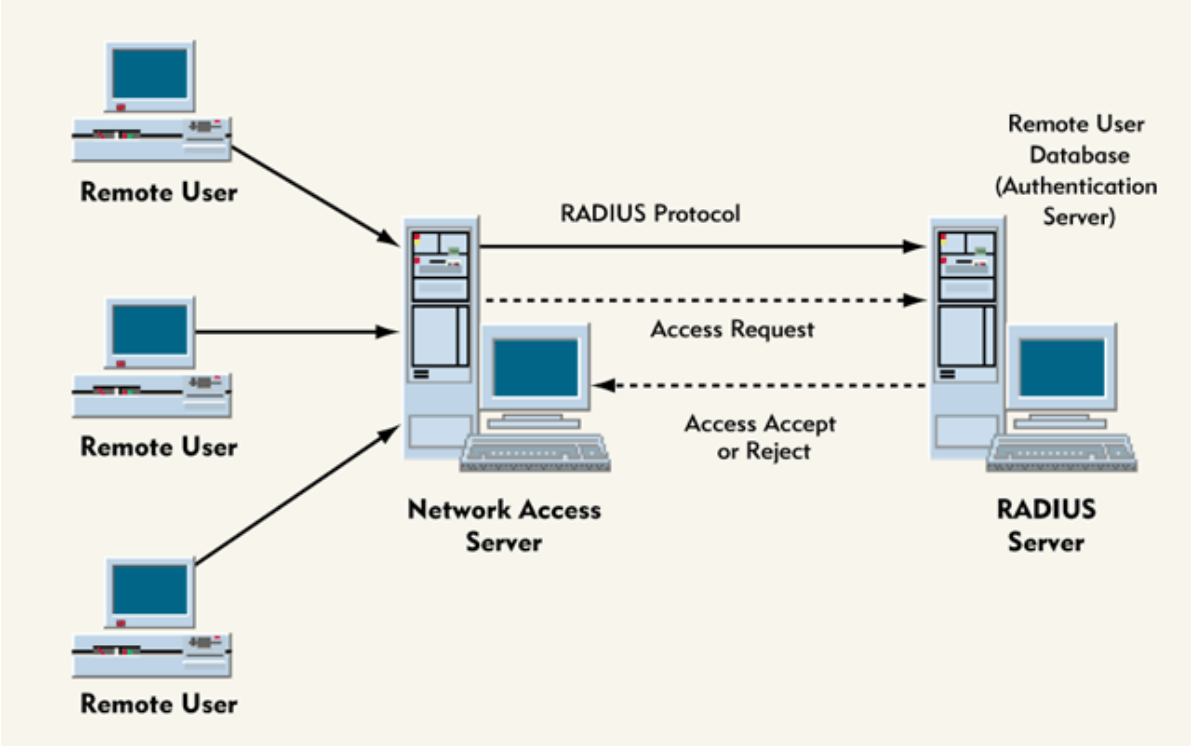
- Remote Authentication Dial-In User Service (RADIUS)
- Networking protocol providing centralized AAA services



QUEEN'S UNIVERSITY BELFAST

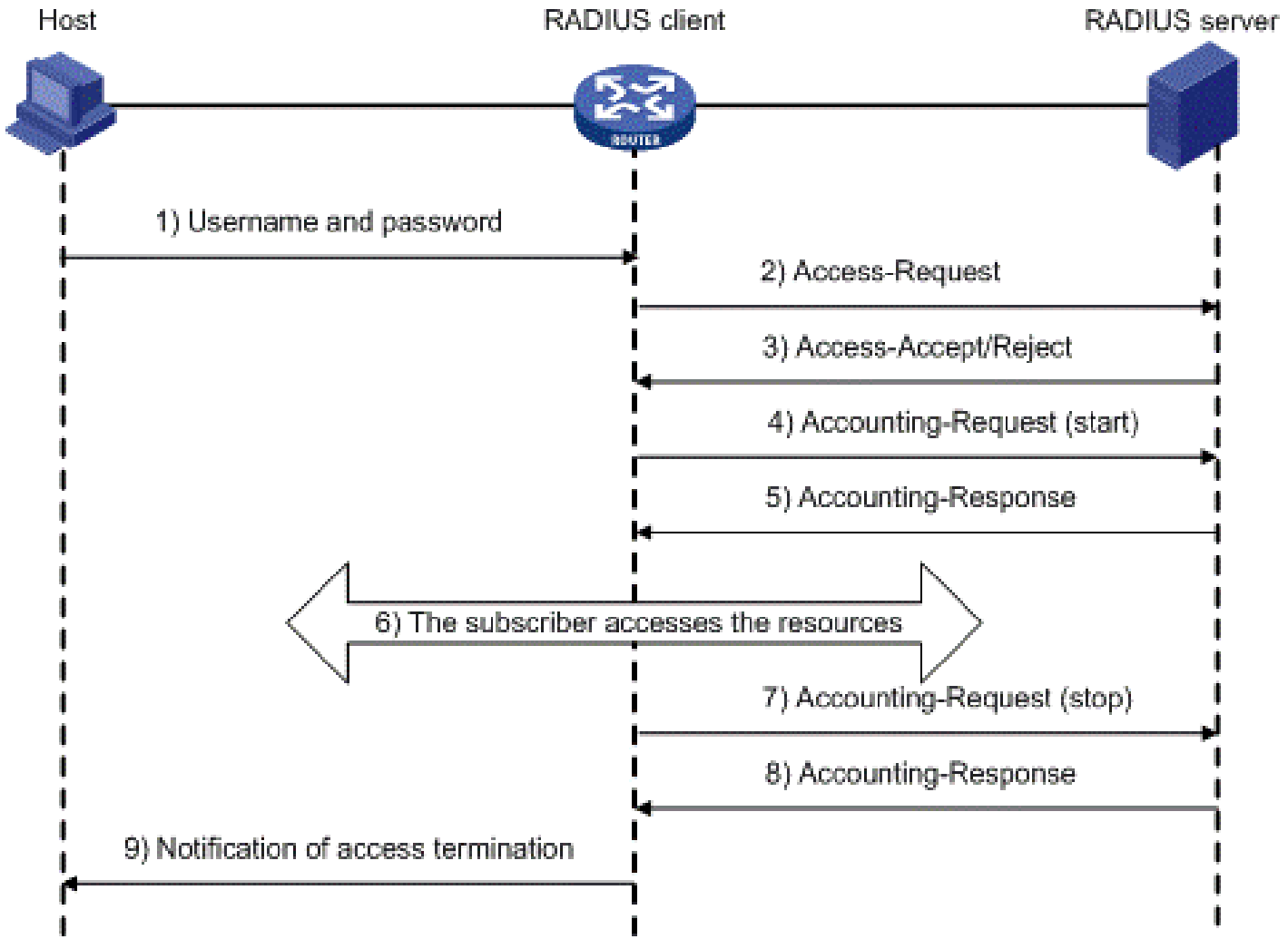
RADIUS

1. User initiates PPP authentication to the NAS.
2. NAS prompts for username and password (if Password Authentication Protocol [PAP]) or challenge (if Challenge Handshake Authentication Protocol [CHAP]).
3. User replies.
4. RADIUS client sends username and encrypted password to the RADIUS server.
5. RADIUS server responds with Accept, Reject, or Challenge.
6. The RADIUS client acts upon services and services parameters bundled with Accept or Reject.



QUEEN'S UNIVERSITY BELFAST

RADIUS - Accounting



QUEEN'S UNIVERSITY BELFAST

Kerberos

- A network authentication protocol
- Provides strong authentication for client/server applications by using secret key cryptography
- Effective in open distributed environments where users have a unique ID for each application
- Verifies that users are who they claim to be and network services they use are within their permission profile

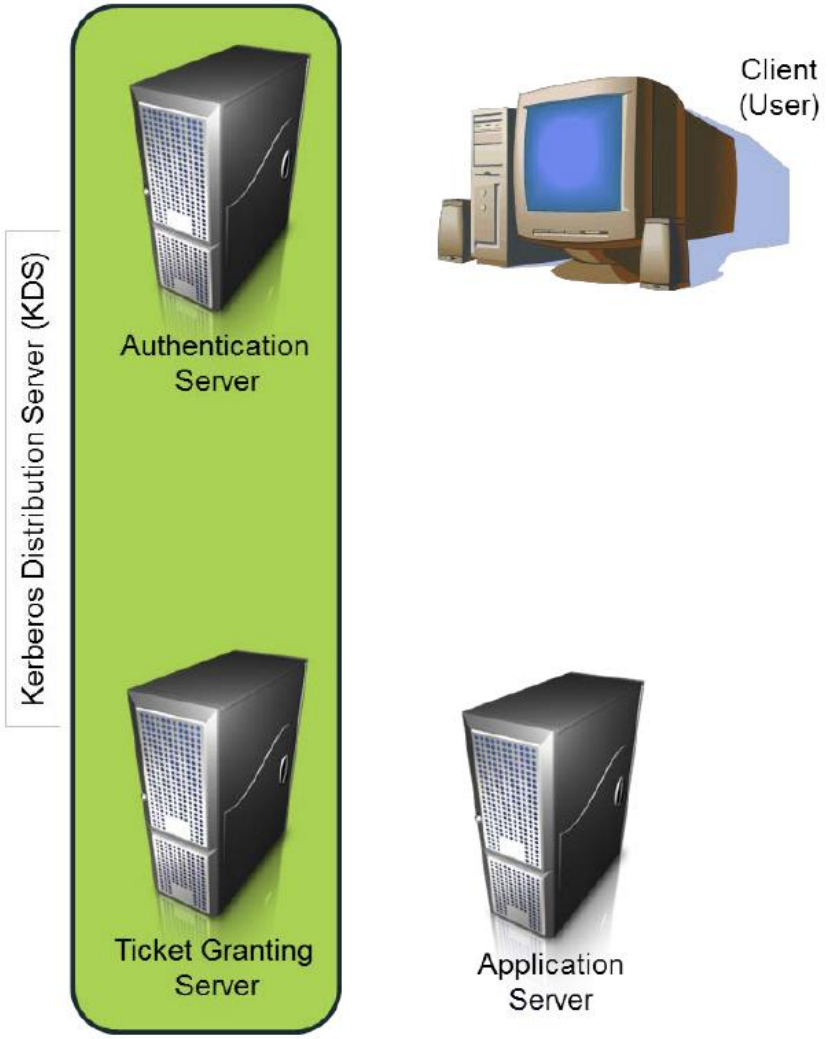
QUEEN'S UNIVERSITY BELFAST

Kerberos

- Based on interaction between:
  - The requesting system (principal)
  - The endpoint destination server (where the app or info resides)
  - The Kerberos or Key Distribution Centre (KDC)

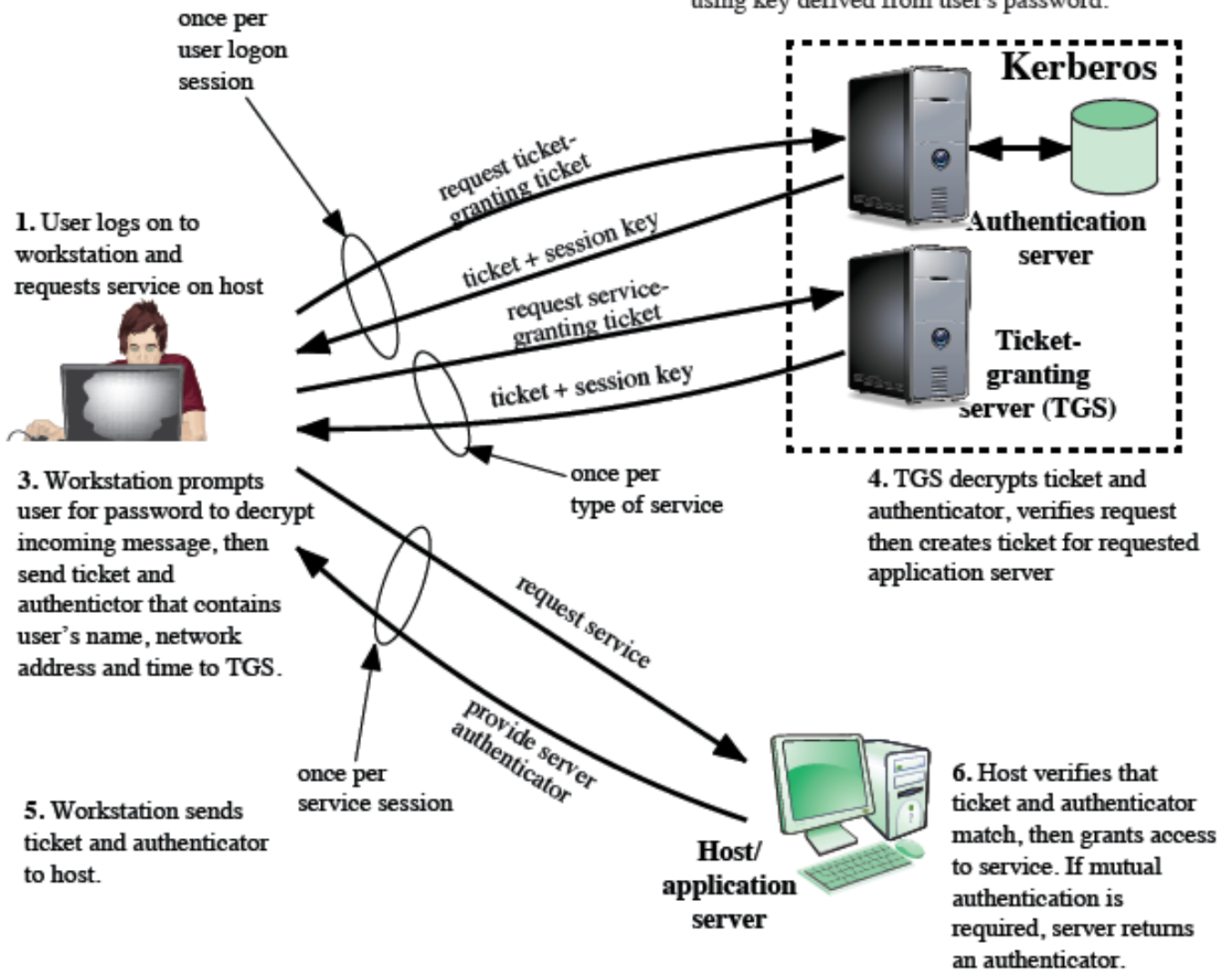
- Principal is an entity that interacts with the Kerberos server

- KDC has two functions:
  - authentication server (AS)
  - ticket-granting server (TGS)



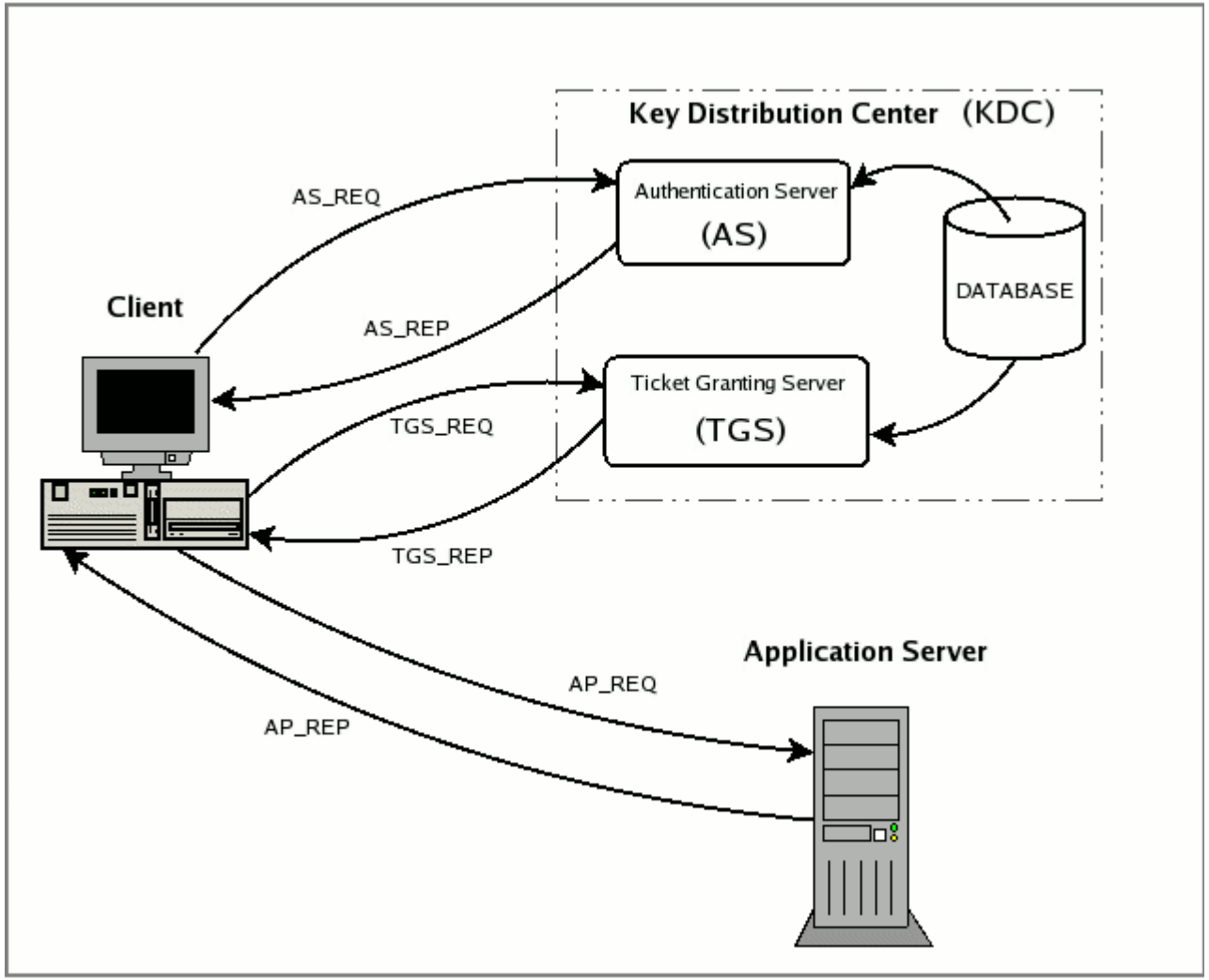
QUEEN'S UNIVERSITY BELFAST

Kerberos – Operation



QUEEN'S UNIVERSITY BELFAST

Kerberos – Operation

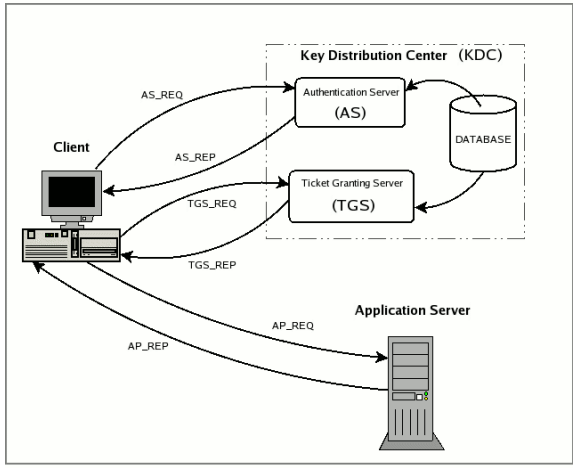


QUEEN'S UNIVERSITY BELFAST

Kerberos – Client Authentication

- **AS_REQ** is the initial user authentication request. This message is directed to the KDC component known as Authentication Server (AS);
- AS checks to see if the client is in its database. If it is,
- **AS_REP** is the reply of the Authentication Server to the previous request. Basically it contains the TGT (encrypted using the TGS secret key) and the session key (encrypted using the secret key of the requesting user);
- The client decrypts the message to retrieve the session key;
- This session key is used for further communications with the TGS. At this point, the client has enough information to authenticate itself to the TGS.

Kerberos – Client Service Request



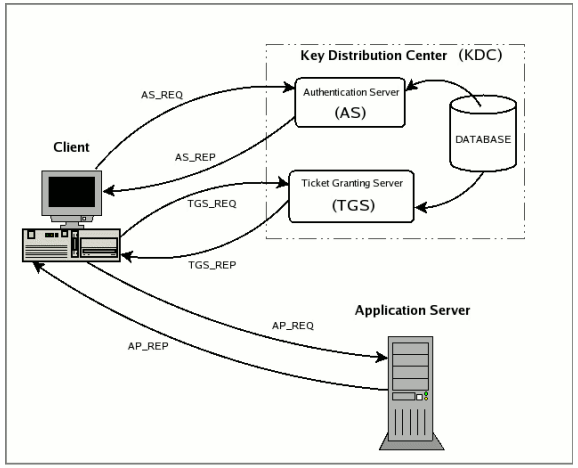
- **TGS_REQ** is the request from the client to the Ticket Granting Server (TGS) for a service ticket. This packet includes the TGT obtained from the previous message and an authenticator generated by the client and encrypted with the session key;

- TGS checks to see if the service (application server) is in its database. If it is,

- **TGS_REP** is the reply of the Ticket Granting Server to the previous request. Located inside is the requested service ticket (encrypted with the secret key of the service) and a service session key generated by TGS and encrypted using the previous session key generated by the AS;

QUEEN'S UNIVERSITY BELFAST

Kerberos – Client Application Request



- **AP_REQ** is the request that the client sends to an application server to access a service. The components are the service ticket obtained from TGS with the previous reply and an authenticator again generated by the client, but this time encrypted using the service session key (generated by TGS);

- **AP_REP** is the reply that the application server gives to the client to prove it really is the server the client is expecting. This packet is not always requested. The client requests the server for it only when mutual authentication is necessary.

- The server provides the requested services to the client.

QUEEN'S UNIVERSITY BELFAST

Kerberos – Issues

- Security depends on careful implementation: Enforcing min lifetimes for the authentication credentials minimises threats of replayed credentials
- KDC must be physically secured and hardened – non-Kerberos activity not permitted
- Can be a single point of failure – should be supported by backup and continuity plans
- Key length is important:
    - Too short, vulnerable to brute force attacks
    - Too long, overloads the system with encryption/decryption computation
    - Achilles heal = Encryption processes are based on passwords – vulnerable to password guessing
- Need to embed Kerberos system calls into any application that uses the system – called Kerberizing

Network Access Enforcement Methods

- The actions that are applied to ARs to regulate access to the enterprise network
  - Many vendors support multiple enforcement methods simultaneously, allowing the customer to tailor the configuration by using one or a combination of methods

Common NAC enforcement methods:
• IEEE 802.1X • Virtual local area networks (VLANs) • Firewall • DHCP management

QUEEN'S UNIVERSITY BELFAST

IEEE 802.1X

The standard IEEE 802.1X:

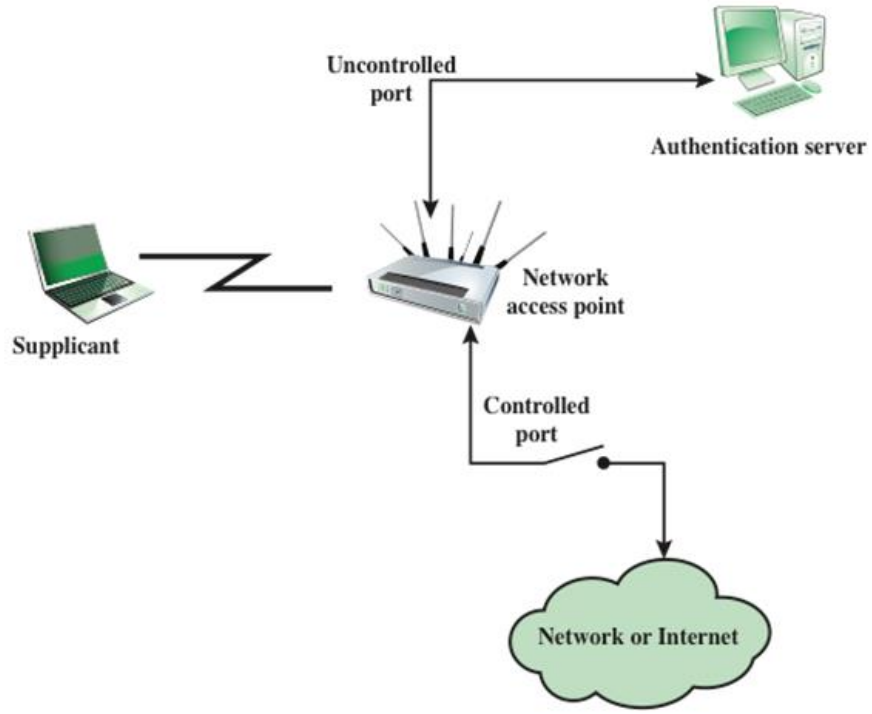
- Aims to *“restrict access to the services offered by a LAN to those users and devices that are permitted to make use of those services”*
- Defines **port based network access control** to provide a means of *“authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics”*

QUEEN'S UNIVERSITY BELFAST

IEEE 802.1X: Controlled and Uncontrolled Ports

IEEE 802.1X introduces the notion of two logical ports:

- The uncontrolled port allows to authenticate a device
- The controlled port allows an authenticated device to access LAN services



QUEEN'S UNIVERSITY BELFAST

IEEE 802.1X: Roles

Three principal roles are distinguished:

- A device that wants to use the service offered by an IEEE 802.1X LAN acts as a ***supplicant*** requesting access to the controlled port
- The point of attachment to the LAN infrastructure (e.g. network access point) acts as the ***authenticator*** demanding the supplicant to authenticate itself
- The authenticator does not check the credentials presented by the supplicant itself, but passes them to the ***authentication server*** for verification

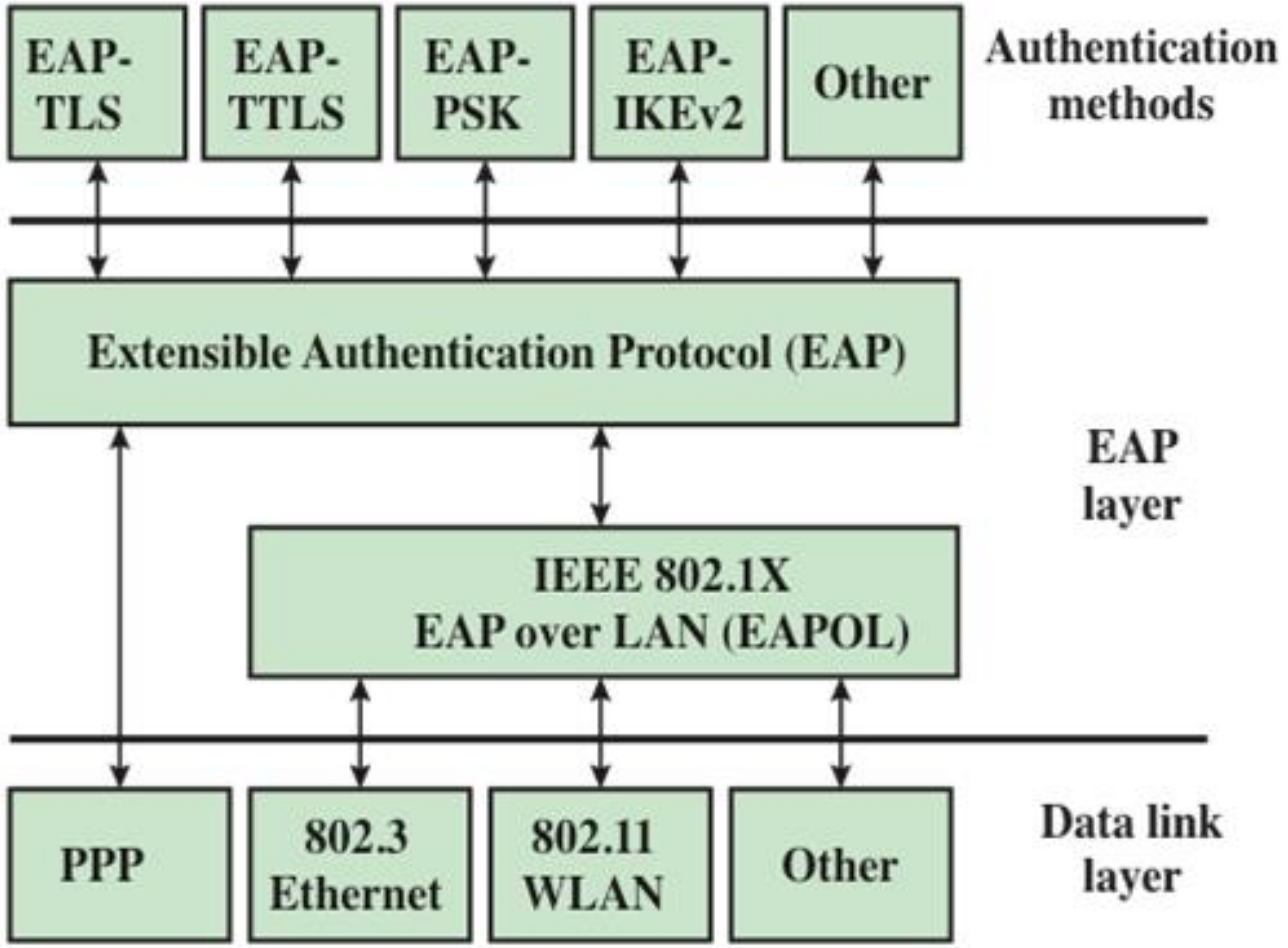
QUEEN'S UNIVERSITY BELFAST

IEEE 802.1X: Roles

Accessing a LAN with IEEE 802.1X security measures:

- Prior to successful authentication the supplicant can access the uncontrolled port:
  - The port is uncontrolled in the sense, that it allows access prior to authentication
  - However, this port allows only restricted access
- After successful authentication the controlled port is opened

IEEE 802.1X: Security Protocols



IEEE 802.1X: Security Protocols

IEEE 802.1X does not define its own security protocols, but advocates the use of existing protocols:

- The *Extensible Authentication Protocol (EAP)* may realize basic device authentication [RFC 3748]
- If negotiation of a session key during authentication is required, the use of the *EAP TLS Authentication Protocol* is recommended [RFC 5216]
- Furthermore, the authentication server is recommended to be realized with the *Remote Authentication Dial In User Service (RADIUS)* [RFC 2865]

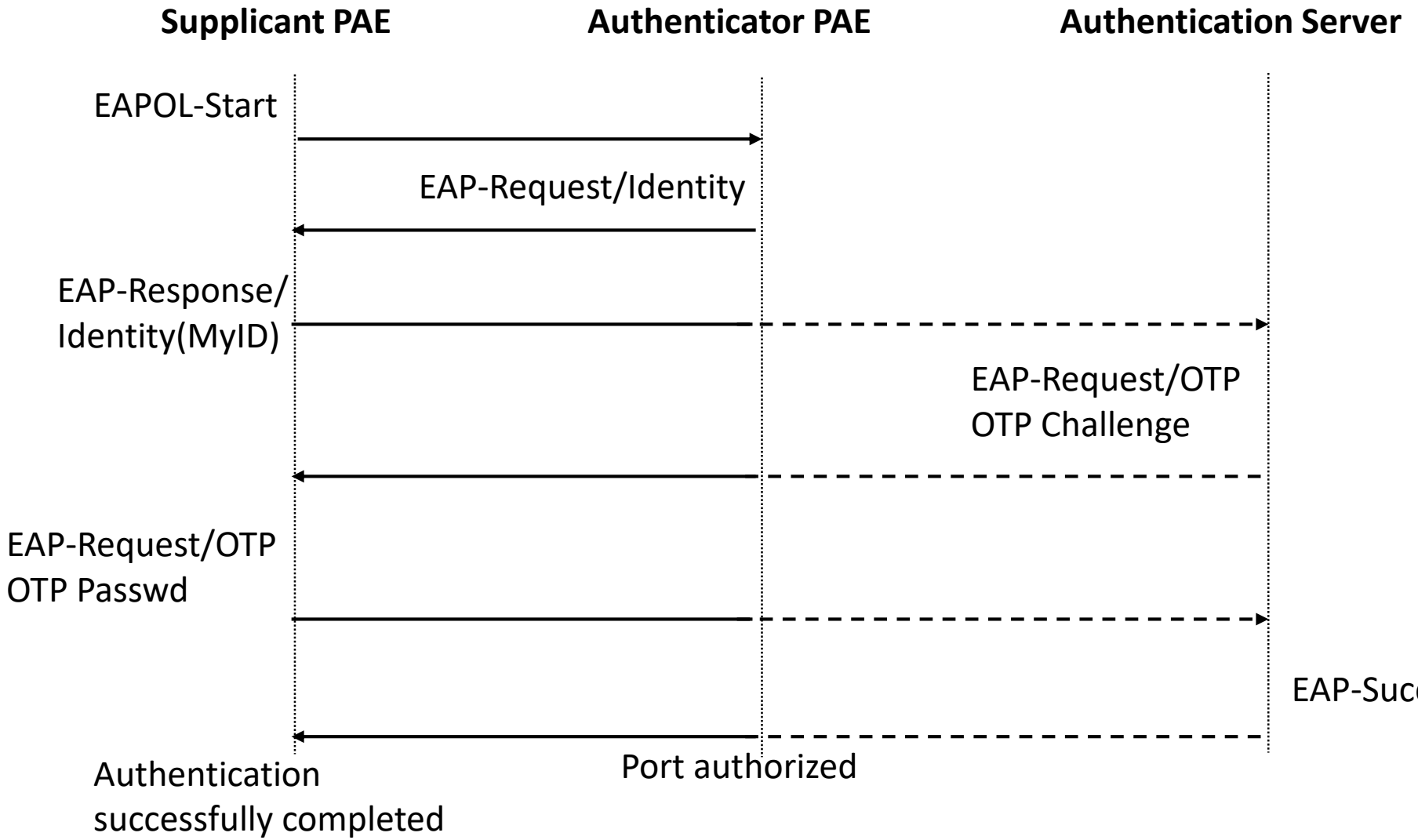
IEEE 802.1X: Message Exchange

Exchange of EAP messages between supplicant and authenticator is realized with the *EAP over LANs (EAPOL)* protocol:

- EAPOL defines the encapsulation techniques that shall be used in order to carry EAP packets between supplicant port access entities (PAE) and Authenticator PAEs in a LAN environment
- EAPOL frame formats have been defined for various members of the 802.x protocol family, e.g. EAPOL for Ethernet, ...
- Between supplicant and authenticator RADIUS messages may be used

IEEE 802.1X: Example of Authentication

Background



QUEEN'S UNIVERSITY BELFAST

IEEE 802.1Q

The standard IEEE 802.1Q:

- Allows to create *“interconnected IEEE 802 standard LANs using different or identical media access control methods“,* i.e., create separate **virtual local area networks (VLANs)** over one physical infrastructure
- Though not a real security standard, it is often used to separate different users and services from each other, e.g., untrusted guest computers from company servers, without deploying a new infrastructure
- Used to realize access control at the link level

QUEEN'S UNIVERSITY BELFAST

IEEE 802.1Q: Basic Operation

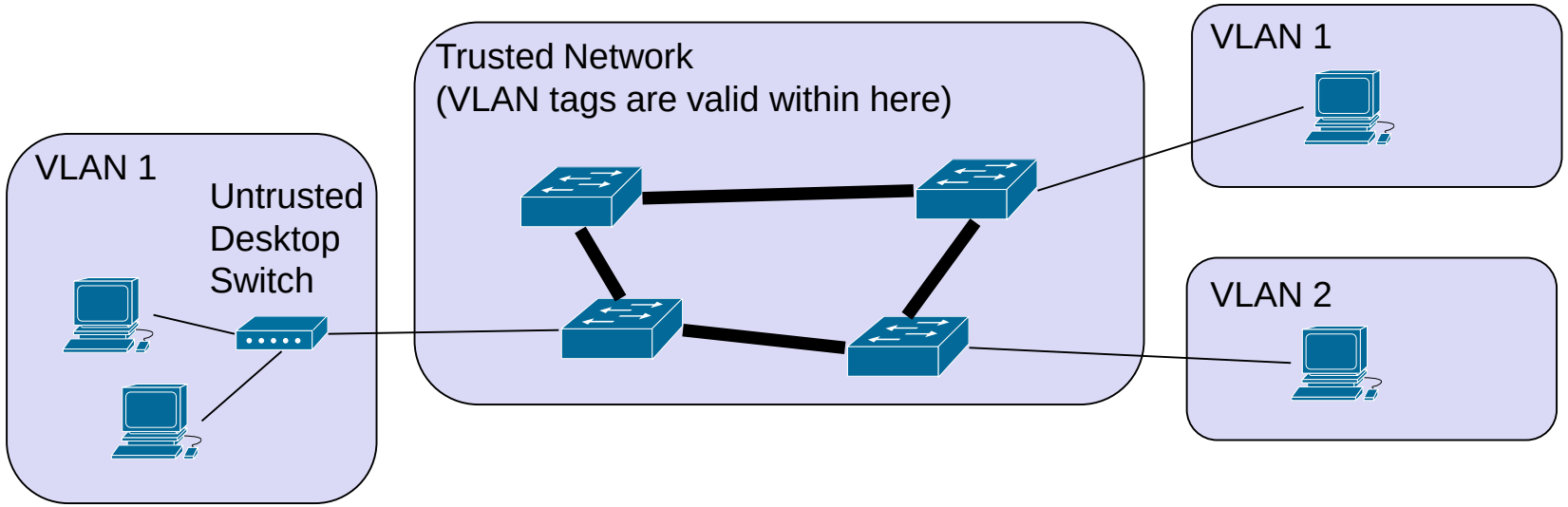
- Each network packet is marked with a VLAN tag including a 12 bit VLAN ID that identifies a virtual network

- Switches ensure that packets with certain VLAN IDs are only delivered to certain network ports, e.g. a VLAN with internal company information is not delivered to a publically available port

- The VLAN ID is not cryptographically protected
  - Usually VLAN IDs are inserted at the first trusted switch and removed at the last trusted switch on the path through the network

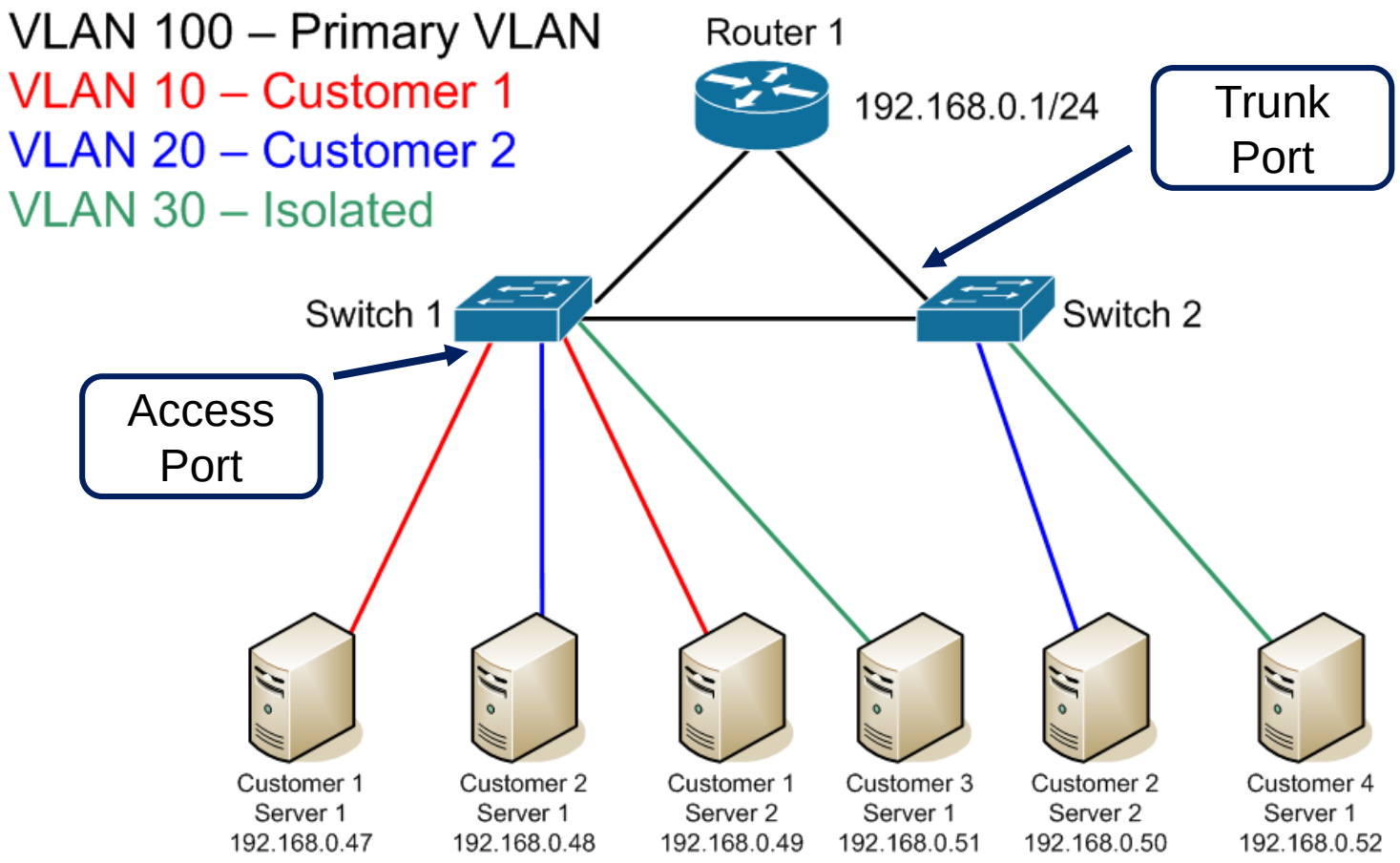
IEEE 802.1Q: Typical Deployment Scenario

- Different ports to the trusted core are mapped to VLANs



QUEEN'S UNIVERSITY BELFAST

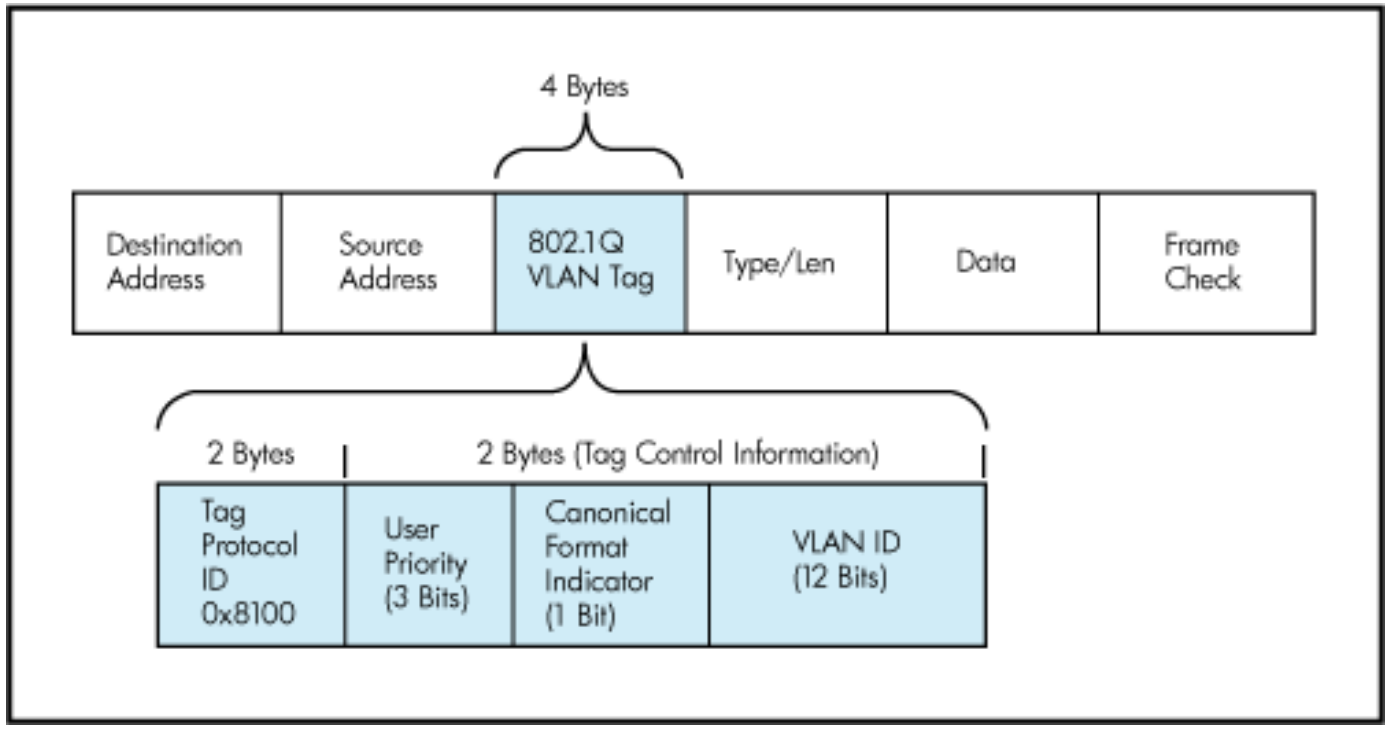
IEEE 802.1Q: Typical Deployment Scenario



QUEEN'S UNIVERSITY BELFAST

IEEE 802.1Q: VLAN Header Format

Background



QUEEN'S UNIVERSITY BELFAST

Summary

- Network Access Control

- Authentication, Authorization, Accounting
  - RADIUS - Networking protocol providing centralized AAA services
  - Kerberos – Network Authentication Protocol

- Network Access Enforcement
  - IEEE 802.1X port-based Network Access Control
  - IEEE 802.1Q virtual local area networks (VLANs)

QUEEN'S UNIVERSITY BELFAST

Questions?

Next Session: AAA/Firewalls – Part 2

Friday, 22 February 2019

QUEEN'S UNIVERSITY BELFAST