

## Rete di ateneo wired

L'infrastruttura di rete implementata è dotata di dorsali in fibra ottica a 10 Gbps. Gli apparati di distribuzione supportano la tecnologia Multi-Gig, consentendo una connettività cablata verso i pc/notebook/apparecchiature con velocità da 1 Gbps fino a 5 Gbps.

Tutte le dorsali sono progettate per la massima resilienza grazie a una ridondanza attiva basata su un doppio collegamento in fibra ottica, assicurando così la continuità del servizio anche in caso di guasto.

## Rete di ateneo wireless

Sono state installate antenne Wi-Fi 6E con interfacce multi-gig a 2,5 Gbps che assicurano connessioni veloci e stabili anche in aree ad alta densità.

Tutte le antenne Wi-Fi sono connesse a un doppio controller configurato in alta affidabilità. Questa architettura garantisce la continuità del servizio e la stabilità della connessione.

## Autenticazione alla rete di Ateneo

L'autenticazione alla rete di ateneo si basa sull'utilizzo del protocollo IEEE 802.1X e di un server centrale RADIUS per la validazione degli accessi (Wired e Wi-Fi), principalmente in due modalità:

- Autenticazione con Certificato (EAP-TLS): Il dispositivo utente e il server RADIUS di zona si autenticano reciprocamente tramite certificati digitali emessi dalla Certification Authority (CA) di Ateneo. Garantisce accesso automatico e trasparente agli utenti e massima integrità della rete.
- MAC Authentication Bypass (MAB): Utilizzato per autenticare dispositivi non-802.1X attraverso l'indirizzo MAC.

Questa modalità di autenticazione permette la gestione centralizzata della segmentazione logica della rete, utilizzando il server Radius per l'assegnazione dinamica delle vlan.

## Cyber Security

La sicurezza della rete è garantita attraverso una suddivisione geografica in zone. Ciascuna zona è protetta da Firewall NGWF (Next-Generation Firewall) configurati in alta affidabilità e caratterizzati da elevate prestazioni.

Questi apparati utilizzano motori di ispezione avanzati, continuamente aggiornati, che permettono:

- **Identificazione Precisa (App-ID):** Di riconoscere e controllare le applicazioni reali in transito, indipendentemente dalla porta utilizzata, superando le limitazioni dei firewall tradizionali.
- **Prevenzione in Linea:** Di confrontare il traffico in tempo reale con le firme di minacce note (malware, exploit) e le liste di siti web malevoli, garantendo prestazioni di prevenzione delle minacce elevate e proattive.

### **Monitoraggio rete di Ateneo:**

Gli apparati della rete di Ateneo sono sottoposti a monitoraggio continuo e vengono regolarmente aggiornati. Tali attività sono gestite da un gruppo NOC (Network Operations Center) dedicato, preposto alla supervisione e alla risoluzione di eventuali guasti.

### **Modalità di utilizzo:**

Per tutti i punti precedenti e per garantire una gestione armonica e funzionale della rete di Ateneo, è prevista la presenza in loco di un team informatico in grado di intervenire con rapidità e autonomia.

Le modalità di utilizzo dei servizi per il personale informatico delle strutture è riportato di seguito.

Le casistiche riportate riguardano interventi "programmati"/evolutivi, resta inteso che in caso di problematiche di funzionamento, i tempi di intervento saranno gestiti con livello di urgenza (risoluzione appena individuato il "guasto"). Si consideri che essendo attivo un servizio di monitoraggio tali casistiche dovrebbero essere gestite in modalità proattiva da ASIT.



TIPOLOGIA INTERVENTO	MODALITA' DI APERTURA DELLA RICHIESTA	TEMPO DI PRESA IN CARICO	TEMPO DI RISOLUZIONE	Descrizione intervento
Autenticazione su rete wired di un dispositivo	giorni lavorativi lun-ven (8.00-17.30) ticket coda ASIT - Infrastrutture Digitali Territoriali "Supporto Informatico Piovego Nord (Zona01)"; in alternativa: 049827(3722). Sconsigliato ma modalità fruibile: sarà l'helpdesk ASIT ad aprire il relativo ticket	immediato	10 minuti	L'intervento consiste nell'abilitare il MAC Address (che dovrà essere fornito dal richiedente) per l'autenticazione in rete del dispositivo (in base al dispositivo ci saranno VLAN differenti).
Collegamento al dominio di Ateneo (Zona 01)	giorni lavorativi lun-ven (8.00-17.30) ticket coda ASIT - Infrastrutture Digitali Territoriali "Supporto Informatico Piovego"	immediato	10 minuti	Il tecnico locale sarà dotato di un account con il quale potrà aggiungere la postazione al dominio. Il ticket servirà per spostare la postazione nella corretta OU (Organization Unit)



	Nord (Zona01)"; in alternativa: 049827(3722) Sconsigliato ma modalità fruibile: sarà l'helpdesk ASIT ad aprire il relativo ticket			
Modifiche alle policy di dominio di Ateneo	giorni lavorativi lun-ven (8.00-17.30) ticket coda ASIT - Infrastrutture Digitali Territoriali "Supporto Informatico Piovego Nord (Zona01)"; in alternativa: 049827(3722) Sconsigliato ma modalità fruibile: sarà l'helpdesk ASIT ad aprire il relativo ticket	2 ore lavorative	NBD (Next Business Day)	La risoluzione dell'intervento dipende dal tipo di richiesta, se compatibile con le policy generali di Ateneo. Se ciò non fosse verrà data evidenza e motivazione al richiedente, con conseguente chiusura del ticket.
Richieste WIFI (richieste utenti guest)	giorni lavorativi lun-ven (8.00-17.30) ticket coda ASIT -	immediato	10 minuti	Già oggi il WIFI è gestito da ASIT Si rappresenta che: - Verrà implementata anche la possibilità di stampa su Eduroam.



	<p>Infrastrutture Digitali Territoriali “Supporto Informatico Piovego Nord (Zona01)”; in alternativa: 049827(3722) Sconsigliato ma modalità fruibile: sarà l’helpdesk ASIT ad aprire il relativo ticket</p>			<ul style="list-style-type: none"> <li>- è in attivazione un portale a disposizione dei dipartimenti per gestione autonoma di queste tipologie di utenti per l’accesso ai servizi digitali di Ateneo.</li> </ul>
<p>Richieste reti WIFI “Custom” (ad es. Convegni/Eventi)</p>	<p>giorni lavorativi lun-ven (8.00-17.30) ticket coda ASIT - Infrastrutture Digitali Territoriali “Supporto Informatico Piovego Nord (Zona01)”; in alternativa: 049827(3722) Sconsigliato ma modalità fruibile: sarà l’helpdesk ASIT ad aprire il relativo ticket</p>	<p>8 ore lavorative</p>	<p>5 giorni lavorativi</p>	



Richieste abilitazioni/modifiche regole firewall/accesso ai sistemi	giorni lavorativi lun-ven (8.00-17.30) ticket coda ASIT - Infrastrutture Digitali Territoriali "Supporto Informatico Piovego Nord (Zona01)"; in alternativa: 049827(3722) Sconsigliato ma modalità fruibile: sarà l'helpdesk ASIT ad aprire il relativo ticket	2 ore lavorative	NBD (Next Business Day)	La risoluzione dell'intervento dipende dal tipo di richiesta, se compatibile con le policy generali di Ateneo. Se ciò non fosse verrà data evidenza e motivazione al richiedente.
Attivazione nuove utenze				In avvio entro fine 2025 una piattaforma di gestione degli utenti esterni a livello di Ateneo con identificazione e rilascio accesso credenziali SSO (@ext.unipd.it) a cura dei singoli referenti di Dipartimento che verranno individuati. Il DPSS è già stato coinvolto per l'avvio.